



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

Cisco IOS Release 15.0(2)SE

2012 年 8 月

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco IE 3000 スイッチ ソフトウェア コンフィギュレーション ガイド
Copyright © 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

はじめに xlix

対象読者 xlix

目的 xlix

表記法 xlix

関連資料 i

マニュアルの入手方法およびテクニカル サポート li

CHAPTER 1

概要 1-1

機能 1-1

使用および導入を簡素化する機能 1-2

パフォーマンス向上機能 1-2

管理オプション 1-4

管理の簡易性に関する機能 1-4

アベイラビリティおよび冗長性に関する機能 1-7

VLAN 機能 1-8

セキュリティ機能 1-8

QoS および CoS 機能 1-12

レイヤ 3 機能 1-13

モニタ機能 1-14

スイッチ初期設定後のデフォルト値 1-15

ネットワークの構成例 1-18

スイッチを使用する場合の設計概念 1-18

Ethernet-to-the-Factory アーキテクチャ 1-20

企業ゾーン 1-20

非武装ゾーン 1-21

製造ゾーン 1-21

トポロジーのオプション 1-23

次の作業 1-26

CHAPTER 2

コマンドライン インターフェイスの使用法 2-1

コマンド モードの概要 2-1

ヘルプ システムの概要 2-3

コマンドの省略形 2-4

コマンドの no 形式および default 形式の概要 2-4

- CLI のエラー メッセージ 2-5
- コンフィギュレーション ロギングの使用法 2-5
- コマンド履歴の使用法 2-6
 - コマンド履歴バッファ サイズの変更 2-6
 - コマンドの呼び出し 2-6
 - コマンド履歴機能のディセーブル化 2-7
- 編集機能の使用法 2-7
 - 編集機能のイネーブル化およびディセーブル化 2-7
 - キーストロークによるコマンドの編集 2-8
 - 画面幅よりも長いコマンドラインの編集 2-9
- show および more コマンド出力の検索およびフィルタリング 2-10
- CLI のアクセス 2-10
 - コンソール接続または Telnet による CLI アクセス 2-10

CHAPTER 3

スイッチ アラームの設定 3-1

- スイッチ アラームの概要 3-1
 - グローバル ステータス モニタリング アラーム 3-2
 - FCS エラー ヒステリシスしきい値 3-2
 - ポート ステータス モニタリング アラーム 3-2
 - アラーム発生オプション 3-3
- 外部アラームの設定 3-4
- スイッチ アラームの設定 3-6
 - デフォルトのスイッチ アラーム設定 3-6
 - 電源装置アラームの設定 3-7
 - スイッチの温度アラームの設定 3-7
 - スイッチのプライマリ温度しきい値の設定 3-7
 - スイッチのセカンダリ温度しきい値の設定 3-8
 - 温度アラームのリレーへの関連付け 3-8
 - FCS Bit Error Rate アラームの設定 3-9
 - FCS エラーしきい値の設定 3-10
 - FCS エラー ヒステリシスしきい値の設定 3-10
 - アラーム プロファイルの設定 3-11
 - アラーム プロファイルの作成または変更 3-11
 - 特定のポートへのアラーム プロファイルの割り当て 3-12
 - SNMP トラップのイネーブル化 3-13
- スイッチ アラーム ステータスの表示 3-13

CHAPTER 4

スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て 4-1

起動プロセスの概要 4-1

スイッチ情報の割り当て 4-3

デフォルトのスイッチ情報 4-3

DHCP ベースの自動設定の概要 4-4

DHCP クライアント要求プロセス 4-4

DHCP ベースの自動設定およびイメージ アップデートの概要 4-5

DHCP 自動設定 4-5

DHCP 自動イメージ アップデート 4-6

制限事項と制約事項 4-6

DHCP ベースの自動設定の設定 4-7

DHCP サーバ設定時の注意事項 4-7

TFTP サーバの設定 4-8

DNS の設定 4-8

リレー デバイスの設定 4-9

コンフィギュレーション ファイルの入手方法 4-9

構成例 4-10

DHCP 自動設定機能およびイメージ アップデート機能 4-12

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定 4-12

DHCP 自動イメージ アップデート（コンフィギュレーション ファイルおよびイメージ）の設定 4-13

クライアントの設定 4-15

手動でのスイッチ情報の割り当て 4-16

実行コンフィギュレーションの確認および保存 4-16

スタートアップ コンフィギュレーションの変更 4-17

起動のデフォルト設定 4-18

コンフィギュレーション ファイルの自動ダウンロード 4-18

システム コンフィギュレーションを読み書きするためのファイル名の指定 4-18

手動で起動する場合 4-19

特定のソフトウェア イメージを起動する場合 4-20

環境変数の制御 4-20

ソフトウェア イメージ リロードのスケジュール設定 4-22

リロードのスケジュール設定 4-22

リロード スケジュール情報の表示 4-23

CHAPTER 5

Cisco IOS Configuration Engine の設定 5-1

Cisco Configuration Engine ソフトウェアの概要 5-1

コンフィギュレーション サービス 5-2

イベント サービス 5-3

NSM	5-3
CNS ID およびデバイスのホスト名に関する重要事項	5-3
ConfigID	5-3
DeviceID	5-4
ホスト名および DeviceID	5-4
ホスト名、DeviceID、ConfigID の使用方法	5-4
Cisco IOS エージェントの概要	5-5
初期設定	5-5
差分（部分）設定	5-6
同期設定	5-6
Cisco IOS エージェントの設定	5-6
自動 CNS 設定のイネーブル化	5-7
CNS イベント エージェントのイネーブル化	5-7
Cisco IOS CNS エージェントのイネーブル化	5-9
初期設定のイネーブル化	5-9
部分設定のイネーブル化	5-13
CNS 設定の表示	5-14

CHAPTER 6

スイッチのクラスタ化 6-1

スイッチ クラスタの概要	6-1
クラスタ コマンド スイッチの特性	6-3
スタンバイ クラスタ コマンド スイッチの特性	6-3
候補スイッチおよびクラスタ メンバ スイッチの特性	6-3
スイッチ クラスタのプランニング	6-4
クラスタ候補およびクラスタ メンバの自動検出	6-4
CDP ホップを使用しての検出	6-5
CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出	6-7
異なる VLAN からの検出	6-7
異なる管理 VLAN からの検出	6-8
RP による検出	6-9
新しく設置したスイッチの検出	6-10
HSRP およびスタンバイ クラスタ コマンド スイッチ	6-11
仮想 IP アドレス	6-12
クラスタ スタンバイ グループに関する他の考慮事項	6-12
クラスタ設定の自動回復	6-13
IP アドレス	6-14
ホスト名	6-14
パスワード	6-15
SNMP コミュニティ ストリング	6-15

TACACS+ および RADIUS	6-15
LRE プロファイル	6-16
CLI によるスイッチ クラスタの管理	6-16
SNMP によるスイッチ クラスタの管理	6-17

CHAPTER 7

スイッチの管理 7-1

システム日時の管理	7-1
システム クロックの概要	7-1
NTP の概要	7-2
NTP バージョン 4	7-3
手動での日時の設定	7-4
システム クロックの設定	7-4
日時設定の表示	7-5
タイム ゾーンの設定	7-5
夏時間の設定	7-6
システム名およびプロンプトの設定	7-7
デフォルトのシステム名およびプロンプトの設定	7-8
システム名の設定	7-8
DNS の概要	7-8
DNS のデフォルト設定	7-9
DNS の設定	7-9
DNS の設定の表示	7-10
バナーの作成	7-10
バナーのデフォルト設定	7-11
MoTD ログイン バナーの設定	7-11
ログイン バナーの設定	7-12
MAC アドレス テーブルの管理	7-12
アドレス テーブルの作成	7-13
MAC アドレスおよび VLAN	7-13
MAC アドレス テーブルのデフォルト設定	7-14
アドレス エージング タイムの変更	7-14
ダイナミック アドレス エントリの削除	7-15
MAC アドレス変更通知トラップの設定	7-15
MAC アドレス移動通知トラップの設定	7-17
MAC しきい値通知トラップの設定	7-19
スタティック アドレス エントリの追加および削除	7-20
ユニキャスト MAC アドレス フィルタリングの設定	7-21
VLAN の MAC アドレス ラーニングのディセーブル化	7-22
アドレス テーブル エントリの表示	7-24

ARP テーブルの管理 7-24

CHAPTER 8

PTP の設定 8-1

- 高精度時間プロトコルの概要 8-1
- PTP の設定 8-2
 - デフォルト コンフィギュレーション 8-2
 - PTP の設定 8-3
- PTP 設定の表示 8-4

CHAPTER 9

PROFINET の設定 9-1

- PROFINET の概要 9-1
 - PROFINET 装置の役割 9-2
 - PROFINET 装置のデータ交換 9-2
- PROFINET の設定 9-4
 - デフォルト コンフィギュレーション 9-4
 - PROFINET のイネーブル化 9-5
- PROFINET 設定の表示 9-5
- PROFINET のトラブルシューティング 9-5

CHAPTER 10

SDM テンプレートの設定 10-1

- SDM テンプレートの概要 10-1
 - デュアル IPv4/IPv6 SDM テンプレート 10-2
- スイッチ SDM テンプレートの設定 10-3
 - デフォルトの SDM テンプレート 10-3
 - SDM テンプレートの設定時の注意事項 10-3
 - SDM テンプレートの設定 10-4
- SDM テンプレートの表示 10-5

CHAPTER 11

スイッチ ベース認証の設定 11-1

- スイッチへの不正アクセスの防止 11-1
- 特権 EXEC コマンドへのアクセスの保護 11-2
 - デフォルトのパスワードおよび権限レベル設定 11-3
 - スタティック イネーブル パスワードの設定または変更 11-3
 - 暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 11-4
 - パスワード回復のディセーブル化 11-5
 - 端末回線に対する Telnet パスワードの設定 11-6
 - ユーザ名とパスワードのペアの設定 11-7
 - 複数の権限レベルの設定 11-9

コマンドの権限レベルの設定	11-9
回線に対するデフォルトの権限レベルの変更	11-10
権限レベルへのログインおよび終了	11-11
TACACS+ によるスイッチ アクセスの制御	11-11
TACACS+ の概要	11-11
TACACS+ の動作	11-13
TACACS+ の設定	11-14
TACACS+ のデフォルト設定	11-14
TACACS+ サーバホストの特定および認証キーの設定	11-14
TACACS+ ログイン認証の設定	11-15
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定	11-17
TACACS+ アカウンティングの起動	11-18
AAA サーバが到達不能な場合のルータとのセッションの確立	11-19
TACACS+ 設定の表示	11-19
RADIUS によるスイッチ アクセスの制御	11-19
RADIUS の概要	11-19
RADIUS の動作	11-21
RADIUS 許可の変更	11-21
概要	11-22
Change-of-Authorization 要求	11-22
CoA 要求応答コード	11-24
CoA 要求コマンド	11-25
RADIUS の設定	11-28
RADIUS のデフォルト設定	11-28
RADIUS サーバホストの識別	11-29
RADIUS ログイン認証の設定	11-31
AAA サーバグループの定義	11-33
ユーザイネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定	11-35
RADIUS アカウンティングの起動	11-36
AAA サーバが到達不能な場合のルータとのセッションの確立	11-37
すべての RADIUS サーバの設定	11-37
ベンダー固有の RADIUS 属性を使用するスイッチ設定	11-37
ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定	11-39
スイッチ上での CoA の設定	11-40
CoA 機能のモニタリングおよびトラブルシューティング	11-41
RADIUS サーバロード バランシングの設定	11-41
RADIUS の設定の表示	11-41
Kerberos によるスイッチ アクセスの制御	11-41

Kerberos の概要	11-42
Kerberos の動作	11-44
境界スイッチに対する認証の取得	11-44
KDC からの TGT の取得	11-45
ネットワーク サービスに対する認証の取得	11-45
Kerberos の設定	11-45
スイッチのローカル認証および許可の設定	11-46
SSH のためのスイッチの設定	11-47
SSH の概要	11-47
SSH サーバ、統合クライアント、およびサポートされているバージョン	11-47
制限事項	11-48
SSH の設定	11-48
設定時の注意事項	11-48
スイッチで SSH を実行するためのセットアップ	11-49
SSH サーバの設定	11-50
SSH の設定およびステータスの表示	11-51
SSL HTTP のためのスイッチの設定	11-51
セキュア HTTP サーバおよびクライアントの概要	11-51
CA のトラストポイント	11-52
CipherSuite	11-53
セキュア HTTP サーバおよびクライアントの設定	11-53
SSL のデフォルト設定	11-54
SSL の設定時の注意事項	11-54
CA のトラストポイントの設定	11-54
セキュア HTTP サーバの設定	11-55
セキュア HTTP クライアントの設定	11-56
セキュア HTTP サーバおよびクライアントのステータスの表示	11-57
SCP のためのスイッチの設定	11-57
Secure Copy に関する情報	11-58

CHAPTER 12

IEEE 802.1x ポートベース認証の設定	12-1
IEEE 802.1x ポートベース認証の概要	12-1
デバイスの役割	12-2
認証プロセス	12-3
認証の開始およびメッセージ交換	12-5
認証マネージャ	12-7
ポートベースの認証方法	12-7
ユーザ単位 ACL および Filter-Id	12-8
認証マネージャ CLI コマンド	12-9

許可ステートおよび無許可ステートのポート	12-10
802.1x のホスト モード	12-11
マルチドメイン認証	12-12
802.1x 複数認証モード	12-13
MAC Move	12-13
MAC 置換	12-14
802.1x アカウンティング	12-14
802.1x アカウンティング属性値ペア	12-15
802.1x 準備状態チェック	12-16
VLAN 割り当てを使用した 802.1x 認証	12-16
ユーザ単位 ACL を使用した 802.1x 認証の使用	12-17
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証	12-19
Cisco Secure ACS およびリダイレクト URL の属性と値のペア	12-20
Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア	12-20
VLAN ID ベース MAC 認証	12-21
ゲスト VLAN を使用した 802.1x 認証	12-21
制限付き VLAN を使用した 802.1x 認証	12-22
アクセス不能認証バイパスを使用した 802.1x 認証	12-23
複数認証ポートのサポート	12-23
認証結果	12-24
機能の相互作用	12-24
音声 VLAN ポートを使用した 802.1x 認証	12-25
ポート セキュリティを使用した 802.1x 認証	12-25
Wake-on-LAN を使用した 802.1x 認証	12-25
MAC 認証バイパスによる 802.1x 認証	12-26
802.1x ユーザ ディストリビューション	12-27
802.1x ユーザ ディストリビューションの設定時の注意事項	12-27
Network Admission Control レイヤ 2 802.1x 検証	12-28
柔軟な認証の順序設定	12-28
Open1x 認証	12-29
音声認識 802.1x セキュリティの使用	12-29
Network Edge Access Topology (NEAT) を使用した 802.1x サプリカントおよび オーセンティケータ	12-29
注意事項	12-30
ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用	12-31
コモン セッション ID	12-31
802.1x 認証の設定	12-32
802.1x 認証のデフォルト設定	12-33
802.1x 認証設定時の注意事項	12-34
802.1x 認証	12-34

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス	12-35
MAC 認証バイパス	12-36
ポートあたりのデバイスの最大数	12-36
802.1x 準備状態チェックの設定	12-36
音声対応 802.1x セキュリティの設定	12-37
802.1x 違反モードの設定	12-38
802.1x 認証の設定	12-39
スイッチおよび RADIUS サーバ間の通信の設定	12-41
ホスト モードの設定	12-42
定期的な再認証の設定	12-43
ポートに接続するクライアントの手動での再認証	12-44
待機時間の変更	12-44
スイッチからクライアントへの再送信時間の変更	12-45
スイッチからクライアントへのフレーム再送信回数の設定	12-46
再認証回数	12-46
MAC Move のイネーブル化	12-47
MAC 置換のイネーブル化	12-48
802.1X アカウンティングの設定	12-48
ゲスト VLAN の設定	12-49
制限付き VLAN の設定	12-50
アクセス不能認証バイパス機能の設定	12-52
WoL を使用した 802.1x 認証の設定	12-55
MAC 認証バイパスの設定	12-56
802.1x ユーザ ディストリビューションの設定	12-56
NAC レイヤ 2 802.1x 検証の設定	12-57
NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定	12-58
Auto Smartport マクロを使用した NEAT の設定	12-60
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定	12-60
ダウンロード可能な ACL の設定	12-60
ダウンロード ポリシーの設定	12-60
VLAN ID ベース MAC 認証の設定	12-62
柔軟な認証順序の設定	12-63
Open1x の設定	12-63
ポート上での 802.1x 認証のディセーブル化	12-64
802.1x 認証設定のデフォルト値へのリセット	12-65
802.1x の統計情報およびステータスの表示	12-65

CHAPTER 13**Web ベース認証の設定 13-1**

Web ベース認証の概要 13-1

デバイスの役割 13-2

ホストの検出 13-2

セッションの作成 13-3

認証プロセス 13-3

ローカル Web 認証バナー 13-4

Web 認証カスタマイズ可能な Web ページ 13-6

注意事項 13-6

その他の機能と Web ベース認証の相互作用 13-7

ポート セキュリティ 13-7

LAN ポート IP 13-7

ゲートウェイ IP 13-8

ACL 13-8

コンテキストベース アクセス コントロール 13-8

802.1x 認証 13-8

EtherChannel 13-8

Web ベース認証の設定 13-9

デフォルトの Web ベース認証の設定 13-9

Web ベース認証の設定に関する注意事項と制約事項 13-9

Web ベース認証の設定タスク リスト 13-10

認証ルールとインターフェイスの設定 13-10

AAA 認証の設定 13-11

スイッチおよび RADIUS サーバ間の通信の設定 13-12

HTTP サーバの設定 13-13

認証プロキシ Web ページのカスタマイズ 13-14

成功ログインに対するリダイレクション URL の指定 13-15

Web ベース認証パラメータの設定 13-16

Web 認証ローカル バナーの設定 13-16

Web ベース認証キャッシュ エントリの削除 13-17

Web ベース認証ステータスの表示 13-17

CHAPTER 14**インターフェイス特性の設定 14-1**

インターフェイス タイプの概要 14-1

ポートベースの VLAN 14-2

スイッチ ポート 14-2

アクセス ポート 14-3

トランク ポート 14-3

トンネル ポート 14-4

ルータポート	14-4
スイッチ仮想インターフェイス	14-5
SVI 自動ステート除外	14-6
EtherChannel ポート グループ	14-6
デュアルパーパス アップリンク ポート	14-7
インターフェイスの接続	14-7
インターフェイス コンフィギュレーション モードの使用法	14-8
インターフェイスの設定手順	14-9
インターフェイス範囲の設定	14-10
インターフェイス レンジ マクロの設定および使用法	14-12
イーサネット インターフェイスの設定	14-13
イーサネット インターフェイスのデフォルト設定	14-14
デュアルパーパス アップリンク ポートのタイプの設定	14-15
インターフェイス速度およびデュプレックス モードの設定	14-17
速度とデュプレックス モードの設定時の注意事項	14-17
インターフェイス速度およびデュプレックス パラメータの設定	14-18
IEEE 802.3x フロー制御の設定	14-19
インターフェイスでの Auto-MDIX の設定	14-20
インターフェイスに関する記述の追加	14-21
レイヤ 3 インターフェイスの設定	14-22
SVI 自動ステート除外の設定	14-24
システム最大伝送単位 (MTU) の設定	14-24
インターフェイスのモニタリングおよびメンテナンス	14-26
インターフェイス ステータスのモニタ	14-26
インターフェイスおよびカウンタのクリアとリセット	14-27
インターフェイスのシャットダウンおよび再起動	14-28

CHAPTER 15**SmartPort マクロの設定 15-1**

SmartPort マクロの概要	15-1
SmartPort マクロの設定	15-1
SmartPort のデフォルト設定	15-1
SmartPort 設定時の注意事項	15-2
SmartPort マクロの適用	15-3
SmartPort マクロの表示	15-5

CHAPTER 16**VLAN の設定 16-1**

VLAN の概要	16-1
サポートされる VLAN	16-2
VLAN ポート メンバーシップ モード	16-3

標準範囲 VLAN の設定	16-5
トークンリング VLAN	16-6
標準範囲 VLAN 設定時の注意事項	16-6
標準範囲 VLAN の設定	16-7
イーサネット VLAN のデフォルト設定	16-7
イーサネット VLAN の作成または変更	16-8
VLAN の削除	16-9
VLAN へのスタティック アクセス ポートの割り当て	16-10
拡張範囲 VLAN の設定	16-11
VLAN のデフォルト設定	16-11
拡張範囲 VLAN 設定時の注意事項	16-11
拡張範囲 VLAN の作成	16-12
内部 VLAN ID を指定した拡張範囲 VLAN の作成	16-14
VLAN の表示	16-15
VLAN トランクの設定	16-15
トランキングの概要	16-15
IEEE 802.1Q の設定に関する考慮事項	16-17
レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定	16-17
トランク ポートとしてのイーサネット インターフェイスの設定	16-17
他の機能との相互作用	16-18
トランク ポートの設定	16-19
トランクでの許可 VLAN の定義	16-20
プルーニング適格リストの変更	16-21
タグなしトラフィック用ネイティブ VLAN の設定	16-22
トランク ポートの負荷分散の設定	16-22
STP ポート プライオリティによる負荷分散	16-23
STP パス コストによる負荷分散	16-24
VMPS の設定	16-26
VMPS の概要	16-26
ダイナミックアクセス ポート VLAN メンバーシップ	16-27
VMPS クライアントのデフォルト設定	16-27
VMPS 設定時の注意事項	16-27
VMPS クライアントの設定	16-28
VMPS の IP アドレスの入力	16-28
VMPS クライアント上のダイナミックアクセス ポートの設定	16-29
VLAN メンバーシップの再確認	16-29
再確認インターバルの変更	16-30
再試行回数の変更	16-30
VMPS のモニタリング	16-31

ダイナミックアクセス ポート VLAN メンバーシップのトラブルシューティング 16-31
 VMPS の設定例 16-32

CHAPTER 17

VTP の設定 17-1

VTP の概要 17-1
 VTP ドメイン 17-2
 VTP モード 17-3
 VTP アドバタイズ 17-3
 VTP バージョン 2 17-4
 VTP バージョン 3 17-5
 VTP プルーニング 17-5
 VTP の設定 17-7
 VTP のデフォルト設定 17-8
 VTP 設定時の注意事項 17-8
 ドメイン名 17-9
 パスワード 17-9
 VTP バージョン 17-9
 設定要件 17-10
 VTP モードの設定 17-10
 VTP バージョン 3 のパスワードの設定 17-13
 VTP バージョン 3 のプライマリ サーバの設定 17-14
 VTP バージョンのイネーブル化 17-14
 VTP プルーニングのイネーブル化 17-15
 ポート単位の VTP の設定 17-16
 VTP ドメインへの VTP クライアント スイッチの追加 17-16
 VTP のモニタ 17-18

CHAPTER 18

音声 VLAN の設定 18-1

音声 VLAN の概要 18-1
 Cisco IP Phone の音声トラフィック 18-2
 Cisco IP Phone のデータ トラフィック 18-2
 音声 VLAN の設定 18-3
 音声 VLAN のデフォルト設定 18-3
 音声 VLAN 設定時の注意事項 18-3
 Cisco7960 IP Phone に接続するポートの設定 18-4
 Cisco IP Phone の音声トラフィックの設定 18-5
 着信データ フレームのプライオリティ設定 18-6
 音声 VLAN の表示 18-7

CHAPTER 19**プライベート VLAN の設定 19-1**

プライベート VLAN の概要 19-1

プライベート VLAN での IP アドレッシング方式 19-3

複数のスイッチの PVLAN 19-4

プライベート VLAN の他機能との相互作用 19-5

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト
トラフィック 19-5

プライベート VLAN と SVI 19-5

プライベート VLAN の設定 19-6

プライベート VLAN の設定手順 19-6

デフォルトのプライベート VLAN 設定 19-6

プライベート VLAN 設定時の注意事項 19-6

セカンダリ VLAN およびプライマリ VLAN の設定 19-7

プライベート VLAN ポート設定 19-8

他の機能に関連する制約事項 19-9

プライベート VLAN 内の VLAN の設定および対応付け 19-10

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定 19-11

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定 19-12

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング
19-13

プライベート VLAN のモニタリング 19-15

CHAPTER 20**IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定 20-1**

IEEE 802.1Q トンネリングの概要 20-1

IEEE 802.1Q トンネリングの設定 20-4

IEEE 802.1Q トンネリングのデフォルト設定 20-4

IEEE 802.1Q トンネリング設定時の注意事項 20-4

ネイティブ VLAN 20-4

システム MTU 20-5

IEEE 802.1Q トンネリングおよびその他の機能 20-6

IEEE 802.1Q トンネリング ポートの設定 20-6

レイヤ 2 プロトコル トンネリングの概要 20-8

レイヤ 2 プロトコル トンネリングの設定 20-11

レイヤ 2 プロトコル トンネリングのデフォルト設定 20-12

レイヤ 2 プロトコル トンネリング設定時の注意事項 20-12

レイヤ 2 プロトコル トンネリングの設定 20-13

EtherChannel のレイヤ 2 トンネリングの設定 20-15

サービスプロバイダー エッジ スイッチの設定 20-15

カスタマー スイッチの設定 20-16

トンネリング ステータスのモニタリングおよびメンテナンス 20-18

CHAPTER 21

STP の設定 21-1

スパニングツリー機能の概要 21-1

STP の概要 21-2

スパニングツリー トポロジと BPDU 21-3

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID 21-4

スパニングツリー インターフェイス ステート 21-4

ブロッキング ステート 21-6

リスニング ステート 21-6

ラーニング ステート 21-6

フォワーディング ステート 21-7

ディセーブル ステート 21-7

スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み 21-7

スパニングツリーおよび冗長接続 21-8

スパニングツリー アドレスの管理 21-8

接続を維持するためのエージング タイムの短縮 21-9

スパニングツリー モードおよびプロトコル 21-9

サポートされるスパニングツリー インスタンス 21-10

スパニングツリーの相互運用性と下位互換性 21-10

STP および IEEE 802.1Q トランク 21-10

VLAN ブリッジ スパニングツリー 21-11

スパニングツリー機能の設定 21-11

スパニングツリー機能のデフォルト設定 21-12

スパニングツリー設定時の注意事項 21-12

スパニングツリー モードの変更 21-14

スパニングツリーのディセーブル化 21-15

ルート スイッチの設定 21-15

セカンダリ ルート スイッチの設定 21-17

ポート プライオリティの設定 21-17

パス コストの設定 21-19

VLAN のスイッチ プライオリティの設定 21-20

スパニングツリー タイマーの設定 21-21

hello タイムの設定 21-21

VLAN の転送遅延時間の設定 21-22

VLAN の最大エージング タイムの設定 21-22

転送保留カウンタの設定 21-23

スパニングツリー ステータスの表示 21-23

CHAPTER 22

MSTP の設定 22-1

- MSTP の概要 22-2
 - MST リージョン 22-2
 - IST、CIST、CST 22-2
 - MST リージョン内の動作 22-3
 - MST リージョン間の動作 22-4
 - IEEE 802.1s の用語 22-5
 - ホップ カウント 22-5
 - 境界ポート 22-6
 - IEEE 802.1s の実装 22-6
 - ポートの役割名の変更 22-7
 - レガシー スイッチと標準スイッチの相互運用 22-7
 - 単一方向リンクの失敗の検出 22-8
 - IEEE 802.1D STP との相互運用性 22-8
- RSTP の概要 22-9
 - ポートの役割およびアクティブ トポロジ 22-9
 - 高速コンバージェンス 22-10
 - ポート ロールの同期 22-11
 - BPDU のフォーマットおよびプロセス 22-12
 - 優位 BPDU 情報の処理 22-13
 - 下位 BPDU 情報の処理 22-13
 - トポロジの変更 22-13
- MSTP 機能の設定 22-14
 - MSTP のデフォルト設定 22-15
 - MSTP 設定時の注意事項 22-15
 - MST リージョンの設定および MSTP のイネーブル化 22-16
 - ルート スイッチの設定 22-18
 - セカンダリ ルート スイッチの設定 22-19
 - ポート プライオリティの設定 22-20
 - パス コストの設定 22-21
 - スイッチのプライオリティの設定 22-22
 - hello タイムの設定 22-23
 - 転送遅延時間の設定 22-24
 - 最大経過時間の設定 22-24
 - 最大ホップ カウントの設定 22-25
 - リンク タイプの指定による高速移行の保証 22-25
 - ネイバー タイプの指定 22-26
 - プロトコル移行プロセスの再起動 22-26
- MST コンフィギュレーションおよびステータスの表示 22-27

CHAPTER 23

オプションのスパニングツリー機能の設定 23-1

オプションのスパニングツリー機能の概要 23-1

PortFast の概要 23-2

BPDU ガードの概要 23-2

BPDU フィルタリングの概要 23-3

UplinkFast の概要 23-3

BackboneFast の概要 23-5

EtherChannel ガードの概要 23-7

ルート ガードの概要 23-8

ループ ガードの概要 23-9

オプションのスパニングツリー機能の設定 23-9

オプションのスパニングツリー機能のデフォルト設定 23-10

オプションのスパニングツリー設定時の注意事項 23-10

PortFast のイネーブル化 23-10

BPDU ガードのイネーブル化 23-11

BPDU フィルタリングのイネーブル化 23-12

冗長リンク用 UplinkFast のイネーブル化 23-14

BackboneFast のイネーブル化 23-14

EtherChannel ガードのイネーブル化 23-15

ルート ガードのイネーブル化 23-16

ループ ガードのイネーブル化 23-16

スパニングツリー ステータスの表示 23-17

CHAPTER 24

Resilient Ethernet Protocol の設定 24-1

REP の概要 24-1

リンク完全性 24-3

短時間でのコンバージェンス 24-4

VLAN ロード バランシング 24-4

スパニングツリー インタラクション 24-6

REP ポート 24-6

REP の設定 24-6

REP のデフォルト設定 24-7

REP 設定時の注意事項 24-7

REP 管理 VLAN の設定 24-9

REP インターフェイスの設定 24-10

VLAN ロード バランシングの手動によるプリエンプシヨンの設定 24-14

REP の SNMP トラップ設定 24-14

REP のモニタ 24-15

CHAPTER 25

Flex Link および MAC アドレス テーブル移動更新機能の設定 25-1

- Flex Link および MAC アドレス テーブル移動更新機能の概要 25-1
 - Flex Link 25-1
 - VLAN Flex Link ロード バランシングおよびサポート 25-2
 - Flex Link マルチキャスト高速コンバージェンス 25-3
 - その他の Flex Link ポートを mrouter ポートとして学習 25-3
 - IGMP レポートの生成 25-4
 - IGMP レポートのリーク 25-4
 - 設定例 25-4
- MAC アドレス テーブル移動更新 25-6
- Flex Link および MAC アドレス テーブル移動更新の設定 25-7
 - デフォルト設定 25-8
 - 設定時の注意事項 25-8
 - Flex Link の設定 25-9
 - Flex Link の VLAN ロード バランシングの設定 25-11
 - MAC アドレス テーブル移動更新機能の設定 25-12
- Flex Link および MAC アドレス テーブル移動更新機能のモニタ 25-15

CHAPTER 26

DHCP 機能と IP ソース ガード機能の設定 26-1

- DHCP スヌーピングの理解 26-1
 - DHCP サーバ 26-2
 - DHCP リレー エージェント 26-2
 - DHCP Snooping 26-2
 - Option 82 データ挿入 26-4
 - Cisco IOS DHCP サーバ データベース 26-7
 - DHCP スヌーピング バインディング データベース 26-7
- DHCP スヌーピングの設定 26-9
 - DHCP スヌーピングのデフォルト設定 26-9
 - DHCP スヌーピング設定時の注意事項 26-10
 - DHCP リレー エージェントの設定 26-11
 - パケット転送アドレスの指定 26-11
 - DHCP スヌーピングおよび Option 82 のイネーブル化 26-13
 - プライベート VLAN での DHCP スヌーピングのイネーブル化 26-14
 - Cisco IOS DHCP サーバ データベースのイネーブル化 26-15
 - DHCP スヌーピング バインディング データベース エージェントのイネーブル化 26-15
- DHCP スヌーピング情報の表示 26-16
- IP ソース ガードの概要 26-17
 - 送信元 IP アドレスのフィルタリング 26-17
 - 送信元 IP アドレスおよび MAC アドレスのフィルタリング 26-17

スタティック ホスト用 IP ソース ガード	26-18
IP ソース ガードの設定	26-19
デフォルトの IP ソース ガード設定	26-19
IP ソース ガード設定時の注意事項	26-19
IP ソース ガードのイネーブル化	26-20
スタティック ホスト用 IP ソース ガードの設定	26-21
レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定	26-21
プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定	26-25
IP ソース ガード情報の表示	26-28
DHCP サーバ ポートベースのアドレス割り当ての概要	26-28
DHCP サーバ ポートベースのアドレス割り当ての設定	26-28
ポートベースのアドレス テーブルのデフォルト設定	26-29
ポートベースのアドレス割り当て設定時の注意事項	26-29
DHCP サーバ ポートベースのアドレス割り当てのイネーブル化	26-29
DHCP サーバ ポートベースのアドレス割り当ての表示	26-31

CHAPTER 27

ダイナミック ARP インспекションの設定	27-1
ダイナミック ARP インспекションの概要	27-1
インターフェイスの信頼状態とネットワーク セキュリティ	27-3
ARP パケットのレート制限	27-4
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ	27-5
廃棄パケットのロギング	27-5
ダイナミック ARP インспекションの設定	27-5
ダイナミック ARP インспекションのデフォルト設定	27-6
ダイナミック ARP インспекション設定時の注意事項	27-6
DHCP 環境でのダイナミック ARP インспекションの設定	27-7
非 DHCP 環境での ARP ACL の設定	27-9
着信 ARP パケットのレート制限	27-11
確認検査の実行	27-12
ログ バッファの設定	27-13
ダイナミック ARP インспекション情報の表示	27-15

CHAPTER 28

IGMP スヌーピングおよび MVR の設定	28-1
IGMP スヌーピングの概要	28-2
IGMP のバージョン	28-3
マルチキャスト グループへの加入	28-3
マルチキャスト グループからの脱退	28-5
即時脱退	28-5

IGMP 脱退タイマーの設定	28-6
IGMP レポート抑制	28-6
IGMP スヌーピングの設定	28-7
IGMP スヌーピングのデフォルト設定	28-7
IGMP スヌーピングのイネーブル化およびディセーブル化	28-7
スヌーピング方法の設定	28-8
マルチキャスト ルータ ポートの設定	28-9
グループに加入するホストの静的な設定	28-10
IGMP 即時脱退のイネーブル化	28-11
IGMP 脱退タイマーの設定	28-11
TCN 関連のコマンドの設定	28-12
TCN イベント後のマルチキャスト フラッディング時間の制御	28-12
フラッディング モードからの回復	28-13
TCN イベント中のマルチキャスト フラッディングのディセーブル化	28-14
IGMP スヌーピング クエリアの設定	28-14
IGMP レポート抑制のディセーブル化	28-16
IGMP スヌーピング情報の表示	28-16
MVR の概要	28-18
マルチキャスト TV アプリケーションで MVR を使用する場合	28-18
MVR の設定	28-20
MVR のデフォルト設定	28-20
MVR 設定時の注意事項および制限事項	28-21
MVR グローバル パラメータの設定	28-21
MVR インターフェイスの設定	28-23
MVR 情報の表示	28-24
IGMP フィルタリングおよびスロットリングの設定	28-25
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定	28-26
IGMP プロファイルの設定	28-26
IGMP プロファイルの適用	28-27
IGMP グループの最大数の設定	28-28
IGMP スロットリング アクションの設定	28-29
IGMP フィルタリングおよび IGMP スロットリング設定の表示	28-30

CHAPTER 29

ポート単位のトラフィック制御の設定 29-1

ストーム制御の設定	29-1
ストーム制御の概要	29-1
ストーム制御のデフォルト設定	29-3
ストーム制御およびしきい値レベルの設定	29-3
小さいフレームの着信レートの設定	29-5

- 保護ポートの設定 29-6
 - 保護ポートのデフォルト設定 29-7
 - 保護ポート設定時の注意事項 29-7
 - 保護ポートの設定 29-7
- ポート ブロッキングの設定 29-7
 - ポート ブロッキングのデフォルト設定 29-8
 - インターフェイスでのフラッディング トラフィックのブロッキング 29-8
- ポート セキュリティの設定 29-9
 - ポート セキュリティの概要 29-9
 - セキュア MAC アドレス 29-9
 - セキュリティ違反 29-10
 - ポート セキュリティのデフォルト設定 29-12
 - ポート セキュリティの設定時の注意事項 29-12
 - ポート セキュリティのイネーブル化および設定 29-14
 - ポート セキュリティ エージングのイネーブル化および設定 29-18
 - ポート セキュリティおよびプライベート VLAN 29-20
- プロトコル ストーム プロテクションの設定 29-20
 - プロトコル ストーム プロテクションの概要 29-21
 - デフォルトのプロトコル ストーム プロテクションの設定 29-21
 - プロトコル ストーム プロテクションのイネーブル化 29-21
- ポート単位のトラフィック制御設定の表示 29-22

CHAPTER 30

- SPAN および RSPAN の設定 30-1**
 - SPAN および RSPAN の概要 30-1
 - ローカル SPAN 30-2
 - リモート SPAN 30-2
 - SPAN と RSPAN の概念および用語 30-3
 - SPAN セッション 30-3
 - 監視対象トラフィック 30-4
 - 送信元ポート 30-5
 - 送信元 VLAN 30-6
 - VLAN フィルタリング 30-6
 - 宛先ポート 30-7
 - RSPAN VLAN 30-8
 - SPAN および RSPAN と他の機能の相互作用 30-8
- SPAN および RSPAN の設定 30-9
 - SPAN および RSPAN のデフォルト設定 30-9
 - ローカル SPAN の設定 30-10
 - SPAN 設定時の注意事項 30-10

ローカル SPAN セッションの作成	30-11
ローカル SPAN セッションの作成および着信トラフィックの設定	30-13
フィルタリングする VLAN の指定	30-15
RSPAN の設定	30-16
RSPAN 設定時の注意事項	30-16
RSPAN VLAN としての VLAN の設定	30-17
RSPAN 送信元セッションの作成	30-18
RSPAN 宛先セッションの作成	30-19
RSPAN 宛先セッションの作成および着信トラフィックの設定	30-20
フィルタリングする VLAN の指定	30-22
SPAN および RSPAN のステータス表示	30-23

CHAPTER 31

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定	31-1
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要	31-1
LLDP-MED	31-2
ワイヤード ロケーション サービス	31-3
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定	31-4
デフォルトの LLDP 設定	31-4
設定時の注意事項	31-4
LLDP のイネーブル化	31-5
LLDP 特性の設定	31-6
LLDP-MED TLV の設定	31-6
Network-Policy TLV の設定	31-7
ロケーション TLV およびワイヤード ロケーション サービスの設定	31-9
LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス	31-10

CHAPTER 32

CDP の設定	32-1
CDP の概要	32-1
CDP の設定	32-2
CDP のデフォルト設定	32-2
CDP の特性の設定	32-3
CDP のディセーブル化およびイネーブル化	32-3
インターフェイス上での CDP のディセーブル化およびイネーブル化	32-4
CDP のモニタおよびメンテナンス	32-5

CHAPTER 33

UDLD の設定	33-1
UDLD の概要	33-1
動作モード	33-1

単一方向の検出方法 33-2

UDLD の設定 33-3

UDLD のデフォルト設定 33-4

設定時の注意事項 33-4

UDLD のグローバルなイネーブル化 33-5

インターフェイス上での UDLD のイネーブル化 33-5

UDLD によってディセーブル化されたインターフェイスのリセット 33-6

UDLD ステータスの表示 33-7

CHAPTER 34**RMON の設定 34-1**

RMON の概要 34-1

RMON の設定 34-3

RMON のデフォルト設定 34-3

RMON アラームおよびイベントの設定 34-3

インターフェイス上でのグループ履歴統計情報の収集 34-5

インターフェイス上でのイーサネット グループ統計情報の収集 34-6

RMON ステータスの表示 34-6

CHAPTER 35**システム メッセージ ロギングの設定 35-1**

システム メッセージ ロギングの概要 35-1

システム メッセージ ロギングの設定 35-2

システム ログ メッセージのフォーマット 35-2

システム メッセージ ロギングのデフォルト設定 35-3

メッセージ ロギングのディセーブル化 35-4

メッセージ表示宛先デバイスの設定 35-5

ログ メッセージの同期化 35-6

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 35-8

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 35-8

メッセージ重大度の定義 35-9

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限 35-10

設定変更ロガーのイネーブル化 35-11

UNIX Syslog サーバの設定 35-12

UNIX Syslog デーモンへのログ メッセージ 35-13

UNIX システム ロギング機能の設定 35-13

ロギング設定の表示 35-14

CHAPTER 36**SNMP の設定 36-1**

SNMP の概要 36-1

SNMP バージョン 36-2

SNMP マネージャ機能	36-3
SNMP エージェント機能	36-4
SNMP コミュニティ スtring	36-4
SNMP を使用して MIB 変数にアクセスする方法	36-4
SNMP 通知	36-5
SNMP ifIndex MIB オブジェクト値	36-6
SNMP の設定	36-6
SNMP のデフォルト設定	36-7
SNMP 設定時の注意事項	36-7
SNMP エージェントのディセーブル化	36-8
コミュニティ スtring の設定	36-8
SNMP グループおよびユーザの設定	36-10
SNMP 通知の設定	36-13
CPU しきい値通知のタイプと値の設定	36-17
エージェント コンタクトおよびロケーションの設定	36-17
SNMP を通して使用する TFTP サーバの制限	36-18
SNMP の例	36-18
SNMP ステータスの表示	36-19

CHAPTER 37**組み込みイベント マネージャの設定 37-1**

組み込みイベント マネージャの概要	37-1
イベント検出器	37-2
組み込みイベント マネージャの処理	37-4
組み込みイベント マネージャ ポリシー	37-4
組み込みイベント マネージャの環境変数	37-4
組み込みイベント マネージャの設定	37-5
組み込みイベント マネージャ アプレットの登録と定義	37-5
組み込みイベント マネージャ TCL スクリプトの登録と定義	37-6
組み込みイベント マネージャ情報の表示	37-7

CHAPTER 38**ACL によるネットワーク セキュリティの設定 38-1**

ACL の概要	38-1
サポートされる ACL	38-2
ポート ACL	38-3
ルータ ACL	38-4
VLAN マップ	38-5
フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理	38-5
IPv4 ACL の設定	38-6

標準 IPv4 ACL および拡張 IPv4 ACL の作成	38-7
アクセス リスト番号	38-8
ACL のロギング	38-8
番号制標準 ACL の作成	38-9
番号付き拡張 ACL の作成	38-10
ACL 内の ACE の並べ替え	38-15
名前付き標準 ACL および名前付き拡張 ACL の作成	38-15
ACL での時間範囲の使用	38-17
ACL へのコメントの挿入	38-19
端末回線への IPv4 ACL の適用	38-20
インターフェイスへの IPv4 ACL の適用	38-20
ハードウェアおよびソフトウェアによる IP ACL の処理	38-22
ACL のトラブルシューティング	38-22
IPv4 ACL の設定例	38-24
番号制 ACL	38-25
拡張 ACL	38-25
名前付き ACL	38-26
IP ACL に適用される時間範囲	38-26
コメント付きの IP ACL エントリ	38-27
ACL のロギング	38-27
名前付き MAC 拡張 ACL の作成	38-28
レイヤ 2 インターフェイスへの MAC ACL の適用	38-30
VLAN マップの設定	38-31
VLAN マップの設定時の注意事項	38-32
VLAN マップの作成	38-33
ACL および VLAN マップの例	38-33
VLAN への VLAN マップの適用	38-35
ネットワークでの VLAN マップの使用法	38-36
ワイヤリング クローゼットの設定	38-36
別の VLAN にあるサーバへのアクセスの拒否	38-37
ルータ ACL を VLAN マップと組み合わせて使用方法	38-38
VLAN マップとルータ ACL の設定時の注意事項	38-38
VLAN に適用されるルータ ACL と VLAN マップの例	38-39
ACL およびスイッチド パケット	38-39
ACL およびブリッジド パケット	38-40
ACL およびルーテッド パケット	38-41
ACL およびマルチキャスト パケット	38-41
IPv4 ACL の設定の表示	38-43

CHAPTER 39

QoS の設定 39-1

QoS の概要 39-2

QoS の基本モデル 39-3

分類 39-5

QoS ACL に基づく分類 39-8

クラス マップおよびポリシー マップに基づく分類 39-8

ポリシングおよびマーキング 39-9

物理ポートのポリシング 39-10

SVI のポリシング 39-11

マッピング テーブル 39-13

キューイングおよびスケジューリングの概要 39-14

WTD 39-14

SRR のシェーピングおよび共有 39-15

入力キューでのキューイングおよびスケジューリング 39-16

出力キューでのキューイングおよびスケジューリング 39-17

パケットの変更 39-20

自動 QoS の設定 39-21

生成される自動 QoS 設定 39-21

コンフィギュレーションにおける自動 QoS の影響 39-26

自動 QoS 設定時の注意事項 39-26

VoIP 用自動 QoS のイネーブル化 39-27

自動 QoS 設定例 39-29

自動 QoS 情報の表示 39-30

標準 QoS の設定 39-31

標準 QoS のデフォルト設定 39-31

入力キューのデフォルト設定 39-32

出力キューのデフォルト設定 39-32

マッピング テーブルのデフォルト設定 39-33

標準 QoS 設定時の注意事項 39-34

QoS ACL の注意事項 39-34

インターフェイスへの QoS の適用 39-34

ポリシングの注意事項 39-35

一般的な QoS の注意事項 39-35

QoS のグローバルなイネーブル化 39-36

物理ポートで VLAN ベースの QoS をイネーブル化 39-36

ポートの信頼状態による分類の設定 39-37

QoS ドメイン内のポートの信頼状態の設定 39-37

インターフェイスの CoS 値の設定 39-39

ポート セキュリティを確保するための信頼境界機能の設定 39-39

DSCP トランスペアレント モードのイネーブル化	39-41
別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定	39-41
QoS ポリシーの設定	39-43
ACL によるトラフィックの分類	39-44
クラス マップによるトラフィックの分類	39-47
ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング	39-49
階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング	39-53
集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング	39-60
DSCP マップの設定	39-62
CoS/DSCP マップの設定	39-63
IP precedence/DSCP マップの設定	39-64
ポリシング済み DSCP マップの設定	39-65
DSCP/CoS マップの設定	39-66
DSCP/DSCP 変換マップの設定	39-67
入力キューの特性の設定	39-68
入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定	39-69
入力キュー間のバッファ スペースの割り当て	39-70
入力キュー間の帯域幅の割り当て	39-71
入力プライオリティ キューの設定	39-71
出力キューの特性の設定	39-72
設定時の注意事項	39-73
出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定	39-73
出力キューおよび ID への DSCP または CoS 値のマッピング	39-75
出力キューでの SRR シェーピング重みの設定	39-76
出力キューでの SRR 共有重みの設定	39-77
出力緊急キューの設定	39-78
出カインターフェイスの帯域幅の制限	39-79
標準 QoS 情報の表示	39-80

CHAPTER 40

EtherChannel およびリンクステート トラッキングの設定 40-1

EtherChannel の概要	40-1
EtherChannel の概要	40-2
ポートチャネル インターフェイス	40-3
ポート集約プロトコル	40-4
PAgP モード	40-5
PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出	40-5

PAgP と他の機能との相互作用	40-6
LACP	40-6
LACP モード	40-6
LACP と他の機能との相互作用	40-7
EtherChannel の On モード	40-7
ロード バランシングおよび転送方式	40-7
EtherChannel の設定	40-9
EtherChannel のデフォルト設定	40-10
EtherChannel 設定時の注意事項	40-10
レイヤ 2 EtherChannel の設定	40-11
レイヤ 3 EtherChannel の設定	40-14
ポートチャネル論理インターフェイスの作成	40-14
物理インターフェイスの設定	40-15
EtherChannel ロード バランシングの設定	40-17
PAgP 学習方式およびプライオリティの設定	40-18
LACP ホットスタンバイ ポートの設定	40-19
LACP システム プライオリティの設定	40-20
LACP ポート プライオリティの設定	40-20
EtherChannel、PAgP、および LACP ステータスの表示	40-21
リンクステート トラッキングの概要	40-22
リンクステート トラッキングの設定	40-24
デフォルトのリンクステート トラッキングの設定	40-25
リンクステート トラッキングの設定時の注意事項	40-25
リンクステート トラッキングの設定	40-25
リンクステート トラッキング ステータスの表示	40-26

CHAPTER 41

IP ユニキャスト ルーティングの設定	41-1
IP ルーティングの概要	41-2
ルーティング タイプ	41-2
ルーティングを設定する手順	41-3
IP アドレス指定の設定	41-4
アドレス指定のデフォルト設定	41-4
ネットワーク インターフェイスへの IP アドレスの割り当て	41-5
サブネット ゼロの使用	41-6
クラスレス ルーティング	41-7
アドレス解決方法の設定	41-8
スタティック ARP キャッシュの定義	41-9
ARP カプセル化の設定	41-10
プロキシ ARP のイネーブル化	41-11

IP ルーティングがディセーブルの場合のルーティング支援機能	41-11
プロキシ ARP	41-11
デフォルト ゲートウェイ	41-12
IRDP	41-12
ブロードキャスト パケットの処理方法の設定	41-14
ダイレクト ブロードキャストから物理ブロードキャストへの変換のイネーブル化	41-14
UDP ブロードキャスト パケットおよびプロトコルの転送	41-15
IP ブロードキャスト アドレスの確立	41-16
IP ブロードキャストのフラッディング	41-17
IP アドレスのモニタリングおよびメンテナンス	41-18
IP ユニキャスト ルーティングのイネーブル化	41-19
RIP の設定	41-20
RIP のデフォルト設定	41-20
基本的な RIP パラメータの設定	41-21
RIP 認証の設定	41-23
サマリー アドレスおよびスプリット ホライズンの設定	41-24
スプリット ホライズンの設定	41-25
OSPF の設定	41-26
OSPF のデフォルト設定	41-27
OSPF NSF 認識	41-28
基本的な OSPF パラメータの設定	41-28
OSPF インターフェイスの設定	41-29
OSPF エリア パラメータの設定	41-31
その他の OSPF パラメータの設定	41-32
LSA グループ ペーシングの変更	41-34
ループバック インターフェイスの設定	41-34
OSPF のモニタリング	41-35
EIGRP の設定	41-35
EIGRP のデフォルト設定	41-37
EIGRP NSF 認識	41-38
基本的な EIGRP パラメータの設定	41-39
EIGRP インターフェイスの設定	41-40
EIGRP ルート認証の設定	41-40
EIGRP スタブルルーティングの設定	41-42
EIGRP のモニタリングおよびメンテナンス	41-43
BGP の設定	41-43
BGP のデフォルト設定	41-45
NSF 認識	41-48

BGP ルーティングのイネーブル化	41-48
ルーティング ポリシー変更の管理	41-51
BGP 判断属性の設定	41-52
ルート マップによる BGP フィルタリングの設定	41-54
ネイバーによる BGP フィルタリングの設定	41-55
BGP フィルタリング用のプレフィックス リストの設定	41-56
BGP コミュニティ フィルタリングの設定	41-57
BGP ネイバーおよびピア グループの設定	41-59
集約アドレスの設定	41-61
ルーティング ドメイン連合の設定	41-62
BGP ルート リフレクタの設定	41-62
ルート ダンプニングの設定	41-63
BGP のモニタリングおよびメンテナンス	41-64
ISO CLNS ルーティングの設定	41-65
IS-IS ダイナミック ルーティングの設定	41-66
IS-IS のデフォルト設定	41-67
NSF 認識	41-68
IS-IS ルーティングのイネーブル化	41-68
IS-IS グローバル パラメータの設定	41-70
IS-IS インターフェイス パラメータの設定	41-73
ISO IGRP と IS-IS のモニタリングおよびメンテナンス	41-75
Multi-VRF CE の設定	41-76
Multi-VRF CE の概要	41-76
Multi-VRF CE のデフォルト設定	41-78
マルチ VRF CE の設定時の注意事項	41-78
VRF の設定	41-80
マルチキャスト VRF の設定	41-80
VRF 認識サービスの設定	41-81
ARP のユーザ インターフェイス	41-82
ping のユーザ インターフェイス	41-82
SNMP のユーザ インターフェイス	41-82
HSRP のユーザ インターフェイス	41-83
Syslog のユーザ インターフェイス	41-83
traceroute のユーザ インターフェイス	41-84
FTP および TFTP のユーザ インターフェイス	41-84
VPN ルーティング セッションの設定	41-85
BGP PE/CE ルーティング セッションの設定	41-85
Multi-VRF CE の設定例	41-86
Multi-VRF CE ステータスの表示	41-90

プロトコル独立機能の設定	41-90
CEF の設定	41-90
等コスト ルーティング パスの個数の設定	41-92
スタティックユニキャスト ルートの設定	41-92
デフォルトのルートおよびネットワークの指定	41-94
ルート マップによるルーティング情報の再配信	41-95
ポリシーベース ルーティングの設定	41-98
PBR 設定時の注意事項	41-99
PBR のイネーブル化	41-100
ルーティング情報のフィルタリング	41-102
受動インターフェイスの設定	41-103
ルーティング アップデートのアドバタイズおよび処理の制御	41-103
ルーティング情報の送信元のフィルタリング	41-104
認証キーの管理	41-105
IP ネットワークのモニタリングおよびメンテナンス	41-106

CHAPTER 42

IPv6 ユニキャスト ルーティングの設定 42-1

IPv6 の概要	42-1
IPv6 アドレス	42-2
サポート対象の IPv6 ユニキャスト ルーティング機能	42-2
128 ビット幅のユニキャスト アドレス	42-3
IPv6 の DNS	42-4
IPv6 ユニキャストのパス MTU ディスカバリ	42-4
ICMPv6	42-4
ネイバー探索	42-4
DRP	42-4
IPv6 のステートレス自動設定および重複アドレス検出	42-5
IPv6 アプリケーション	42-5
デュアル IPv4/IPv6 プロトコル スタック	42-5
DHCP for IPv6 アドレスの割り当て	42-6
IPv6 のスタティック ルート	42-7
IPv6 の RIP	42-7
IPv6 の OSPF の設定	42-7
OSPFv3 グレースフル リスタート	42-7
EIGRP IPv6	42-8
IPv6 の HSRP	42-8
IPv6 上の SNMP および Syslog	42-8
IPv6 による HTTP (S)	42-9
サポートされていない IPv6 ユニキャスト ルーティング機能	42-9
制限事項	42-10

IPv6 の設定	42-10
IPv6 のデフォルト設定	42-11
IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル	42-11
DRP の設定	42-14
IPv4 および IPv6 プロトコル スタックの設定	42-15
DHCP for IPv6 アドレス割り当ての設定	42-16
DHCPv6 アドレス割り当てのデフォルト設定	42-16
DHCPv6 アドレス割り当ての設定時の注意事項	42-16
DHCPv6 サーバ機能のイネーブル化	42-17
DHCPv6 クライアント機能のイネーブル化	42-19
IPv6 ICMP レート制限の設定	42-19
IPv6 の CEF の設定	42-20
IPv6 のスタティック ルートの設定	42-20
IPv6 RIP の設定	42-22
IPv6 OSPF の設定	42-23
IPv6 の EIGRP の設定	42-25
IPv6 の HSRP の設定	42-25
HSRP バージョン 2 のイネーブル化	42-26
IPv6 の HSRP グループのイネーブル化	42-26
IPv6 の表示	42-28

CHAPTER 43

IPv6 マルチキャストの実装 43-1

IPv6 マルチキャストの実装に関する情報	43-1
IPv6 マルチキャストの概要	43-1
IPv6 マルチキャスト ルーティングの実装	43-2
MLD アクセス グループ	43-4
受信側の明示的トラッキング	43-4
IPv6 マルチキャスト ユーザ認証およびプロファイル サポート	43-4
IPv6 MLD プロキシ	43-5
プロトコル独立マルチキャスト	43-5
PIM スパース モード	43-5
IPv6 BSR : RP マッピングの設定	43-7
PIM 送信元固有マルチキャスト	43-8
ルーティング可能アドレスの hello オプション	43-10
双方向 PIM	43-10
スタティック mroute	43-11
MRIB	43-11
MFIB	43-11
分散型 MFIB	43-12
IPv6 マルチキャスト VRF Lite	43-12

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング	43-12
IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP	43-13
IPv6 マルチキャストでの NSF と SSO のサポート	43-14
IPv6 マルチキャストの帯域幅ベースの CAC	43-14
IPv6 マルチキャストの実装	43-14
IPv6 マルチキャスト ルーティングのイネーブル化	43-14
MLD プロトコルのカスタマイズおよび確認	43-15
インターフェイスでの MLD のカスタマイズおよび確認	43-15
MLD グループ制限の実装	43-16
受信側の明示的トラッキングによってホストの動作を追跡するための設定	43-17
マルチキャスト ユーザ認証およびプロファイル サポートの設定	43-18
IPv6 での MLD プロキシのイネーブル化	43-19
MLD トラフィック カウンタのリセット	43-20
MLD インターフェイス カウンタのクリア	43-21
PIM の設定	43-21
PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示	43-21
PIM オプションの設定	43-22
双方向 PIM の設定および双方向 PIM 情報の表示	43-23
PIM トラフィック カウンタのリセット	43-24
PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット	43-24
BSR の設定	43-25
BSR の設定および BSR 情報の確認	43-25
BSR への PIM RP アドバタイズメントの送信	43-26
限定スコープ ゾーン内で BSR を使用できるようにするための設定	43-26
BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定	43-27
SSM マッピングの設定	43-27
スタティック mroute の設定	43-28
IPv6 マルチキャストでの MFIB の使用	43-29
IPv6 マルチキャストでの MFIB の動作の確認	43-30
MFIB トラフィック カウンタのリセット	43-31

CHAPTER 44

IPv6 MLD スヌーピングの設定 44-1

MLD スヌーピングの概要	44-1
MLD メッセージ	44-2
MLD クエリー	44-3
マルチキャスト クライアント エージングの堅牢性	44-3
マルチキャスト ルータ検出	44-3
MLD レポート	44-4
MLD Done メッセージおよび即時脱退	44-4
TCN 処理	44-5

IPv6 MLD スヌーピングの設定	44-5
MLD スヌーピングのデフォルト設定	44-5
MLD スヌーピング設定時の注意事項	44-6
MLD スヌーピングのイネーブル化またはディセーブル化	44-6
スタティックなマルチキャスト グループの設定	44-8
マルチキャスト ルータ ポートの設定	44-8
MLD 即時脱退のイネーブル化	44-9
MLD スヌーピング クエリーの設定	44-10
MLD リスナー メッセージ抑制のディセーブル化	44-11
MLD スヌーピング情報の表示	44-12

CHAPTER 45**IPv6 ACL の設定 45-1**

IPv6 ACL の概要	45-1
サポートされる ACL 機能	45-2
IPv6 ACL の制限事項	45-3
IPv6 ACL の設定	45-3
IPv6 ACL のデフォルト設定	45-4
他の機能との相互作用	45-4
IPv6 ACL の作成	45-4
インターフェイスへの IPv6 ACL の適用	45-7
IPv6 ACL の表示	45-8

CHAPTER 46**HSRP および VRRP の設定 46-1**

HSRP の概要	46-1
HSRP のバージョン	46-3
MHSRP	46-4
HSRP の設定	46-4
HSRP のデフォルト設定	46-5
HSRP HSRP 設定時の注意事項	46-6
HSRP のイネーブル化	46-6
HSRP のプライオリティの設定	46-8
MHSRP の設定	46-10
HSRP 認証およびタイマーの設定	46-11
ICMP リダイレクト メッセージの HSRP サポートのイネーブル化	46-12
HSRP グループおよびクラスタリングの設定	46-12
HSRP のトラブルシューティング	46-12
HSRP 設定の表示	46-13
VRRP の設定	46-13
VRRP の制限事項	46-14

CHAPTER 47

Cisco IOS IP SLA 動作の設定 47-1

Cisco IOS IP SLA の概要 47-1

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定 47-3

IP SLA Responder と IP SLA コントロール プロトコル 47-4

IP SLA の応答時間の計算 47-4

IP SLA 動作のスケジューリング 47-5

IP SLA 動作のしきい値のモニタリング 47-5

IP SLA 動作の設定 47-6

デフォルト設定 47-6

設定時の注意事項 47-6

IP SLA Responder の設定 47-8

UDP ジッタ動作を使用した IP サービス レベルの分析 47-8

ICMP エコー動作を使用した IP サービス レベルの分析 47-11

IP SLA 動作のモニタリング 47-13

CHAPTER 48

拡張オブジェクト トラッキングの設定 48-1

拡張オブジェクト トラッキングの概要 48-1

拡張オブジェクト トラッキング機能の設定 48-2

デフォルト設定 48-2

インターフェイス ラインプロトコルまたは IP ルーティング ステートの追跡 48-2

追跡リストの設定 48-3

ブール式による追跡リストの設定 48-4

重みしきい値による追跡リストの設定 48-5

パーセントしきい値による追跡リストの設定 48-6

HSRP オブジェクト トラッキングの設定 48-7

その他の追跡特性の設定 48-8

IP SLA オブジェクト トラッキングの設定 48-9

スタティック ルーティング サポートの設定 48-10

プライマリ インターフェイスの設定 48-11

Cisco IP SLA モニタリング エージェントおよびトラック オブジェクトの設定 48-11

ルーティング ポリシーおよびデフォルト ルートの設定 48-12

拡張オブジェクト トラッキングのモニタリング 48-13

CHAPTER 49

WCCP を使用した Web キャッシュ サービスの設定 49-1

WCCP の概要 49-1

WCCP メッセージ交換 49-2

WCCP ネゴシエーション 49-3

MD5 セキュリティ 49-3

パケットのリダイレクトおよびサービス グループ 49-3

サポートしない WCCP 機能	49-4
WCCP の設定	49-5
WCCP のデフォルト設定	49-5
WCCP 設定時の注意事項	49-5
Web Cache Service のイネーブル化	49-6
WCCP のモニタおよびメンテナンス	49-10

CHAPTER 50

IP マルチキャスト ルーティングの設定 50-1

Cisco IP マルチキャスト ルーティングの実装の概要	50-1
IGMP の概要	50-3
IGMPv1	50-3
IGMPv2	50-4
PIM の概要	50-4
PIM のバージョン	50-4
PIM のモード	50-4
PIM スタブルーティング	50-5
IGMP ヘルパー	50-6
自動 RP	50-7
BSR	50-7
マルチキャスト転送および逆経路チェック	50-8
DVMRP の概要	50-9
CGMP の概要	50-9
IP マルチキャスト ルーティングの設定	50-10
マルチキャスト ルーティングのデフォルト設定	50-10
マルチキャスト ルーティング設定時の注意事項	50-11
PIMv1 および PIMv2 の相互運用性	50-11
自動 RP および BSR 設定時の注意事項	50-12
基本的なマルチキャスト ルーティングの設定	50-12
Source-Specific Multicast の設定	50-14
SSM コンポーネントの概要	50-14
Internet Standard Multicast と SSM の違い	50-14
SSM IP アドレスの範囲	50-15
SSM の動作	50-15
IGMPv3 ホスト シグナリング	50-16
設定時の注意事項	50-16
SSM の設定	50-17
SSM のモニタリング	50-17
Source-Specific Multicast マッピングの設定	50-17
設定時の注意事項	50-18

SSM マッピングの概要	50-18
SSM マッピングの設定	50-20
SSM マッピングのモニタリング	50-23
PIM スタブルルーティングの設定	50-23
PIM スタブルルーティングの設定時の注意事項	50-23
PIM スタブルルーティングのイネーブル化	50-24
RP の設定	50-25
マルチキャスト グループへの RP の手動割り当て	50-25
自動 RP の設定	50-27
PIMv2 BSR の設定	50-31
自動 RP および BSR の使用法	50-35
RP マッピング情報のモニタ	50-36
PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング	50-36
高度な PIM 機能の設定	50-37
PIM 共有ツリーおよび送信元ツリーの概要	50-37
PIM SPT 使用の延期	50-38
PIM ルータクエリー メッセージ インターバルの変更	50-39
オプションの IGMP 機能の設定	50-40
IGMP のデフォルト設定	50-41
グループのメンバーとしてのスイッチの設定	50-41
IP マルチキャスト グループへのアクセスの制御	50-42
IGMP バージョンの変更	50-43
IGMP ホストクエリー メッセージ インターバルの変更	50-43
IGMPv2 の IGMP クエリー タイムアウトの変更	50-44
IGMPv2 の最大クエリー応答時間の変更	50-45
静的に接続されたメンバーとしてのスイッチの設定	50-45
オプションのマルチキャスト ルーティング機能の設定	50-46
CGMP サーバ サポート機能のイネーブル化	50-46
sdr リスナー サポート機能の設定	50-47
sdr リスナー サポート機能のイネーブル化	50-48
sdr キャッシュ エントリの存在期間の制限	50-48
IP マルチキャスト境界の設定	50-49
基本的な DVMRP 相互運用性機能の設定	50-50
DVMRP 相互運用性設定	50-51
DVMRP トンネルの設定	50-53
DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ	50-55
mrinfo 要求への応答	50-55
高度な DVMRP 相互運用性機能の設定	50-56
DVMRP ユニキャスト ルーティングのイネーブル化	50-56

DVMRP の非ルーティング ネイバーの拒否	50-57
ルート交換の制御	50-59
アダプタイズされる DVMRP ルート数の制限	50-59
DVMRP ルートしきい値の変更	50-59
DVMRP サマリー アドレスの設定	50-60
DVMRP 自動サマライズのディセーブル化	50-62
DVMRP ルートへのメトリック オフセットの追加	50-62
IP マルチキャスト ルーティングのモニタおよびメンテナンス	50-63
キャッシュ、テーブル、およびデータベースのクリア	50-63
システムおよびネットワーク統計情報の表示	50-64
IP マルチキャスト ルーティングのモニタ	50-65

CHAPTER 51**MSDP の設定 51-1**

MSDP の概要	51-1
MSDP の動作	51-2
MSDP の利点	51-3
MSDP の設定	51-3
MSDP のデフォルト設定	51-4
デフォルトの MSDP ピアの設定	51-4
SA ステートのキャッシング	51-6
MSDP ピアからの送信元情報の要求	51-8
スイッチから発信される送信元情報の制御	51-8
送信元の再配信	51-9
SA 要求メッセージのフィルタリング	51-10
スイッチで転送される送信元情報の制御	51-11
フィルタの使用法	51-12
SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限	51-13
スイッチで受信される送信元情報の制御	51-13
MSDP メッシュ グループの設定	51-15
MSDP ピアのシャットダウン	51-15
MSDP への境界 PIM DM 領域の追加	51-16
RP アドレス以外の発信元アドレスの設定	51-17
MSDP のモニタおよびメンテナンス	51-18

CHAPTER 52**フォールバック ブリッジングの設定 52-1**

フォールバック ブリッジングの概要	52-1
フォールバック ブリッジングの設定	52-3
フォールバック ブリッジングのデフォルト設定	52-3

フォールバック ブリッジング設定時の注意事項	52-4
ブリッジ グループの作成	52-4
スパニングツリー パラメータの調整	52-6
VLAN ブリッジ スパニングツリー プライオリティの変更	52-6
インターフェイス プライオリティの変更	52-7
パス コストの割り当て	52-7
BPDU インターバルの調整	52-8
インターフェイスでのスパニングツリーのディセーブル化	52-10
フォールバック ブリッジングのモニタおよびメンテナンス	52-11

CHAPTER 53

トラブルシューティング 53-1

ソフトウェアで障害が発生した場合の回復	53-2
パスワードを忘れた場合の回復	53-3
コマンド スイッチで障害が発生した場合の回復	53-4
故障したコマンド スイッチをクラスタ メンバと交換する場合	53-5
故障したコマンド スイッチを他のスイッチと交換する場合	53-6
クラスタ メンバスイッチとの接続の回復	53-8
自動ネゴシエーションの不一致の防止	53-8
PoE スイッチ ポートのトラブルシューティング	53-8
電力消失によるポートの障害	53-9
不正リンク アップによるポート障害	53-9
SFP モジュールのセキュリティと識別	53-9
SFP モジュール ステータスのモニタリング	53-10
ping の使用	53-10
ping の概要	53-10
ping の実行	53-10
レイヤ 2 traceroute の使用	53-11
レイヤ 2 traceroute の概要	53-12
使用上のガイドライン	53-12
物理パスの表示	53-13
IP traceroute の使用	53-13
IP traceroute の概要	53-13
IP traceroute の実行	53-14
TDR の使用	53-15
TDR の概要	53-15
TDR の実行および結果の表示	53-15
debug コマンドの使用	53-16
特定機能に関するデバッグのイネーブル化	53-16

システム全体診断のイネーブル化	53-17
デバッグおよびエラーメッセージ出力のリダイレクト	53-17
show platform forward コマンドの使用	53-17
crashinfo ファイルの使用	53-20
基本 crashinfo ファイル	53-20
拡張 crashinfo ファイル	53-20
トラブルシューティング表	53-21
CPU 使用率に関するトラブルシューティング	53-21
CPU 使用率が高い場合に起こりうる症状	53-21
問題と原因の検証	53-21

APPENDIX A

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作 A-1

フラッシュ ファイル システムの操作	A-1
使用可能なファイル システムの表示	A-2
デフォルト ファイル システムの設定	A-2
ファイル システムのファイルに関する情報の表示	A-3
ディレクトリの変更および作業ディレクトリの表示	A-4
ディレクトリの作成および削除	A-4
ファイルのコピー	A-5
ファイルの削除	A-5
tar ファイルの作成、表示、および抽出	A-6
tar ファイルの作成	A-6
tar ファイルの内容の表示	A-7
tar ファイルの抽出	A-7
ファイルの内容の表示	A-8
コンフィギュレーション ファイルの操作	A-8
コンフィギュレーション ファイルの作成および使用上の注意事項	A-9
コンフィギュレーション ファイルのタイプおよび場所	A-10
テキスト エディタによるコンフィギュレーション ファイルの作成	A-10
TFTP によるコンフィギュレーション ファイルのコピー	A-11
TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	A-11
TFTP によるコンフィギュレーション ファイルのダウンロード	A-11
TFTP によるコンフィギュレーション ファイルのアップロード	A-12
FTP によるコンフィギュレーション ファイルのコピー	A-13
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	A-13
FTP によるコンフィギュレーション ファイルのダウンロード	A-14
FTP によるコンフィギュレーション ファイルのアップロード	A-15

RCPによるコンフィギュレーション ファイルのコピー	A-16
RCPによるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	A-16
RCPによるコンフィギュレーション ファイルのダウンロード	A-17
RCPによるコンフィギュレーション ファイルのアップロード	A-18
設定情報の消去	A-19
スタートアップ コンフィギュレーション ファイルの消去	A-19
格納されたコンフィギュレーション ファイルの削除	A-19
コンフィギュレーションの交換またはロールバック	A-19
コンフィギュレーションの交換およびロールバックの概要	A-20
設定時の注意事項	A-21
コンフィギュレーション アーカイブの設定	A-21
コンフィギュレーション交換またはロールバック動作の実行	A-22
ソフトウェア イメージの操作	A-23
スイッチ上のイメージの場所	A-24
サーバまたは Cisco.com 上のイメージの tar ファイル形式	A-24
TFTPによるイメージ ファイルのコピー	A-25
TFTPによるイメージ ファイルのダウンロードまたはアップロードの準備	A-25
TFTPによるイメージ ファイルのダウンロード	A-26
TFTPによるイメージ ファイルのアップロード	A-28
FTPによるイメージ ファイルのコピー	A-28
FTPによるイメージ ファイルのダウンロードまたはアップロードの準備	A-29
FTPによるイメージ ファイルのダウンロード	A-30
FTPによるイメージ ファイルのアップロード	A-32
RCPによるイメージ ファイルのコピー	A-32
RCPによるイメージ ファイルのダウンロードまたはアップロードの準備	A-33
RCPによるイメージ ファイルのダウンロード	A-34
RCPによるイメージ ファイルのアップロード	A-36

APPENDIX B

Cisco IOS Release 15.0(1)SE でサポートされていないコマンド B-1

アクセス コントロール リスト	B-2
サポートされていない特権 EXEC コマンド	B-2
サポートされていないグローバル コンフィギュレーション コマンド	B-2
サポートされていないルートマップ コンフィギュレーション コマンド	B-2
アーカイブ コマンド	B-2
サポートされていない特権 EXEC コマンド	B-2
ARP コマンド	B-3
サポートされていないグローバル コンフィギュレーション コマンド	B-3
サポートされていないインターフェイス コンフィギュレーション コマンド	B-3

ブートローダ コマンド	B-3
サポートされていないグローバル コンフィギュレーション コマンド	B-3
組み込まれている Event Manager	B-3
サポートされていない特権 EXEC コマンド	B-3
サポートされていないグローバル コンフィギュレーション コマンド	B-3
サポートされていないアプレット コンフィギュレーション モードのコマンド	B-4
Embedded Syslog Manager	B-4
サポートされていないグローバル コンフィギュレーション コマンド	B-4
サポートされていない特権 EXEC コマンド	B-4
debug コマンド	B-4
サポートされていない特権 EXEC コマンド	B-4
フォールバック ブリッジング	B-4
サポートされていない特権 EXEC コマンド	B-4
サポートされていないグローバル コンフィギュレーション コマンド	B-5
サポートされていないインターフェイス コンフィギュレーション コマンド	B-5
ハイ アベイラビリティ	B-6
サポートされていない SSO 認識 HSRP コマンド	B-6
HSRP	B-6
サポートされていないグローバル コンフィギュレーション コマンド	B-6
サポートされていないインターフェイス コンフィギュレーション コマンド	B-6
IGMP スヌーピング コマンド	B-7
サポートされていないグローバル コンフィギュレーション コマンド	B-7
インターフェイス コマンド	B-7
サポートされていない特権 EXEC コマンド	B-7
サポートされていないグローバル コンフィギュレーション コマンド	B-7
サポートされていないインターフェイス コンフィギュレーション コマンド	B-7
IP マルチキャスト ルーティング	B-7
サポートされていない特権 EXEC コマンド	B-7
サポートされていないグローバル コンフィギュレーション コマンド	B-8
サポートされていないインターフェイス コンフィギュレーション コマンド	B-8
IP SLA	B-8
サポートされていない MPLS ヘルス モニタ コマンド	B-8
サポートされていないイーサネット ゲートキーパー登録コマンド	B-9
サポートされていない VoIP コール セットアップ プロブ コマンド	B-9
IP ユニキャスト ルーティング	B-9
サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド	B-9
サポートされていないグローバル コンフィギュレーション コマンド	B-9
サポートされていないインターフェイス コンフィギュレーション コマンド	B-10

- サポートされていない BGP ルータ コンフィギュレーション コマンド B-10
- サポートされていない VPN コンフィギュレーション コマンド B-10
- サポートされていないルート マップ コマンド B-10
- IPv6 B-11
 - IPv4/v6 トンネリング コマンド B-11
- レイヤ 3 B-11
 - BGP B-11
 - その他のサポートされていない BGP コマンド B-12
 - OSPF B-13
 - VRF 認識 AAA B-13
- MAC アドレス コマンド B-13
 - サポートされていない特権 EXEC コマンド B-13
 - サポートされていないグローバル コンフィギュレーション コマンド B-13
- Miscellaneous B-14
 - サポートされていないユーザ EXEC コマンド B-14
 - サポートされていない特権 EXEC コマンド B-14
 - サポートされていないグローバル コンフィギュレーション コマンド B-14
- MSDP B-14
 - サポートされていない特権 EXEC コマンド B-14
 - サポートされていないグローバル コンフィギュレーション コマンド B-15
- マルチキャスト B-15
 - サポートされていない BiDirectional PIM (bidir-PIM; 双方向 PIM) コマンド B-15
 - サポートされていないマルチキャストルーティング マネージャ コマンド B-15
 - サポートされていない IP マルチキャスト レート制限コマンド B-15
 - サポートされていない UDLR コマンド B-15
 - サポートされていない GRE でのマルチキャスト コマンド B-15
- NetFlow コマンド B-15
 - サポートされていないグローバル コンフィギュレーション コマンド B-15
- NAT コマンド B-16
 - サポートされていない特権 EXEC コマンド B-16
- QoS B-16
 - サポートされていないグローバル コンフィギュレーション コマンド B-16
 - サポートされていないインターフェイス コンフィギュレーション コマンド B-16
 - サポートされていないポリシーマップ コンフィギュレーション コマンド B-16
- RADIUS B-16
 - サポートされていないグローバル コンフィギュレーション コマンド B-16
- SNMP B-17
 - サポートされていないグローバル コンフィギュレーション コマンド B-17

SNMPv3 B-17

サポートされていない 3DES 暗号化コマンド B-17

スパニングツリー B-17

サポートされていないグローバル コンフィギュレーション コマンド B-17

サポートされていないインターフェイス コンフィギュレーション コマンド B-17

VLAN B-17

サポートされていないグローバル コンフィギュレーション コマンド B-17

サポートされていないユーザ EXEC コマンド B-17

サポートされていない VLAN データベース コマンド B-18

VTP B-18

サポートされていない特権 EXEC コマンド B-18

INDEX



はじめに

対象読者

このマニュアルは、IE 3000 スイッチを管理するネットワーキング専門家を対象としています。Cisco IOS ソフトウェアの使用経験があり、イーサネットおよび LAN の概念や専門用語を十分理解していることが前提です。

目的

このマニュアルでは、スイッチ上で Cisco IOS ソフトウェア機能を設定するために必要な情報について説明します。このマニュアルでは、スイッチで使用するために作成または変更されたコマンドの使用手順を扱っています。これらのコマンドの詳細は扱いません。これらのコマンドの詳細については、このリリースの『*IE 3000 Switch Command Reference*』を参照してください。Cisco IOS Release 12.2 の標準コマンドについては、Cisco.com ([Documentation] > [Cisco IOS Software]) にアクセスし、Cisco IOS のマニュアルセットを参照してください。

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

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

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

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

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

- 任意で選択する要素の中で、必ずどれか1つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って (`{|}`) 示しています。

対話形式の例では、次の表記法を使用しています。

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

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



(注)

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



注意

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

関連資料

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

http://www.cisco.com/en/US/products/ps11245/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps9703/tsd_products_support_series_home.html



(注)

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

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

スイッチに関するその他の情報については、次の資料を参照してください。

- 『*Release Notes for the Cisco IE 3000 Switch*』
- 『*Cisco IE 3000 スイッチ ソフトウェア コンフィギュレーション ガイド*』
- 『*Cisco IE 3000 Switch Command Reference*』
- 『*Cisco IE 3000 Switch System Message Guide*』
- デバイス マネージャのオンライン ヘルプ（スイッチで利用可能）
- 『*Cisco IE 3000 Switch Hardware Installation Guide*』
- 『*Cisco IE 3000 Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch*』

- 『Cisco Small Form-Factor Pluggable Modules Installation Notes』
- Network Admission Control (NAC) の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- これらの互換性マトリクス ドキュメントは、Cisco.com の次のページで入手可能です。

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

– 『Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix』

マニュアルの入手方法およびテクニカル サポート

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

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

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



CHAPTER 1

概要

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

- 「機能」 (P.1-1)
- 「スイッチ初期設定後のデフォルト値」 (P.1-15)
- 「ネットワークの構成例」 (P.1-18)
- 「次の作業」 (P.1-26)

このマニュアルでは、IP Version 6 (IPv6) に関して特に記載がない限り、IP は IP Version 4 (IPv4) を指します。

機能

スイッチには、アクセス コントロール リスト (ACL) や Quality of Service (QoS) などの基本的なレイヤ 2 インテリジェント機能をサポートする LAN ベース イメージが搭載されています。

- IP サービス イメージには、すべてのレイヤ 2+ 機能と、すべてのレイヤ 3 ルーティング (IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、フォールバック ブリッジング) が含まれています。



(注) IP サービス イメージをダウンロードして、レイヤ 3 機能を使用する場合は、ルーティング Switch Database Management (SDM) テンプレートを使用する必要があります。**show sdm prefer** コマンドを入力すると、現在アクティブなテンプレートを表示できます。また、必要に応じて **sdm prefer routing** グローバル コンフィギュレーション コマンドを入力すると、SDM テンプレートをルーティング テンプレートに変更できます。スイッチをリロードして新しいテンプレートをアクティブにするよう求めるプロンプトが表示されます。

この章で取り上げる一部の機能は、ソフトウェアの暗号化 (暗号化をサポートする) バージョンだけに対応しています。この機能を使用し、Cisco.com からソフトウェアの暗号化バージョンをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

- 「使用および導入を簡素化する機能」 (P.1-2)
- 「パフォーマンス向上機能」 (P.1-2)
- 「管理オプション」 (P.1-4)
- 「管理の簡易性に関する機能」 (P.1-4)
- 「アベイラビリティおよび冗長性に関する機能」 (P.1-7)

- 「VLAN 機能」 (P.1-8)
- 「セキュリティ機能」 (P.1-8)
- 「QoS および CoS 機能」 (P.1-12)
- 「レイヤ 3 機能」 (P.1-13) (IP サービス イメージが必要な機能を含む)
- 「モニタ機能」 (P.1-14)

使用および導入を簡素化する機能

- Express Setup : 基本的な IP 情報、コンタクト情報、スイッチおよび Telnet のパスワード、および Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) に関する情報を使用し、ブラウザ ベースのプログラムを通じて、スイッチの初回設定を迅速に行うことができます。Express Setup の詳細については、スタートアップ ガイドを参照してください。
- ユーザ定義およびデフォルト設定の SmartPort マクロ : ネットワークへの配置を簡単にするためにカスタム スイッチ設定を作成します。
- 着脱式のコンパクト フラッシュ カードに、Cisco IOS ソフトウェア イメージと、スイッチのコンフィギュレーション ファイルが格納されています。ソフトウェア機能を再設定せずに、スイッチの交換やアップグレードを実行できます。更新版のブートローダに含まれるセカンダリ ブートローダ イメージがサポートするコンパクト フラッシュ ファイル システム ドライバにより、コンパクト フラッシュ メモリ カードにアクセスできます。スイッチのブートローダにはプライマリ ブートローダとセカンダリ ブートローダが含まれ、どちらもブート フラッシュに格納されています。
- 組み込みのデバイス マネージャ GUI : 単体のスイッチを Web ブラウザから設定、管理します。デバイス マネージャの起動については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- スイッチのクラスタ化テクノロジーの機能概要
 - イーサネット、ファストイーサネット、Fast EtherChannel、Small Form-Factor Pluggable モジュール、ギガビットイーサネット、Gigabit EtherChannel 接続を含めて、地理的な近接にも相互接続メディアにも関係なく、複数のクラスタ対応スイッチの設定、モニタ、認証、およびソフトウェア アップグレードをまとめて実行できます。クラスタ対応スイッチのリストについては、リリース ノートを参照してください。
 - 候補スイッチの自動検出と、最大 16 台のスイッチからなるクラスタの作成機能。1 つの IP アドレスを使用してクラスタを管理できます。
 - 拡張検出機能により、コマンド スイッチに直接接続されていないクラスタ候補を検出できます。
- Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。シスコと直接サービス契約を結んでいるお客様は、Call Home デバイスを TAC へのサービス要求を自動で生成する Cisco Smart Call Home サービスに登録できます。

パフォーマンス向上機能

- Cisco EnergyWise は、Power over Ethernet (PoE) エンティティのエネルギー使用量を管理します。
詳細については、Cisco.com の『Cisco EnergyWise Version 2 Configuration Guide』を参照してください。
- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。

- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Auto MDIX 機能により、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定。
- ルーテッド フレームの場合は最大 1546 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート。
- すべてのポートにおける IEEE 802.3x フロー制御（スイッチはポーズ フレームを送信しません）
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（Fast EtherChannel）全二重の帯域幅を確保
- ポート集約プロトコル（PAgP）および Link Aggregation Control Protocol（LACP）により、EtherChannel リンクを自動的に作成
- ポート単位のストーム制御。ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止します。
- レイヤ 2 の不明なユニキャスト、マルチキャスト、およびブリッジドブロードキャスト トラフィック転送に対するポート ブロッキング
- Cisco Group Management Protocol（CGMP）サーバのサポートおよび Internet Group Management Protocol（IGMP）バージョン 1、バージョン 2、およびバージョン 3 対応の IGMP スヌーピング。
 - （CGMP デバイスの場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減
 - （IGMP デバイスの場合）IGMP スヌーピングによってマルチメディア トラフィックとマルチキャスト トラフィックを転送。
- IGMP レポート抑制。1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します（IGMPv1 または IGMPv2 クエリーだけをサポート）。
- IGMP スヌーピング クエリー サポート。IGMP 一般クエリー メッセージを定期的に生成するようにスイッチを設定します。
- IGMP ヘルパーにより、スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャスト ストリームを加入させることが可能。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）により、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信しながら、帯域幅およびセキュリティ上の理由から、加入者 VLAN からストリームを分離します。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループ セットを管理します。
- IGMP スロットリング。IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定します。
- ネットワーク終了の待ち時間を設定できる IGMP の Leave タイマー
- Switch Database Management（SDM）テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。
- Web Cache Communication Protocol（WCCP）。トラフィックのローカル広域アプリケーション エンジンへのリダイレクト、コンテンツ要求のローカルでの対処、およびネットワーク内の Web トラフィック パターンのローカライズ（IP サービス イメージが必要）を行います。
- Cisco IOS ソフトウェアの一部である Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）により、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます。

- 設定可能なスモールフレーム着信しきい値により、スモール フレーム (64 バイト以下) が指定されたレート (しきい値) でインターフェイスに着信した場合のストーム制御を防止します。
- Flex Link に障害が発生したあとのマルチキャスト トラフィックのコンバージェンス時間を短縮するための Flex Link マルチキャスト高速コンバージェンス。
- サーバ グループに均等にアクセスおよび認証要求を分散できるようにするための RADIUS サーバ ロード バランシング。
- CPU 生成トラフィックの QoS マーキングのサポートと、出力ネットワーク ポートへの CPU 生成トラフィックのキュー。

管理オプション

- 組み込みデバイス マネージャ : GUI のデバイス マネージャがソフトウェア イメージに組み込まれています。このデバイス マネージャは、単体のスイッチの設定、管理に使用します。デバイス マネージャの起動については、スタートアップ ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant : Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に使用します。Network Assistant の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。
- CLI : Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、管理ステーションをスイッチ コンソール ポートに直接接続するか、リモート管理ステーションから Telnet を利用します。CLI の詳細については、第 2 章「コマンドライン インターフェイスの使用法」を参照してください。
- SNMP : CiscoWorks 2000 LAN Management Suite (LMS) および HP OpenView などの SNMP 管理アプリケーション。HP OpenView、SunNet Manager などのプラットフォームが稼働している SNMP 対応管理ステーションから管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring (RMON) グループをサポートします。SNMP の詳しい使用方法については、第 36 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine (旧称 Cisco IOS CNS エージェント) : コンフィギュレーション サービスは、ネットワーク デバイスおよびサービスの導入と管理を自動化します。スイッチごとに設定変更の内容を生成してスイッチに送信し、その設定変更を適用した後、その結果を記録することで初期設定および設定の更新を自動化できます。
CNS の詳細については、第 5 章「Cisco IOS Configuration Engine の設定」を参照してください。
- CIP : Common Industrial Protocol (CIP) はピアツーピアのアプリケーション プロトコルであり、スイッチと工業用装置 (I/O コントローラ、センサー、リレーなど) 間でアプリケーション レベルの接続を実現します。CIP ベースの管理ツール (RSLogix など) を使用してスイッチを管理できます。スイッチでサポートされる CIP コマンドの詳細については、コマンド リファレンスを参照してください。
- Common Industrial Protocol (CIP) の機能拡張により、CIP で DHCP パラメータを設定できるようになりました。

管理の簡易性に関する機能

- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。

- Dynamic Host Configuration Protocol (DHCP) によるスイッチ情報 (IP アドレス、デフォルトゲートウェイ、ホスト名、Domain Name System (DNS; ドメイン ネーム システム)、TFTP サーバ名) の自動設定。
- DHCP リレーによる DHCP クライアントからの UDP ブロードキャストの転送 (IP アドレス要求を含む)。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 新しいイメージの指定された設定を多数のスイッチにダウンロードするために、DHCP ベースの自動設定およびイメージをアップデート。
- 新しいバルク リース クエリー タイプ (RFC5460 で定義) をサポートする DHCPv6 バルクリース クエリー。
- DHCPv6 リレー エージェントの送信元アドレスを設定する DHCPv6 リレー送信元設定機能。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送。
- Address Resolution Protocol (ARP; アドレス解決プロトコル)。IP アドレスおよび対応する MAC アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットをドロップするユニキャスト MAC アドレス フィルタリング。
- 設定可能な MAC アドレス スケーリング。これにより、VLAN で MAC アドレス ラーニングをディセーブルにし、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol (CDP) バージョン 1 および 2。ネットワーク トポロジを検出し、ネットワーク上のスイッチと他のシスコ デバイスとのマッピングを行います。
- リンク層検出プロトコル (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED) によるサードパーティ製 IP 電話との相互運用性の確保。
- スイッチからエンドポイント デバイスへロケーション情報を提供する LLDP メディア拡張 (LLDP-MED) ロケーション TLV。
- ネットワーク タイム プロトコル (NTP) により、外部ソースから全スイッチに一貫したタイムスタンプを提供します。
- IPv4 と IPv6 の両方をサポートし、NTPv3 と互換性のある Network Time Protocol version 4 (NTPv4)。
- IEEE 1588 標準で定められた Precision Time Protocol (PTP; 高精度時間プロトコル) により、ネットワーク内の装置のリアルタイム クロックをナノ秒精度で同期できます。
 - 拡張モジュール ポートの PTP メッセージをサポートする PTP 拡張機能。
- Cisco IOS File System (IFS)。スイッチが使用するすべてのファイル システムに対して単一インターフェイスを提供します。
- マルチキャスト アプリケーションに対する Source Specific Multicast (SSM) マッピング。グループへ送信元をマッピングしてリスナーをマルチキャスト ソースへ動的に接続させ、アプリケーションの依存性を軽減します。
- IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズするための Enhanced Interior Gateway Routing Protocol (EIGRP) v6 のサポート

- IP サービス (HSRP、ARP、SNMP、IP SLA、TFTP、FTP、Syslog、traceroute、ping) をサポート。これらのサービスを VRF 認識にすることで、複数のルーティング インスタンスで動作させます。
- スイッチの設定変更を記録して表示させるコンフィギュレーション ロギング。
- 一意のデバイス ID。 **show inventory** ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Communicator または Microsoft Internet Explorer ブラウザセッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベースセッションを実行できます。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの同時暗号化 Secure Shell (SSH; セキュア シェル) 接続の確立によって帯域内管理アクセス。
- SNMP のバージョン 1、バージョン 2c、およびバージョン 3 の get および set 要求による帯域内管理アクセス。
- 帯域外管理アクセス。スイッチのコンソール ポートに端末を直接接続するか、またはシリアル接続とモデム経由でリモート端末に接続します。
- Secure Copy Protocol (SCP) 機能により、セキュアかつ認証済みの方法でスイッチ設定またはスイッチ イメージ ファイルをコピーできます (暗号化バージョンのソフトウェアが必要)。
- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼働している設定を交換します。
- Cisco IOS サポートの HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバに要求を送信することができます。また、Cisco IOS の HTTP サーバは、IPv4 と IPv6 の両方の HTTP クライアントから、HTTP 要求にサービスを提供することができます。
- Simple Network and Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを送信し、IPv6 を実行しているデバイスから SNMP 通知を受信できるようにすることができます。
- ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理するための IPv6 ステートレス自動設定。
- VLAN の MAC アドレス ラーニングをディセーブルにします。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにしたアドレス割り当て。
- 有線ロケーション サービスは、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine (MSE) に送信します。
- CPU 使用率しきい値トラップによる CPU 使用率の監視。
- VLAN、サービス クラス (CoS)、DiffServ コード ポイント (DSCP)、およびタグ付けモードを指定して音声と音声シグナリングのプロファイルを作成する LLDP-MED ネットワークポリシー Time、Length、Value (TLV; 時間、長さ、時間)。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名の入力をサポート。これにより、DHCP プロトコルを使用して同一のコンフィギュレーション ファイルを複数送信できます。
- DHCP スヌーピング拡張機能。これにより、Option 82 DHCP フィールドで指定する回線 ID サブオプションに、固定文字列ベースのフォーマットを選択できるようになります。
- PROFINET IO (分散型オートメーションアプリケーション用のモジュラ通信フレームワーク) をサポートします。スイッチから IO コントローラへの PROFINET 管理接続が可能です。
- Cisco EnergyWise により、power over Ethernet (PoE) デバイスなどの EnergyWise エンティティ およびデーモンが動作するエンド ポイントの電力消費量を管理します。

アベイラビリティおよび冗長性に関する機能

- HSRP により、コマンド スイッチおよびレイヤ 3 ルータの冗長構成が可能です (IP サービス イメージが必要)
- 拡張オブジェクト追跡により、HSRP から追跡メカニズムが分離され、HSRP 以外のプロセスで使用できる個別のスタンダロン追跡プロセスが作成されます (IP サービス イメージが必要)。
- Unidirectional Link Detection (UDLD; 単一方向リンク検出) およびアグレッシブ UDLD。光ファイバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向リンクを検出し、ディセーブルにします。
- IEEE 802.1D Spanning-Tree Protocol (STP; スパニングツリー プロトコル) による冗長バックボーン接続およびループフリー ネットワーク。STP には次の機能があります。
 - 最大 128 のスパニングツリー インスタンスをサポート。
 - Per-VLAN Spanning-Tree Plus (PVST+) による VLAN 間でのロード バランシング。
 - Rapid PVST+ による、VLAN 間でのロード バランシングおよびスパニングツリー インスタンスの高速コンバージェンスの実現。
- IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) により、VLAN をスパニングツリー インスタンスに分類、またデータ トラフィックおよびロード バランシング用に複数の転送パスを確保します。また、IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) に基づいた Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) により、ルートと指定ポートをただちにフォワーディング ステートに変更することで、スパニングツリーの高速コンバージェンスが実現されます。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニングツリーのオプション機能は次のとおりです。
 - PortFast。ポートをブロッキング ステートからフォワーディング ステートへただちに變更させることによって、転送遅延を防ぎます。
 - BPDU ガード。Bridge Protocol Data Unit (BPDU; ブリッジプロトコル データ ユニット) を受信する PortFast 対応ポートをシャットダウンします。
 - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
 - ルート ガード。ネットワーク コア外のスイッチがスパニングツリー ルートになることを防ぎます。
 - ループ ガード。代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。
- 等コスト ルーティングにより、リンクレベルおよびスイッチレベルの冗長性を実現します (IP サービス イメージが必要)。
- Flex Link レイヤ 2 インターフェイス。基本リンク冗長の STP に代わるものとして、互いにバックアップします。
- リンクステート トラッキング。接続されたホストとサーバからのアップストリーム トラフィックを伝送するポートの状態をミラーリングします。また、別のシスコ製イーサネット スイッチで動作するリンクへサーバ トラフィックをフェールオーバーすることができます。
- 短い Resilient Ethernet Protocol (REP) hello : REP Link Status Layer (LSL; リンク ステータス レイヤ) のエイジング タイマーの範囲を 3000 ~ 10000 ms (500 ms 間隔) から 120 ~ 10000 ms (40 ms 間隔) に変更します。

VLAN 機能

- 最大 1005 の VLAN をサポート。適切なネットワーク リソース、トラフィック パターン、および帯域幅を対応付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 規格で認められている 1 ~ 4094 の範囲で VLAN ID をサポート。
- ダイナミック VLAN メンバーシップに対応する VLAN Query Protocol (VQP)。
- すべてのポート上で稼働する IEEE 802.1Q トランキング カプセル化。ネットワークの移動、追加、変更や、ブロードキャストおよびマルチキャスト トラフィックの管理および制御、さらに、ハイセキュリティ ユーザおよびネットワーク リソース別の VLAN グループの確立によるネットワークセキュリティを実現します。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)。2 台のデバイス間のリンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタイプ (IEEE 802.1Q) もネゴシエートします。
- VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) および VTP プルーニング。トラフィックのフラディングをそのトラフィックを受信するステーションへのリンクだけに制限することによって、ネットワーク トラフィックを削減します。
- 音声 VLAN。Cisco IP Phone から音声トラフィック用のサブネットを作成します。
- VLAN 1 の最小化 : VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニングツリー ループまたはストームのリスクを軽減。この機能をイネーブルに設定すると、トランク上でユーザ トラフィックは送受信されません。スイッチの CPU は、引き続き制御プロトコル フレームの送受信を行います。
- プライベート VLAN により、VLAN のスケーラビリティ問題に対処し、制御性の高い IP アドレス 割り当てを実現し、スイッチ上の他のポートからレイヤ 2 ポートを分離することができます (IP サービス イメージが必要)。
- ポートで学習する MAC アドレス数を制限する、またはポートで学習する MAC アドレスを定義する、PVLAN ホストでのポートセキュリティ。
- VLAN Flex Link ロード バランシング : Spanning Tree Protocol (STP; スパニングツリー プロトコル) を必要としないレイヤ 2 冗長性を提供。プライマリおよびバックアップ リンクとして設定したインターフェイスのペアを使用して、VLAN ベースによるトラフィックのロード バランシングが可能です。
- 制限付き VLAN (認証失敗 VLAN と呼ばれる) による 802.1X 認証のサポート。
- VTP バージョン 3 のサポート。具体的には、任意の VTP モードによる拡張範囲 VLAN (VLAN 1006 ~ 4094) 設定のサポート、認証の拡張機能 (非表示パスワードまたはシークレット パスワード)、VTP に加えて他のデータベースの伝播、VTP プライマリ サーバおよびセカンダリ サーバ、VTP のポートによるオン/オフの切り替えオプションがあります。

セキュリティ機能

- IP サービス レベル契約 (IP SLA) のサポートにより、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます (IP サービス イメージが必要)。
- IP SLA EOT により、スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッタ、パケット損失などのアクションによってトリガーされる IP SLA 追跡動作からの出力を使用できます (IP サービス イメージが必要)。
- Web 認証。IEEE 802.1x 機能をサポートしないサブリカント (クライアント) に Web ブラウザを使用して認証可能になります。

- ローカル Web 認証バナー。これにより、カスタム バナー、またはイメージファイルを Web 認証ログイン画面に表示することができます。
- MAC authentication bypass (MAB; MAC 認証バイパス) エージング タイマー。MAB を使用して認証した後に認証された非アクティブのホストを検出します。
- 管理インターフェイス (デバイス マネージャ、Network Assistant、CLI) へのパスワード保護付きアクセス (読み取り専用および読み書きアクセス)。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポートセキュリティ オプション。
- VLAN 認識ポート セキュリティ オプション。違反の発生時にポート全体をシャットダウンするのではなく、そのポート上の VLAN をシャットダウンします。
- ポート セキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP ACL。ルーテッド インターフェイス (ルータ ACL) と VLAN の双方向およびレイヤ 2 インターフェイス (ポート ACL) の受信方向に関するセキュリティ ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- VLAN ACL (VLAN マップ) により、MAC、IP、および TCP/UDP ヘッダー内の情報に基づいてトラフィックをフィルタリングすることで、VLAN 内のセキュリティを実現できます (IP サービス イメージが必要)。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- IPv6 ACL をインターフェイスに適用して、IPv6 トラフィックをフィルタリングできます (IP サービス イメージが必要)。
- untrusted (信頼性のない) ホストと DHCP サーバの間の untrusted DHCP メッセージをフィルタリングする DHCP スヌーピング。
- DHCP スヌーピング データベース、および IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド インターフェイスでのトラフィックを制限する IP ソース ガード。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のある攻撃を回避するためのダイナミック ARP インスペクション。
- IEEE 802.1Q トンネリングにより、サービス プロバイダー ネットワークを介したリモートサイトのユーザがいるカスタマーが、VLAN を他のカスタマーから分離することができます。また、レイヤ 2 プロトコル トンネリングにより、カスタマーのネットワークで全ユーザに関する完全な STP、CDP、および VTP 情報を取得することができます (IP サービス イメージが必要)。
- レイヤ 2 ポイントツーポイント トンネリングにより、EtherChannels を自動的に作成できます (IP サービス イメージが必要)。

- レイヤ 2 プロトコル トネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベース認証。不正なデバイス (クライアント) によるネットワーク アクセスを防止します。次の機能がサポートされています。
 - データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにする Multidomain Authentication (MDA; マルチドメイン認証)。
 - MDA のダイナミック音声 VLAN (仮想 LAN)。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
 - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
 - ポートセキュリティ。802.1x ポートへのアクセスを制御します。
 - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
 - IP Phone 検出機能拡張。Cisco IP Phone を検出し識別します。
 - ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
 - 制限付き VLAN。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャルを持っていないユーザに制限付きのサービスを提供します。
 - 802.1x アカウンティング。ネットワーク使用をトラッキングします。
 - 802.1x と LAN の Wake-on-LAN (WoL) 機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
 - 802.1x 準備状態チェック。スイッチで IEEE 802.1x を設定する前に、接続されたエンドホストの準備状態を判断します。
 - セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。
 - MAC 認証バイパス。クライアント MAC アドレスに基づいてクライアントを許可します。
 - 802.1X スイッチ サブリカントを持つ Network Edge Access Topology (NEAT)、CISP を使ったホスト認証、および自動イネーブル化。これらにより、別のスイッチへのサブリカントとして、配線クローゼットの外のスイッチが認証されます。
 - 認証される前にネットワークへのアクセスをホストに許可するための、オープン アクセスを使用した IEEE 802.1x。
 - ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを使用できるようになります。
 - 新しいホストを認証するときに、ポートが思考する認証メソッドの順序を設定するための柔軟な認証シーケンス。
 - マルチユーザ認証。複数のホストが、802.1x 対応ポートを認証できるようになります。
- Network Admission Control (NAC) 機能 :
 - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャに関する NAC レイヤ 2 802.1x 検証
NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「[NAC レイヤ 2 802.1x 検証の設定](#)」(P.12-57) を参照してください。
 - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムまたはクライアントのポスチャに関する NAC レイヤ 2 IP 検証

NAC レイヤ 2 IP 検証の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

– IEEE 802.1x アクセス不能認証バイパス

この機能の設定については、「[アクセス不能認証バイパス機能の設定](#)」(P.12-52)を参照してください。

– Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) ダウンポリシー。ポスチャ検証が発生したときに、AAA サーバが利用できない場合のホストの NAC レイヤ 2 IP 検証

この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

- Terminal Access Controller Access Control System Plus (TACACS+)。TACACS サーバを介してネットワークセキュリティを管理する独自の機能です。
- RADIUS により、AAA サービスを通じてリモート ユーザの ID の確認、アクセス権の付与、アクションの追跡を実行できます。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- Kerberos セキュリティ システム。信頼できるサードパーティを使用して、ネットワーク リソースに対する要求を認証します (ソフトウェアの暗号化バージョンが必要)。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer (SSL) バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります (ソフトウェアの暗号化バージョンが必要)。
- 音声認識 IEEE 802.1X および MAB セキュリティ違反。セキュリティ違反が発生すると、ポートのデータ VLAN だけがシャットダウンされます。
- スタティック ホストでの IP ソース ガードのサポート。
- RADIUS Change of Authorization (CoA; 認証の変更)。特定のセッションが認証された後で、その属性を変更します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は AAA サーバから、Cisco Secure ACS などの RADIUS CoA パケットを送信し、新しいポリシーに適用することができます。
- IEEE 802.1x ユーザ ディストリビューション。さまざまな VLAN にわたってユーザをロード バランシングすることにより、(ユーザ グループに対して) 複数の VLAN を使った配置で、ネットワークのスケラビリティを向上させることができます。認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- マルチ ホスト認証を使った、重要な VLAN のサポート。これにより、ポートがマルチ認証用に設定され、AAA サーバが到達不能になった場合でも、重要なリソースへのアクセスができるように、このポートが重要な VLAN に配置されます。
- カスタマイズ可能な Web 認証機能強化。ローカル Web 認証で、ユーザ定義の *login*、*success*、*failure*、および *expire Web* ページの作成ができるようになります。
- ポート ホスト モードを変更し、オーセンティケータのスイッチ ポートに標準ポート設定を適用するために Network Edge Access Topology (NEAT) をサポート。
- VLAN-ID ベースの MAC 認証。ユーザ認証のために VLAN と MAC のアドレス情報を結合して、許可されていない VLAN からのネットワーク アクセスを阻止します。
- MAC Move。モビリティのイネーブル化を制約することなく、ホスト (IP 電話の背後で接続されたホストを含む) が同じスイッチ内のポート間を移動できるようになります。MAC Move では、もう 1 つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。

- Simple Network Management Protocol バージョン 3 (SNMPv3; 簡易ネットワーク管理プロトコルバージョン 3) を使った 3DES および AES のサポート。このリリースでは、168 ビット Triple Data Encryption Standard (3DES) と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard (AES; 高度暗号化規格) 暗号化アルゴリズムに対するサポートが追加されます。

QoS および CoS 機能

- auto-QoS (自動 QoS)。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。
- ポートベースの信頼の自動 Quality of Service (QoS) VoIP 拡張と DSCP および出力トラフィックのプライオリティ キューイング
- 分類
 - IP Type of Service/Differentiated Services Code Point (IP ToS/DSCP) および IEEE 802.1p CoS のポート単位でのプライオリティ設定。ミッションクリティカルなアプリケーションのパフォーマンスを保護します。
 - IP ToS/DSCP および IEEE 802.1p CoS (サービス クラス) のフローベースの packets 分類 (MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく) によるマーキング。ネットワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化されたサービス レベルを可能にするとともに、ネットワーク上のミッションクリティカルなトラフィックにプライオリティを設定します。
 - QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted (信頼性のある) ポート ステート (CoS、DSCP、および IP precedence)。
 - 信頼境界機能。Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを確保します。
- ポリシング
 - 特定のトラフィック フローに対してどの程度のポート帯域幅を割り当てるかを管理する、スイッチ ポート上のトラフィック ポリシング ポリシー。
 - 階層型のポリシーマップで複数のクラスマップを作成する場合、各クラスマップを自身のポート レベル (第 2 レベル) ポリシーマップと関連付けることができます。第 2 レベルのポリシーマップは、それぞれ異なるポリサーを保有できます。
 - トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーションまたはトラフィック フローをあらかじめ定義された特定のレートに制限します。
- 不適合
 - 帯域幅の使用制限を超過したパケットの不適合マークダウン。
- 入力キューイングおよびスケジューリング
 - ユーザ トラフィック用に設定可能な 2 つの入力キュー (一方のキューをプライオリティ キューにできます)。
 - 輻輳回避メカニズムとしての Weighted Tail Drop (WTD)。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
 - シェイプド ラウンドロビン (SRR) : パケットがキューからリングへ送出される際のレートを決定するスケジューリング サービス (入力キューでサポートされる唯一のモードはシェアリング)。
- 出力キューおよびスケジューリング

- 1 ポートに 4 つの出力キュー。
- 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
- スケジューリング サービスとしての SRR。キューからパケットを出して出力インターフェイスに入れる速度を指定します（出力キューではシェーピングおよび共有がサポートされます）。シェーピング型出力キューは、ポート帯域幅の割り当てが保証されますが、割り当てられたポート帯域幅の使用に制限されています。共有型出力キューは、設定された帯域幅の割り当てが保証されるだけでなく、他のキューが空になり、その割り当て分の帯域幅が使用されない場合、保証された割り当てより多く使用できます。

レイヤ 3 機能

次に、レイヤ 3 機能について説明します。



(注)

ここに記載する機能は、IP サービス イメージだけで使用できます。

- レイヤ 3 ルータの冗長性を確保するための HSRP バージョン 1 (HSRPv1) および HSRP バージョン 2 (HSRPv2)
- IP ルーティング プロトコルによるロード バランシングとスケーラブルなルーテッド バックボーン の構築
 - RIP バージョン 1 および 2
 - OSPF
 - Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6。IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズします。
 - HSRP for IPv6
 - Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) バージョン 4。
- OSPFv2 の NSF IETF モード : IPv4 の OSPFv2 グレースフル リスタートのサポート
- OSPFv3 の NSF IETF モード : IPv6 の OSPFv3 グレースフル リスタートのサポート
- 2 つ以上の VLAN 間の完全レイヤ 3 ルーティング対応の IP ルーティング (VLAN 間ルーティング) により、各 VLAN が独自の自律データリンク ドメインのメンテナンスが可能
- ポリシーベース ルーティング (PBR)。トラフィック フローに定義済みポリシーを設定。
- カスタマー エッジ装置内の Multiple VPN Routing/Forwarding (multi-VRF) インスタンスにより、サービス プロバイダーが複数の Virtual Private Networks (VPN; 仮想私設網) をサポートし、VPN 間で IP アドレスが重複できるようにします。
- フォールバック ブリッジングにより、2 つ以上の VLAN 間で非 IP トラフィックを転送できます。
- スタティック IP ルーティングによるネットワーク パス情報のルーティング テーブル手動作成
- 等価コスト ルーティングによるロード バランシングおよび冗長構成
- Internet Control Message Protocol (ICMP) および ICMP Router Discovery Protocol (IRDP) : ルータのアドバタイズおよびルータ請求メッセージによる直接接続サブネット上のルータのアドレス検索

- Protocol-Independent Multicast (PIM) によるネットワーク内マルチキャストルーティング。これにより、ネットワーク内のデバイスは要求されたマルチキャストフィードの受信が可能になり、マルチキャストに参加しないスイッチのプルニングが可能になります。PIM Sparse Mode (PIM-SM; PIM sparse (スパース) モード)、PIM Dense Mode (PIM-DM; PIM dense (デンス) モード)、および PIM sparse-dense モードのサポートが含まれます。
- Multicast Source Discovery Protocol (MSDP) により、複数の PIM-SM ドメインを接続できます。
- Distance Vector Multicast Routing Protocol (DVMRP) トンネリングにより、非マルチキャストネットワークを経由した 2 つのマルチキャスト対応ネットワーク間のインターオペラビリティが実現されます。
- DHCP リレーによる、IP アドレス要求など DHCP クライアントからの UDP ブロードキャストの転送
- IPv6 のリレー、クライアント、サーバアドレス割り当て、プレフィックス委任に対応した DHCP
- 新しいバルク リース クエリータイプ (RFC5460 で定義) をサポートする DHCPv6 バルクリース クエリー
- DHCPv6 リレー エージェントの送信元アドレスを設定する DHCPv6 リレー送信元設定機能
- IPv6 ユニキャストルーティング機能により、設定したインターフェイスを通じて IPv6 トラフィックを転送できます。
- IPv6 Default Router Preference (DRP; デフォルト ルータの初期設定)。ホスト性能を改善することで、適切なルータを選択します。
- Nonstop Forwarding (NSF; ノンストップ フォワーディング) 認識により、プライマリ ルート プロセッサ (RP) に障害が発生したためにバックアップ RP が引き継ぐ場合や、中断のないソフトウェア アップグレードのためにプライマリ RP が手動でリロードされる場合に、レイヤ 3 スイッチが NSF 対応の隣接ルータからパケット転送を継続できるようにします。
- Intermediate System-to-Intermediate System (IS-IS) ルーティングは、Connectionless Network Service (CLNS) ネットワーク用にダイナミック ルーティング プロトコルをサポート
- Virtual Router Redundancy Protocol (VRRPv4; 仮想ルータ冗長プロトコル)。LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当て、マルチアクセス リンク上にある複数台のルータが同じ仮想 IP アドレスを使用できるようにします。

モニタ機能

- EOT および IP SLA EOT スタティック ルートのサポート。事前に設定したスタティック ルートまたは DHCP ルートがダウンした場合に特定します。
- デバイスおよびシステム管理用の Embedded Event Manager (EEM)。主なシステム イベントをモニタし、ポリシーに従って動作します (IP サービス イメージが必要)。
- MAC アドレス通知トラップおよび RADIUS アカウンティング。スイッチが学習または削除した MAC アドレスを保存することによって、ネットワーク上のユーザをトラッキングします。
- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN)。任意のポートまたは VLAN について、トラフィック モニタリングが可能です。
- Intrusion Detection System (IDS; 侵入検知システム) における SPAN および RSPAN のサポート。ネットワーク セキュリティ違反をモニタ、撃退、およびレポートします。
- 組み込み RMON エージェントの 4 つのグループ (履歴、統計、アラーム、およびイベント) を使用して、ネットワークをモニタし、トラフィック解析を行うことができます。
- Syslog 機能。認証または許可エラー、リソースの問題、およびタイムアウト イベントに関するシステム メッセージを記録します。

- レイヤ 2 traceroute。パケットが送信元デバイスから宛先デバイスへ送られる物理パスを識別します。
- Time Domain Reflector (TDR)。10/100 および 10/100/1000 の銅線イーサネット ポートでケーブル接続の問題を診断し、解決します。
- SFP モジュール診断管理インターフェイス。SFP モジュールの物理または動作ステータスをモニタします。
- 温度、電源状態、イーサネット ポートのステータスに関するアラームの処理機能が備わっています。
- 外部のリレー システムに使用できるアラーム リレー接点が備わっています。
- HSRP に対する拡張オブジェクト トラッキング
- Digital Optical Monitoring (DOM; デジタル オプティカル モニタリング)。X2 SFP モジュールのステータスを確認します。

スイッチ初期設定後のデフォルト値

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



(注)

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

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

- デフォルト スイッチ IP アドレス、サブネット マスク、デフォルト ゲートウェイは 0.0.0.0 です。詳細については、第 4 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- ドメイン名はデフォルトで設定されていません。詳細については、第 4 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブルに設定されています (DHCP サーバとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。DHCP リレー エージェントはイネーブルに設定されています (DHCP リレー エージェントとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。詳細については、第 4 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- スイッチ クラスタはディセーブルに設定されています。スイッチ クラスタの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチの管理」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチの管理」を参照してください。
- NTP はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。

- DNS はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。
- TACACS+ はディセーブルに設定されています。詳細については、第 11 章「スイッチ ベース認証の設定」を参照してください。
- RADIUS はディセーブルに設定されています。詳細については、第 11 章「スイッチ ベース認証の設定」を参照してください。
- 標準の HTTP サーバおよび SSL HTTPS サーバは両方ともイネーブルに設定されています。詳細については、第 11 章「スイッチ ベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルに設定されています。詳細については、第 12 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- ポート パラメータ
 - 動作モードはレイヤ 2 (スイッチポート) です。詳細については、第 14 章「インターフェイス特性の設定」を参照してください。
 - インターフェイス速度およびデュプレックス モードが自動ネゴシエーションに設定されています。詳細については、第 14 章「インターフェイス特性の設定」を参照してください。
 - Auto MDIX は、イネーブルです。詳細については、第 14 章「インターフェイス特性の設定」を参照してください。
 - フロー制御はディセーブルに設定されています。詳細については、第 14 章「インターフェイス特性の設定」を参照してください。
- VLAN
 - デフォルト VLAN は VLAN 1 です。詳細については、第 16 章「VLAN の設定」を参照してください。
 - VLAN トランッキング設定は dynamic auto (DTP) です。詳細については、第 16 章「VLAN の設定」を参照してください。
 - トランク カプセル化はネゴシエーションです。詳細については、第 16 章「VLAN の設定」を参照してください。
 - VTP モードはサーバです。詳細については、第 17 章「VTP の設定」を参照してください。
 - VTP バージョンはバージョン 1 です。詳細については、第 17 章「VTP の設定」を参照してください。
 - プライベート VLAN は設定されていません。詳細については、第 19 章「プライベート VLAN の設定」を参照してください。
 - 音声 VLAN はディセーブルに設定されています。詳細については、第 18 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルに設定されています。詳細については、第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
- STP、PVST+ は VLAN 1 でイネーブルに設定されています。詳細については、第 21 章「STP の設定」を参照してください。
- MSTP はディセーブルに設定されています。詳細については、第 22 章「MSTP の設定」を参照してください。
- オプションのスパニングツリー機能はディセーブルに設定されています。詳細については、第 23 章「オプションのスパニングツリー機能の設定」を参照してください。
- Flex Link は設定されていません。詳細については、第 25 章「Flex Link および MAC アドレス テーブル移動更新機能の設定」を参照してください。

- DHCP スヌーピングは、ディセーブルです。DHCP スヌーピング情報オプションはイネーブルに設定されています。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- IP 送信元ガードはディセーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- すべての VLAN 上でダイナミック ARP インスペクションがディセーブルになっています。詳細については、第 27 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルです。IGMP のフィルタは適用されていません。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否されます。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クェリア機能はディセーブルに設定されています。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- ポートベース トラフィック
 - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルに設定されています。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
 - 保護ポートは定義されていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
 - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
 - セキュア ポートは設定されていません。詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。
- CDP はイネーブルに設定されています。詳細については、第 32 章「CDP の設定」を参照してください。
- UDLD はディセーブルです。詳細については、第 33 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細については、第 34 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています (バージョン 1)。詳細については、第 36 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- QoS はディセーブルです。詳細については、第 39 章「QoS の設定」を参照してください。
- EtherChannel は設定されていません。詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

- IP ユニキャスト ルーティングはディセーブルに設定されています。詳細については、[第 41 章「IP ユニキャスト ルーティングの設定」](#)を参照してください。
- IPv6 ユニキャスト ルーティングはディセーブルに設定されています。詳細については、[第 42 章「IPv6 ユニキャスト ルーティングの設定」](#)を参照してください。
- HSRP グループは設定されていません。詳細については、[第 46 章「HSRP および VRRP の設定」](#)を参照してください。
- IP マルチキャスト ルーティングはすべてのインターフェイスでディセーブルに設定されています。詳細については、[第 50 章「IP マルチキャスト ルーティングの設定」](#)を参照してください。
- MSDP はディセーブルに設定されています。詳細については、[第 51 章「MSDP の設定」](#)を参照してください。
- フォールバック ブリッジングは設定されていません。詳細については、[第 52 章「フォールバック ブリッジングの設定」](#)を参照してください。

ネットワークの構成例

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

- 「[スイッチを使用する場合の設計概念](#)」 (P.1-18)
- 「[Ethernet-to-the-Factory アーキテクチャ](#)」 (P.1-20)

スイッチを使用する場合の設計概念

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

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

表 1-1 ネットワーク パフォーマンスの向上

ネットワークに対する需要	推奨する設計方式
1つのネットワーク セグメントに多くのユーザが集中しすぎ、インターネットへアクセスするユーザが増加している	<ul style="list-style-type: none"> 帯域幅を共有するユーザ数が少なくなるように、より小さいネットワーク セグメントを作成します。さらに VLAN および IP サブネットを使用して、ネットワーク リソースに頻繁にアクセスするユーザと同じ論理ネットワーク上に、そのリソースを配置します。 スイッチと接続先ワークステーションとの間で、全二重通信を使用します。
<ul style="list-style-type: none"> 新しい PC、ワークステーション、およびサーバのパワーの増大 ネットワーク アプリケーション（大容量の添付ファイル付き電子メールなど）および帯域幅を多用するアプリケーション（マルチメディアなど）による帯域幅需要の増大 	<ul style="list-style-type: none"> ネットワーク ユーザが等しくアクセスする必要があるサーバ、ルータなどのグローバル リソースを高速スイッチ ポートに直接接続し、各ユーザに専用の高速セグメントを与えます。 スイッチと接続先サーバおよびルータ間で EtherChannel 機能を使用します。

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

表 1-2 ネットワーク サービスの提供

ネットワークに対する需要	推奨する設計方式
マルチメディア アプリケーションにおける帯域幅の効率的な利用およびミッションクリティカルなアプリケーションに対する帯域幅保証	<ul style="list-style-type: none"> IGMP スヌーピングを利用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 パケット分類、マーキング、スケジューリング、輻輳回避など、他の QoS メカニズムを使用し、適切なプライオリティ レベルを指定してトラフィックを分類し、最大限の柔軟性を得ながら、ミッションクリティカルなユニキャスト、マルチキャスト、およびマルチメディア アプリケーションをサポートできるようにします。 MVR を使用して、マルチキャスト VLAN 上でマルチキャスト ストリームを継続的に送信し、なおかつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。

表 1-2 ネットワーク サービスの提供 (続き)

ネットワークに対する需要	推奨する設計方式
常時オンのミッションクリティカルなアプリケーションを実現するための、ネットワークの冗長性およびアベイラビリティに対する大きな需要	<ul style="list-style-type: none"> • HSRP を使用して、クラスタ コマンド スイッチとルータの冗長構成を確立します。 • VLAN トランク、および BackboneFast を使用して、アップリンク ポート上でトラフィックのロード バランシングを実行し、VLAN トラフィックの転送時にポート コストが低いアップリンク ポートが選択されるようにします。
IP テレフォニーに対する新しい需要	<ul style="list-style-type: none"> • QoS を使用して、輻輳の発生時に IP テレフォニーなどのアプリケーションを優先順位付けし、ネットワーク内で発生する遅延およびジッタを制御できるようにします。 • 1 ポートあたり少なくとも 2 つのキューをサポートするスイッチを使用して、音声およびデータ トラフィックのプライオリティを IEEE 802.1p/Q に基づくハイプライオリティまたはロープライオリティのいずれかに設定します。スイッチは、1 ポートあたり少なくとも 4 つのキューをサポートします。 • Voice VLAN ID (VVID) を使用して、音声トラフィックに別個の VLAN を用意します。

Ethernet-to-the-Factory アーキテクチャ

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

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

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

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

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

企業ゾーン

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

非武装ゾーン

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

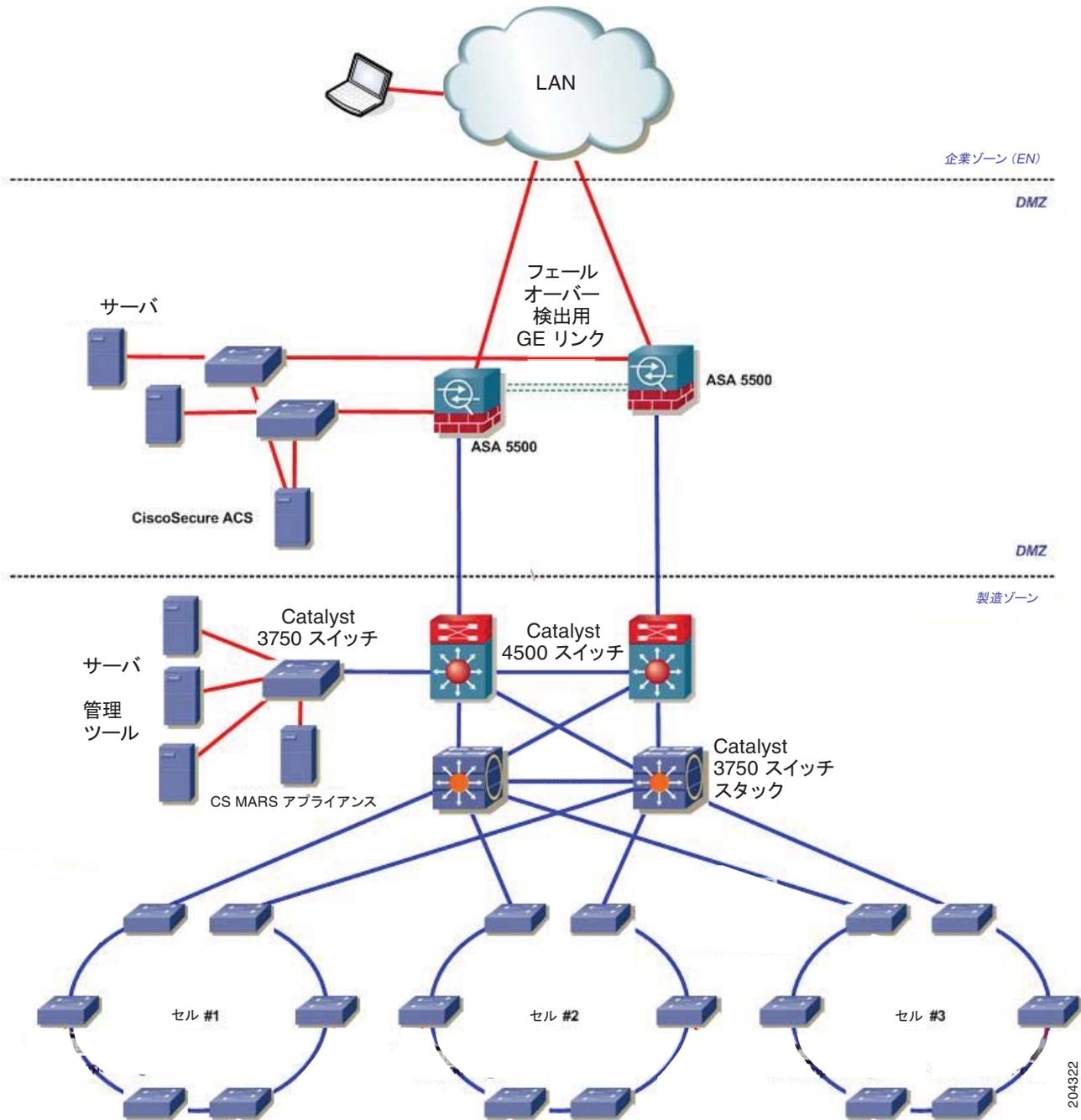
製造ゾーン

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

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

図 1-1 に、EttF アーキテクチャを示します。

図 1-1 Ethernet-to-the-Factory アーキテクチャ



トポロジのオプション

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

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

接続に関する主な考慮事項は次のとおりです。

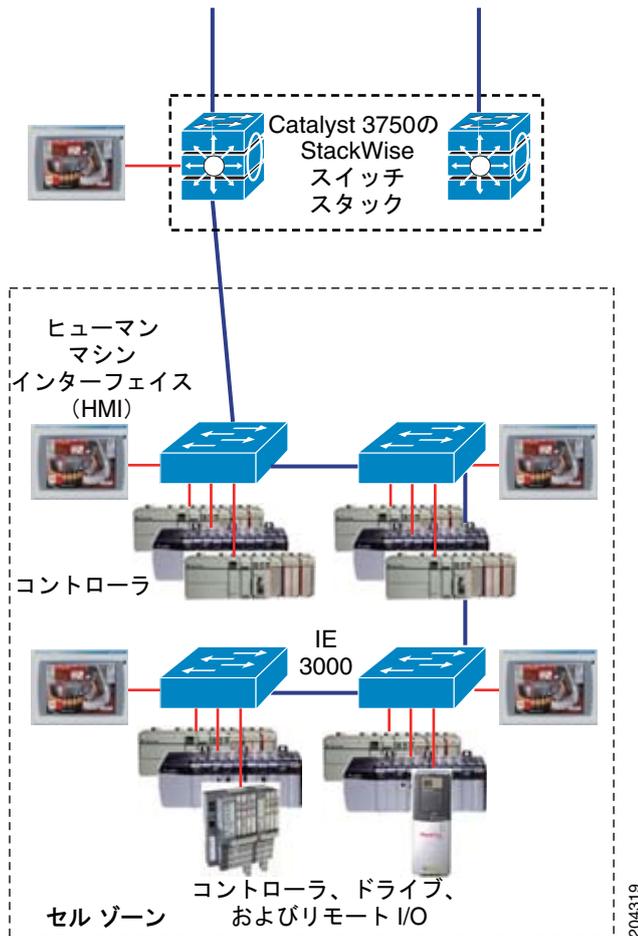
- 装置は、単一のネットワーク接続または IP 対応の I/O ブロックやリンク装置（イーサネットがサポートされていない場合）を通じてスイッチに接続されます。大半の装置にはフェールオーバー機能がないか、あっても機能が制限されているため、冗長構成のネットワーク接続を効果的に利用できません。
- 冗長構成の接続は、基幹インフラストラクチャに該当するプロセス関連の産業など、特定の産業やアプリケーションで利用されます。

セル ネットワーク：トランク廃棄トポロジ

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

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

図 1-2 セル ネットワーク : トランク廃棄トポロジ

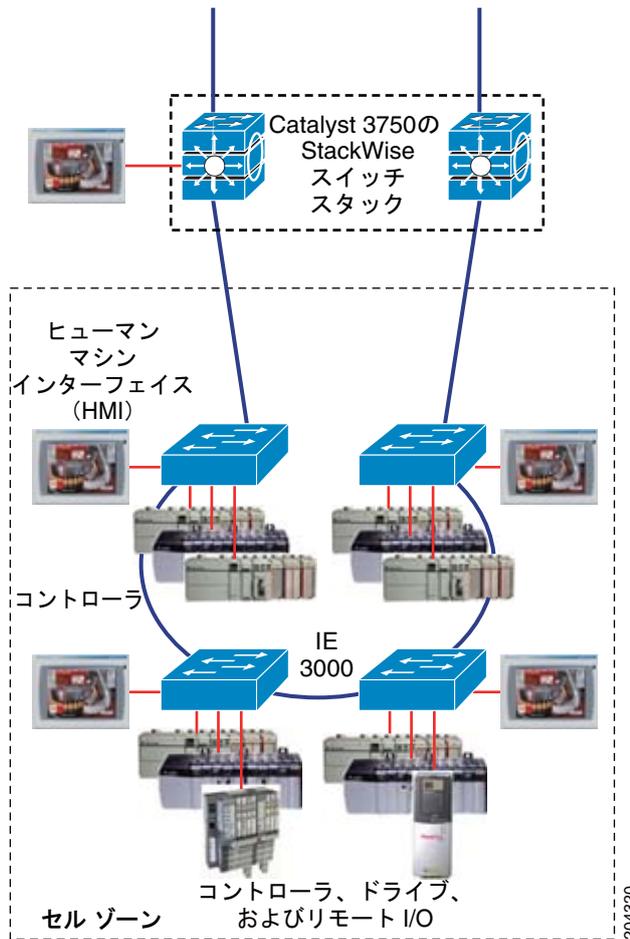


セル ネットワーク : リング トポロジ

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

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

図 1-3 セルネットワーク：リングトポロジ

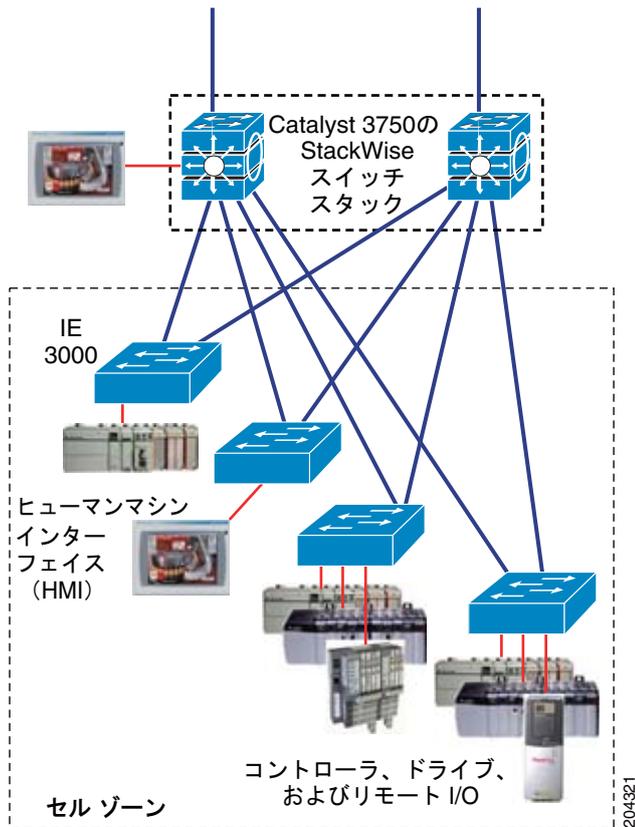


セルネットワーク：冗長構成のスタートポロジ

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

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

図 1-4 セル ネットワーク : 冗長構成のスタートポロジ



次の作業

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

- 第 2 章「コマンドラインインターフェイスの使用方法」
- 第 4 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」

特定のシスコ製品およびリリースに対する MIB の検索とダウンロードには、Cisco MIB Locator を使用します。

<http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>



CHAPTER 2

コマンドライン インターフェイスの使用法

この章では、IE 3000 スイッチを設定するための Cisco IOS コマンドライン インターフェイス (CLI) とその使用方法について説明します。特に指示がない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

この章の内容は、次のとおりです。

- 「コマンド モードの概要」 (P.2-1)
- 「ヘルプ システムの概要」 (P.2-3)
- 「コマンドの省略形」 (P.2-4)
- 「コマンドの no 形式および default 形式の概要」 (P.2-4)
- 「CLI のエラー メッセージ」 (P.2-5)
- 「コンフィギュレーション ロギングの使用法」 (P.2-5)
- 「コマンド履歴の使用法」 (P.2-6)
- 「編集機能の使用法」 (P.2-7)
- 「show および more コマンド出力の検索およびフィルタリング」 (P.2-10)
- 「CLI のアクセス」 (P.2-10)

コマンド モードの概要

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

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

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

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

■ コマンド モードの概要

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

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

表 2-1 コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	Switch>	logout または quit を入力します。	このモードを使用して次の作業を行います。 <ul style="list-style-type: none"> • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、 enable コマンドを入力します。	Switch#	disable を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、 configure コマンドを入力します。	Switch(config) #	終了して特権 EXEC モードに戻るには、 exit または end コマンドを入力するか、 Ctrl+Z を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
config-vlan	グローバル コンフィギュレーション モードで、 vlan vlan-id コマンドを入力します。	Switch(config-vlan) #	グローバル コンフィギュレーション モードに戻る場合は、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、VLAN (仮想 LAN) パラメータを設定します。VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) モードがトランスパレントであるときは、拡張範囲 VLAN (VLAN ID が 1006 以上) を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
VLAN コンフィギュレーション	特権 EXEC モードで、 vlan database コマンドを入力します。	Switch(vlan) #	終了して特権 EXEC モードに戻るには、 exit を入力します。	このモードを使用して、VLAN データベースに VLAN 1 ~ 1005 の VLAN パラメータを設定します。

表 2-1 コマンド モードの概要 (続き)

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

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

ヘルプ システムの概要

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

表 2-2 ヘルプの概要

コマンド	目的
help	任意のコマンド モードで、ヘルプ システムの概要を表示します。
コマンドの先頭部分?	入力した文字列で始まるコマンドの一覧を表示します。 次に例を示します。 Switch# di? dir disable disconnect
コマンドの先頭部分<Tab>	途中まで入力したコマンド名を完全なコマンドにします。 次に例を示します。 Switch# sh conf <tab> Switch# show configuration

表 2-2 ヘルプの概要 (続き)

コマンド	目的
?	特定のコマンド モードで使用できるすべてのコマンドの一覧を表示します。 次に例を示します。 Switch> ?
コマンド?	コマンドのキーワードの一覧を表示します。 次に例を示します。 Switch> show ?
コマンド キーワード?	キーワードに対応する引数の一覧を表示します。 次に例を示します。 Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet

コマンドの省略形

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

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

```
Switch# show conf
```

コマンドの no 形式および default 形式の概要

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** を指定せずにコマンドを使用すると、ディセーブルにした機能が再びイネーブルになり、また、デフォルトでディセーブルに設定されている機能がイネーブルになります。

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

CLI のエラー メッセージ

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

表 2-3 CLI の代表的なエラー メッセージ

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

コンフィギュレーション ロギングの使用法

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



(注)

CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用法

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

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

コマンド履歴バッファ サイズの変更

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

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

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

指定できる範囲は 0 ~ 256 です。

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

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

指定できる範囲は 0 ~ 256 です。

コマンドの呼び出し

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

表 2-4 コマンドの呼び出し

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

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

コマンド履歴機能のディセーブル化

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

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

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

編集機能の使用法

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

- 「編集機能のイネーブル化およびディセーブル化」(P.2-7) (任意)
- 「キーストロークによるコマンドの編集」(P.2-8) (任意)
- 「画面幅よりも長いコマンドラインの編集」(P.2-9) (任意)

編集機能のイネーブル化およびディセーブル化

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

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

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

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

```
Switch# terminal editing
```

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

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

キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集 (続き)

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

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

画面幅よりも長いコマンドラインの編集

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

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

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

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

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

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

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

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が 80 カラム幅以外である場合には、**terminal width** 特権 EXEC コマンドを使用して、端末の幅を設定してください。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンド エントリを呼び出して変更できます。前に入力したコマンド エントリの呼び出し方法については、「[キーストロークによるコマンドの編集](#)」(P.2-8) を参照してください。

show および more コマンド出力の検索およびフィルタリング

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

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

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

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

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

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

CLI のアクセス

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

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのスタートアップガイドに記載されている手順で、スイッチのコンソールポートに端末または PC を接続し、スイッチの電源をオンにする必要があります。また、起動プロセスおよび IP 情報を指定する場合に使用できるオプションについて理解するため、[第 4 章「スイッチの IP アドレスおよびデフォルトゲートウェイの割り当て」](#)を参照してください。

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

次のいずれかの方法で、スイッチとの接続を確立できます。

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

Telnet アクセスのためのスイッチ設定については、「[端末回線に対する Telnet パスワードの設定](#)」(P.11-6)を参照してください。スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

SSH のためのスイッチ設定については、「[SSH のためのスイッチの設定](#)」(P.11-47)を参照してください。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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



CHAPTER 3

スイッチ アラームの設定

この章では、IE 3000 スイッチのアラームを設定する方法について説明します。

この章の内容は、次のとおりです。

- 「スイッチ アラームの概要」(P.3-1)
- 「外部アラームの設定」(P.3-4)
- 「スイッチ アラームの設定」(P.3-6)
- 「スイッチ アラーム ステータスの表示」(P.3-13)



(注)

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



(注)

アラームの入力ポートおよび出力ポートの詳細については、『Cisco Switch Hardware Installation Guide』を参照してください。

スイッチ アラームの概要

スイッチ ソフトウェアは、ポート単位またはスイッチ単位でスイッチの状態をモニタします。スイッチまたはポートの現在の状態と設定されているパラメータとが一致しない場合、スイッチ ソフトウェアはアラームを発生させるかシステム メッセージを表示します。デフォルトでは、スイッチ ソフトウェアは、システム メッセージ ロギング ファシリティ (*syslog* ファシリティ) にシステム メッセージを送信します。また、簡易ネットワーク管理プロトコル (SNMP) トラップを SNMP サーバに送信するようにスイッチを設定することもできます。アラーム リレーを使用すると、外部のアラーム デバイスをトリガーするようにスイッチを設定できます。アラームの設定方法の詳細については、「[スイッチ アラームの設定](#)」(P.3-6) を参照してください。

- 「グローバル ステータス モニタリング アラーム」(P.3-2)
- 「FCS エラー ヒステリシスしきい値」(P.3-2)
- 「ポート ステータス モニタリング アラーム」(P.3-2)
- 「アラーム発生オプション」(P.3-3)

グローバル ステータス モニタリング アラーム

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

表 3-1 グローバル ステータス モニタリング アラーム

アラーム	説明
電源装置アラーム	スイッチは、デュアル電源装置レベルをモニタします。2つの電源がスイッチにインストールされている場合は、1つの電源に障害が発生するとアラームが発生します。両方の電源装置が稼働状態になると、アラームは自動的にクリアされます。電源装置アラームをハードウェアリレーに接続するように設定できます。詳細については、「 電源装置アラームの設定 」(P.3-7)を参照してください。
温度アラーム	<p>スイッチは、スイッチ内部の環境条件をモニタする温度センサーを2つ備えています。</p> <ul style="list-style-type: none"> プライマリ アラームは、低温時 (-20 °C) および高温時 (95 °C) で、発生し自動的にイネーブルになります。これをディセーブルにはできません。デフォルトでは、プライマリ温度アラームはメジャー リレーに関連付けられています。 セカンダリ アラームは、設定されている高温と低温の温度しきい値よりシステムの温度が高くなった場合もしくは低くなった場合に発生します。デフォルトでは、セカンダリ アラームはディセーブルになっています。 <p>詳細については、「スイッチの温度アラームの設定」(P.3-7)を参照してください。</p>

FCS エラー ヒステリシスしきい値

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

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

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

$$h = \text{アラーム クリアしきい値} / \text{アラーム設定しきい値}$$

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

FCS ヒステリシスしきい値は、スイッチのすべてのポートに適用されます。指定できる範囲は1 ~ 10% です。デフォルト値は10% です。詳細については、「[FCS Bit Error Rate アラームの設定](#)」(P.3-9)を参照してください。

ポート ステータス モニタリング アラーム

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

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



(注)

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

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

表 3-2 ポート ステータス モニタリング アラーム

アラーム	説明
Link Fault アラーム	ポートの物理層に問題があり、データ伝送の信頼性が低い場合、スイッチは Link Fault アラームを生成します。一般的なリンク障害は信号またはクロック消失です。リンク障害がクリアされると、Link Fault アラームも自動的にクリアされます。このアラームの重大度は、レベル 3、エラー状態です。
Port not Forwarding アラーム	ポートでパケット転送が行われていない場合、スイッチは Port not Forwarding アラームを生成します。ポートでパケット転送が開始されると、このアラームは自動的にクリアされます。このアラームの重大度は、レベル 4、警告です。
Port not Operating アラーム	起動時のセルフテスト中にポート障害が発生すると、スイッチは Port not Operating アラームを生成します。発生した Port not Operating アラームは、スイッチの再起動時にポートが動作可能である場合にだけ、クリアされます。このアラームの重大度は、レベル 3、エラー状態です。
FCS Bit Error Rate アラーム	設定されている FCS ビット エラー レートに実際のレートが近づくと、スイッチは FCS Bit Error Rate アラームを生成します。各ポートの FCS ビット エラー レートは、インターフェイス コンフィギュレーション CLI を使用して設定できます。詳細については、「 FCS Bit Error Rate アラームの設定 」(P.3-9) を参照してください。このアラームの重大度は、レベル 3、エラー状態です。

アラーム発生オプション

スイッチでは、次のアラーム発生方法がサポートされています。

- 設定可能なリレー

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

リレーを設定する方法については、「[スイッチアラームの設定](#)」(P.3-6) を参照してください。

- SNMP トラップ

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

`snmp-server enable traps` コマンドを変更すると、アラーム トラップを SNMP サーバに送信できるようになります。アラーム プロファイルを使用して、SNMP アラーム トラップを送信するための環境またはポート ステータス アラーム条件を設定できます。詳細については、「[SNMP トラップのイネーブル化](#)」(P.3-13) を参照してください。

- Syslog メッセージ

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

外部アラームの設定

スイッチの前面パネル上のアラーム入力ポートに対して、ドア、温度計、火災報知機といった、ご使用の環境内に存在する外部デバイスからのアラーム入力を最大 4 つまで接続できます。

図 3-1 アラーム ポートのピン割り当て

ピン	アラーム接続	1 2 3 4 5 6 7 8
1	アラーム 1 入力	
2	アラーム 2 入力	
3	通常閉	
4	アラーム 3 入力	
5	アラーム 4 入力	
6	通常開	
7	アラーム出力コモン	
8	アラーム入力コモン	

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

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

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

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

アラーム接点を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>alarm contact contact-number description string</code>	(任意) アラーム接点番号の説明を設定します。 <ul style="list-style-type: none"> <code>contact-number</code> の値は 1 ~ 4 です。 説明の文字列は 80 文字までの英数字で指定し、この文字列は、生成されるすべてのシステム メッセージに表示されます。
ステップ3	<code>alarm contact {contact-number all} {severity {critical major minor} trigger {closed open}}</code>	アラーム接点番号またはすべての接点番号の、トリガーおよび重大度を設定します。 <ul style="list-style-type: none"> 接点番号 (1 ~ 4) を入力するか、すべてのアラームを設定することを指定します。アラーム接点のピン割り当てについては、図 3-1 を参照してください。 <code>severity</code> には、<code>critical</code>、<code>major</code>、または <code>minor</code> を入力します。重大度を設定しない場合、デフォルトは <code>minor</code> となります。 <code>trigger</code> には、<code>open</code> または <code>closed</code> を入力します。トリガーを設定しない場合、回路が <code>closed</code> のときにアラームがトリガーされます。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show env alarm-contact</code>	設定されたアラーム接点を表示します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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



(注)

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

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

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

```

Severity:    critical
Trigger:    open
ALARM CONTACT 2
Status:     not asserted
Description: door sensor
Severity:   major
Trigger:    closed
ALARM CONTACT 3
Status:     not asserted
Description: flood sensor
Severity:   critical
Trigger:    closed
ALARM CONTACT 4
Status:     not asserted
Description:
Severity:   critical
Trigger:    closed

```

スイッチ アラームの設定

- ・ 「デフォルトのスイッチ アラーム設定」 (P.3-6)
- ・ 「電源装置アラームの設定」 (P.3-7)
- ・ 「スイッチの温度アラームの設定」 (P.3-7)
- ・ 「FCS Bit Error Rate アラームの設定」 (P.3-9)
- ・ 「アラーム プロファイルの設定」 (P.3-11)
- ・ 「SNMP トラップのイネーブル化」 (P.3-13)

デフォルトのスイッチ アラーム設定

表 3-3 デフォルトのスイッチ アラーム設定

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

電源装置アラームの設定

電源の存在は、動的に検出されます。スイッチの電源情報を表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show env power** コマンドを使用します。

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

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

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

デフォルトの電源装置アラームをディセーブルにするには、**alarm facility power-supply disable** グローバル コンフィギュレーション コマンドを使用します。

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



(注) **notifies** コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「[SNMP トラップのイネーブル化](#)」(P.3-13)を参照してください。

次に、電源装置モニタリングアラームをメジャー リレーに設定する例を示します。

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

スイッチの温度アラームの設定

プライマリ温度アラームおよびセカンダリ温度アラームの温度しきい値は変更できます。また、プライマリ温度アラームまたはセカンダリ温度アラームのいずれかをリレーに関連付けることもできます。

- 「[スイッチのプライマリ温度しきい値の設定](#)」(P.3-7)
- 「[スイッチのセカンダリ温度しきい値の設定](#)」(P.3-8)
- 「[温度アラームのリレーへの関連付け](#)」(P.3-8)

スイッチのプライマリ温度しきい値の設定

alarm facility temperature primary グローバル コンフィギュレーション コマンドを使用すると、プライマリ温度モニタリングアラームの低温しきい値および高温しきい値を設定できます。

高温しきい値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>alarm facility temperature primary high threshold</code>	プライマリ 高温しきい値を設定します。しきい値は、-150 °C ~ 300 °C の範囲に設定します。
ステップ3	<code>alarm facility temperature primary low threshold</code>	プライマリ 低温しきい値を設定します。しきい値は、-200 °C ~ 250 °C の範囲に設定します。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show alarm settings</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

スイッチのセカンダリ 温度しきい値の設定

alarm facility temperature secondary グローバル コンフィギュレーション コマンドを使用すると、セカンダリ 温度モニタリング アラームの低温しきい値および高温しきい値を設定できます。

低温しきい値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>alarm facility temperature secondary high threshold</code>	セカンダリ 高温しきい値を設定します。しきい値は、-150 °C ~ 300 °C の範囲に設定します。
ステップ3	<code>alarm facility temperature secondary low threshold</code>	セカンダリ 低温しきい値を設定します。しきい値は、-200 °C ~ 250 °C の範囲に設定します。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show alarm settings</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、セカンダリ 温度しきい値アラームをディセーブルにする例を示します。

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

温度アラームのリレーへの関連付け

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



(注) スイッチのシングル リレーは、メジャー リレーと呼ばれます。

特権 EXEC モードから、次の手順に従ってプライマリ温度アラームまたはセカンダリ温度アラームをリレーに関連付けます。

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



(注) `notifies` コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず `snmp-server enable traps alarms` グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「[SNMP トラップのイネーブル化](#)」(P.3-13) を参照してください。

セカンダリ温度アラームをディセーブルにするには、`no alarm facility temperature secondary` を使用します。

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

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

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

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

FCS Bit Error Rate アラームの設定

- 「[FCS エラーしきい値の設定](#)」(P.3-10)
- 「[FCS エラー ヒステリシスしきい値の設定](#)」(P.3-10)

FCS エラーしきい値の設定

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

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

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

デフォルトの FCS しきい値に戻すには、**no fcs-threshold** インターフェイス コンフィギュレーション コマンドを使用します。

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

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

FCS エラー ヒステリシスしきい値の設定

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



(注) FCS ヒステリシスしきい値は、スイッチのすべてのポートに適用されます。

特権 EXEC モードから、次の手順に従って、スイッチに対する FCS エラー ヒステリシスしきい値を設定します。

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

FCS エラー ヒステリシスしきい値をデフォルト値に設定するには、**no alarm facility fcs-hysteresis** コマンドを使用します。



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

次に、FCS エラー ヒステリシスを 5% に設定する例を示します。

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

アラーム プロファイルの設定

- 「アラーム プロファイルの作成または変更」 (P.3-11)
- 「特定のポートへのアラーム プロファイルの割り当て」 (P.3-12)

アラーム プロファイルの作成または変更

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



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

特権 EXEC モードから、次の手順に従ってアラーム プロファイルを作成します。

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

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

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

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



(注)

notifies コマンドを使用してアラーム トラップを SNMP サーバに送信するには、まず **snmp-server enable traps alarms** グローバル コンフィギュレーション コマンドを使用して SNMP サーバをセットアップする必要があります。「[SNMP トラップのイネーブル化](#)」(P.3-13) を参照してください。

表 3-4 に、*alarmList* ID と、対応するアラーム定義の一覧を示します。これらのアラームの詳細については、「[ポート ステータス モニタリング アラーム](#)」(P.3-2) を参照してください。

表 3-4 AlarmList ID 番号とアラームの説明

AlarmList ID	アラームの説明
1	リンク障害
2	ポートで転送が行われていない
3	ポートが動作していない
4	FCS エラー レートがしきい値を超えている

特定のポートへのアラーム プロファイルの割り当て

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

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

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

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

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

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

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

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

SNMP トラップのイネーブル化

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



(注)

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

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

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

スイッチ アラーム ステータスの表示

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

表 3-5 グローバルおよびポートのアラーム ステータスを表示するコマンド

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



CHAPTER 4

スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て

この章では、自動および手動の各方法を使用して IE 3000 スwitchのスイッチ初期設定（IP アドレスおよびデフォルト ゲートウェイ情報の割り当てなど）を作成する方法について説明します。Switch のスタートアップ コンフィギュレーションを変更する方法についても説明します。



(注)

この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスと、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』を参照してください。

この章の内容は、次のとおりです。

- 「起動プロセスの概要」(P.4-1)
- 「スイッチ情報の割り当て」(P.4-3)
- 「実行コンフィギュレーションの確認および保存」(P.4-16)
- 「スタートアップ コンフィギュレーションの変更」(P.4-17)
- 「ソフトウェア イメージ リロードのスケジュール設定」(P.4-22)



(注)

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

起動プロセスの概要

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

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

- 下位レベルの CPU 初期化を行います。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの Power-on Self-Test (POST; 電源投入時セルフテスト) を行います。CPU DRAM と、フラッシュ ファイル システムを構成するフラッシュ デバイスの部分をテストします。
- システム ボード上のコンパクト フラッシュ ファイル システムを初期化します。
- デフォルトの OS (オペレーティング システム) ソフトウェアをメモリにロードし、スイッチを起動します。

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

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

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

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

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

また、OS が使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。トラップドアからシステムへアクセスして、必要があれば、フラッシュ ファイル システムをフォーマットし、XMODEM プロトコルを使用して OS のソフトウェアイメージを再インストールし、失われたパスワードを回復し、最終的に OS を再起動できます。詳細については、「ソフトウェアで障害が発生した場合の回復」(P.53-2) および「パスワードを忘れた場合の回復」(P.53-3) を参照してください。



(注)

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

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

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



(注)

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

- デフォルトのストップ ビットは 1 です。

- デフォルトのパリティ設定は「なし」です。

スイッチ情報の割り当て

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

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

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



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

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

ここでは、次の設定について説明します。

- 「デフォルトのスイッチ情報」(P.4-3)
- 「DHCP ベースの自動設定の概要」(P.4-4)
- 「手動でのスイッチ情報の割り当て」(P.4-16)

デフォルトのスイッチ情報

表 4-1 に、デフォルトのスイッチ情報を示します。

表 4-1 デフォルトのスイッチ情報

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

DHCP ベースの自動設定の概要

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

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

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

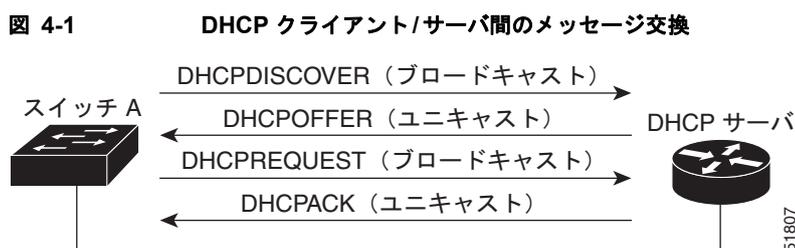
スイッチの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが異なる LAN 上で動作している場合、スイッチと DHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャスト トラフィックを転送します。ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

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

DHCP クライアント要求プロセス

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

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



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

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

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

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

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

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

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

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

DHCP ベースの自動設定およびイメージ アップデートの概要

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

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

DHCP 自動設定

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

DHCP 自動イメージ アップデート

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

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



(注)

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

スイッチを DHCP サーバとして設定する場合の手順については、「[DHCP ベースの自動設定の設定 \(P.4-7\)](#)」および『[Cisco IOS IP Configuration Guide, Release 12.2](#)』の「IP Addressing and Services」の章にある「[Configuring DHCP](#)」を参照してください。

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

制限事項と制約事項

次に、制限事項について説明します。

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



(注)

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

DHCP ベースの自動設定の設定

ここでは、次の設定について説明します。

- 「DHCP サーバ設定時の注意事項」 (P.4-7)
- 「TFTP サーバの設定」 (P.4-8)
- 「DNS の設定」 (P.4-8)
- 「リレー デバイスの設定」 (P.4-9)
- 「コンフィギュレーション ファイルの入手方法」 (P.4-9)
- 「構成例」 (P.4-10)

DHCP サーバ設定時の注意事項

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

DHCP サーバには、スイッチのハードウェア アドレスによって各スイッチと結び付けられている予約済みのリースを設定する必要があります。

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

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

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

- TFTP サーバ名 (必須)
- ブート ファイル名 (クライアントが必要とするコンフィギュレーション ファイル名) (推奨)
- ホスト名 (任意)

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

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

スイッチは、DHCP サーバとして機能できます。デフォルトでは、Cisco IOS DHCP サーバおよび DHCP リレー エージェント機能はスイッチ上でイネーブルにされていますが、設定されていません。これらの機能は動作しません。DHCP サーバがシスコ デバイスである場合、DHCP 設定に関する詳細については、Cisco.com のホームページから [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] を選択し、『Cisco IOS IP Configuration Guide』の「IP Addressing and Services」の章にある「Configuring DHCP」の部分を参照してください。

TFTP サーバの設定

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

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

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

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

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

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

DNS の設定

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

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

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

リレー デバイスの設定

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

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

図 4-2 では、ルータ インターフェイスを次のように設定しています。

インターフェイス 10.0.0.2 では、

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

インターフェイス 20.0.0.1 では、

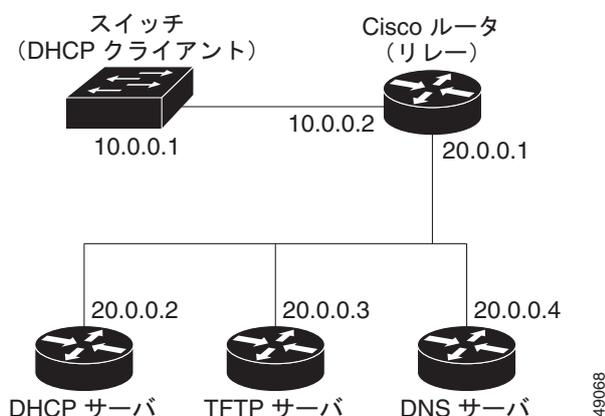
```
router(config-if)# ip helper-address 10.0.0.1
```



(注)

スイッチをリレー デバイスとして機能させる場合は、インターフェイスをルーテッド ポートに設定してください。詳細については、「ルーテッド ポート」(P.14-4) および「レイヤ 3 インターフェイスの設定」(P.14-22) を参照してください。

図 4-2 自動設定でのリレー デバイスの使用



コンフィギュレーション ファイルの入手方法

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

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

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

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

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

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

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

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

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

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



(注)

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

構成例

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

図 4-3 DHCP ベースの自動設定を使用するネットワークの構成例

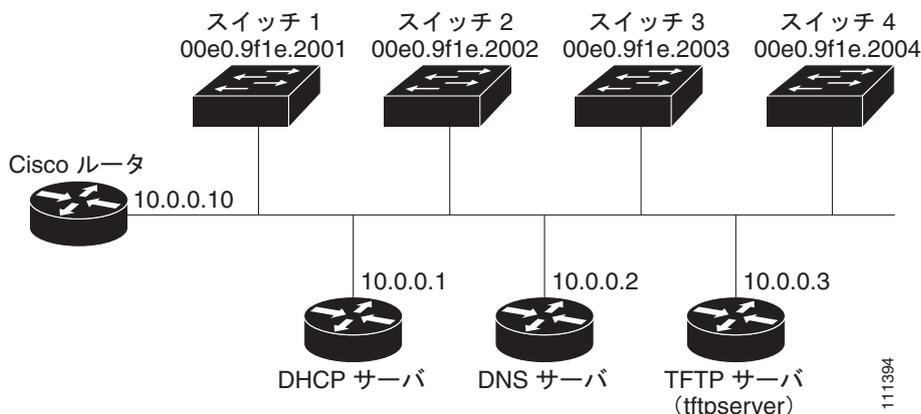


表 4-2 は、DHCP サーバ上の予約リースの設定例です。

表 4-2 DHCP サーバ コンフィギュレーション

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

DNS サーバ コンフィギュレーション

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

TFTP サーバ コンフィギュレーション (UNIX)

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

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

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

DHCP クライアント コンフィギュレーション

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

コンフィギュレーションの説明

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

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

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

DHCP 自動設定機能およびイメージ アップデート機能

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

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dhcp pool name</code>	DHCP サーバのアドレス プール名を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	<code>bootfile filename</code>	ブート イメージとして使用されるコンフィギュレーション ファイルの名前を指定します。
ステップ 4	<code>network network-number mask prefix-length</code>	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。 (注) プレフィックス長は、アドレス プレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワーク マスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ (/) で開始する必要があります。
ステップ 5	<code>default-router address</code>	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。

	コマンド	目的
ステップ6	option 150 address	TFTP サーバの IP アドレスを指定します。
ステップ7	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ8	tftp-server flash:filename.text	TFTP サーバ上のコンフィギュレーション ファイルを指定します。
ステップ9	interface interface-id	コンフィギュレーション ファイルを受信するクライアントのアドレスを指定します。
ステップ10	no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ11	ip address address mask	インターフェイスの IP アドレスおよびマスクを指定します。
ステップ12	end	特権 EXEC モードに戻ります。
ステップ13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

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

DHCP 自動設定の設定により新しいスイッチに TFTP および DHCP の設定をして新しいイメージおよび新しいコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。



(注)

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip dhcp pool name	DHCP サーバのアドレス プール名を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ3	bootfile filename	ブート イメージとして使用されるファイルの名前を指定します。

■ スイッチ情報の割り当て

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

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

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

Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

クライアントの設定

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	boot host dhcp	保存されているコンフィギュレーションで自動設定をイネーブルにします。
ステップ3	boot host retry timeout <i>timeout-value</i>	(任意) システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 (注) タイムアウトを設定しないと、システムは無期限に DHCP サーバから IP アドレスを取得しようとします。
ステップ4	banner config-save ^C <i>warning-message</i> ^C	(任意) コンフィギュレーション ファイルを NVRAM に保存しようとするときに表示される警告メッセージを作成します。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show boot	設定を確認します。

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

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



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

手動でのスイッチ情報の割り当て

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



(注) スイッチで IP サービス イメージを実行している場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してポートをレイヤ 3 モードにすると、IP 情報をポートに手動で割り当てることもできます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface vlan <i>vlan-id</i>	インターフェイス コンフィギュレーション モードを開始し、IP 情報を割り当てる VLAN を入力します。指定できる VLAN 範囲は 1 ~ 4094 です。
ステップ 3	ip address <i>ip-address subnet-mask</i>	IP アドレスおよびサブネット マスクを入力します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ip default-gateway <i>ip-address</i>	スイッチに直接接続しているネクスト ホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。デフォルト ゲートウェイは、スイッチから宛先 IP アドレスを取得していない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 (注) IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces vlan <i>vlan-id</i>	設定された IP アドレスを確認します。
ステップ 8	show ip redirects	設定されたデフォルト ゲートウェイを確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

スイッチのシステム名の設定、特権 EXEC コマンドへのアクセスの保護、時刻および日付の設定については、第 7 章「スイッチの管理」を参照してください。

実行コンフィギュレーションの確認および保存

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

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

Current configuration: 1363 bytes
!
version 12.2
```

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch A
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxEO
!
.
<output truncated>
.
interface gigabitethernet1/1
no switchport
ip address 172.20.137.50 255.255.255.0
!

interface gigabitethernet1/2
mvr type source

<output truncated>

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

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

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

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

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

スタートアップ コンフィギュレーションの変更

ここでは、スイッチのスタートアップ コンフィギュレーションを変更する方法について説明します。

- 「起動のデフォルト設定」(P.4-18)
- 「コンフィギュレーション ファイルの自動ダウンロード」(P.4-18)
- 「手動で起動する場合」(P.4-19)

- 「特定のソフトウェア イメージを起動する場合」 (P.4-20)
- 「環境変数の制御」 (P.4-20)

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

起動のデフォルト設定

表 4-3 に、起動のデフォルト設定を示します。

表 4-3 起動のデフォルト設定

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

コンフィギュレーション ファイルの自動ダウンロード

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

システム コンフィギュレーションを読み書きするためのファイル名の指定

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

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	boot config-file flash:/file-url	<p>次の起動時に読み込むコンフィギュレーション ファイルを指定します。</p> <p><i>file-url</i> に、パス (ディレクトリ) およびコンフィギュレーション ファイル名を指定します。</p> <p>ファイル名およびディレクトリ名は、大文字と小文字を区別しません。</p>
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show boot	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

手動で起動する場合

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

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	boot manual	次の起動時に、スイッチを手動で起動できるようにします。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show boot	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

特定のソフトウェア イメージを起動する場合

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	boot system filesystem:/file-url	<p>次の起動時に、フラッシュ メモリ内の特定のイメージを起動するようにスイッチを設定します。</p> <ul style="list-style-type: none"> filesystem: には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。 file-url には、パス (ディレクトリ) および起動可能なイメージの名前を指定します。 <p>ファイル名およびディレクトリ名は、大文字と小文字を区別します。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show boot	<p>設定を確認します。</p> <p>boot system グローバル コンフィギュレーション コマンドによって、BOOT 環境変数の設定が変更されます。</p> <p>次の起動時に、スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとしません。</p>
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

環境変数の制御

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

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

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

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

環境変数には 2 種類のデータが保存されます。

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

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



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

表 4-4 で、代表的な環境変数の機能について説明します。

表 4-4 環境変数

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

ソフトウェア イメージ リロードのスケジュール設定

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



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

リロードのスケジュール設定

ソフトウェア イメージを後でリロードするようにスイッチを設定するには、特権 EXEC モードで次のいずれかのコマンドを使用します。

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

指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされるようにスケジュールを設定します。リロードは、約 24 日以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。

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

指定した時刻（24 時間形式を使用）にソフトウェアがリロードされるように、スケジュールを設定します。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現在時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。



(注) **at** キーワードを使用するのは、スイッチのシステム クロックが（Network Time Protocol (NTP)、ハードウェア カレンダー、または手動で）設定されている場合だけです。時刻は、スイッチに設定されたタイムゾーンに基づきます。複数のスイッチで同時にリロードが行われるように設定する場合は、各スイッチの時刻を NTP によって同期させる必要があります。

reload コマンドはシステムを停止させます。手動で起動することが設定されていない限り、システムは自動的に再起動します。**reload** コマンドは、スタートアップ コンフィギュレーションにスイッチの設定情報を保存（**copy running-config startup-config**）した後で使用します。

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

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

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

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

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

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

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

リロード スケジュール情報の表示

スケジュールがすでに設定されているリロードの情報を表示する、またはスイッチ上でリロードのスケジュールが設定されているかどうかを調べるには、**show reload** 特権 EXEC コマンドを使用します。

リロードが予定されている時刻、リロードの理由を含め（リロードのスケジュール設定時に指定されている場合）、リロード情報が表示されます。



CHAPTER 5

Cisco IOS Configuration Engine の設定

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



(注)

Cisco Configuration Engine の設定情報については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

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

- 「Cisco Configuration Engine ソフトウェアの概要」 (P.5-1)
- 「Cisco IOS エージェントの概要」 (P.5-5)
- 「Cisco IOS エージェントの設定」 (P.5-6)
- 「CNS 設定の表示」 (P.5-14)

Cisco Configuration Engine ソフトウェアの概要

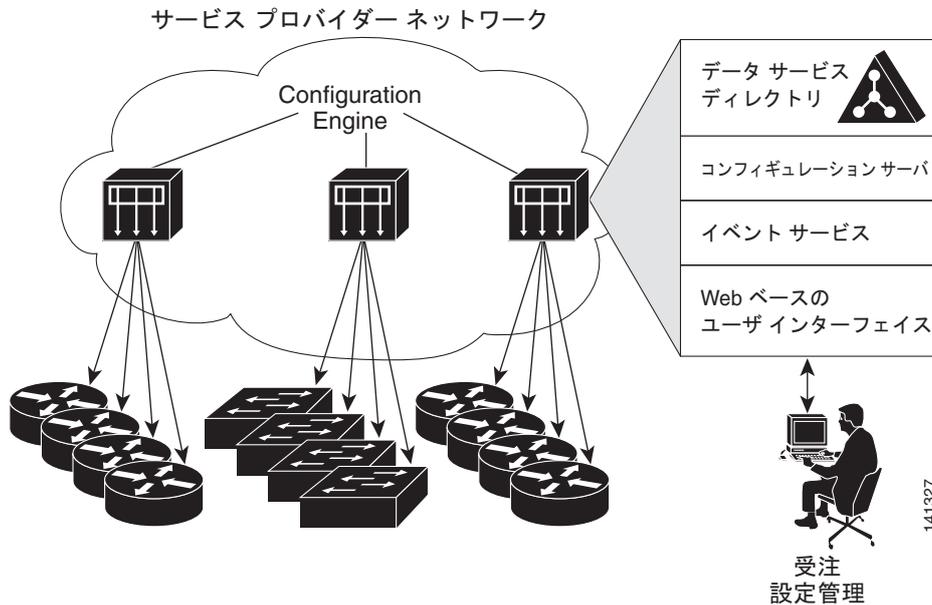
Cisco Configuration Engine は、ネットワーク管理ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します (図 5-1 を参照)。各 Configuration Engine は、シスコ デバイス (スイッチとルータ) のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Configuration Engine はデバイス固有の設定変更を生成してデバイスに送信し、設定変更を実行してその結果をロギングすることで、初期設定および設定の更新を自動化します。

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

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

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

図 5-1 Configuration Engine アーキテクチャの概要



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

コンフィギュレーション サービス

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

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

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

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

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

イベント サービス

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

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

NSM

Configuration Engine には NameSpace Mapper (NSM) を装備しています。NSM は、アプリケーション、デバイス、またはグループ ID、およびイベントに基づくデバイスの論理グループ管理用に検索 サービスを提供します。

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

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

CNS ID およびデバイスのホスト名に関する重要事項

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

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

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

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

ConfigID

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

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

DeviceID

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

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

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

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

ホスト名および DeviceID

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

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

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



注意

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

ホスト名、DeviceID、ConfigID の使用方法

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

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

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



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

Cisco IOS エージェントの概要

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

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

初期設定

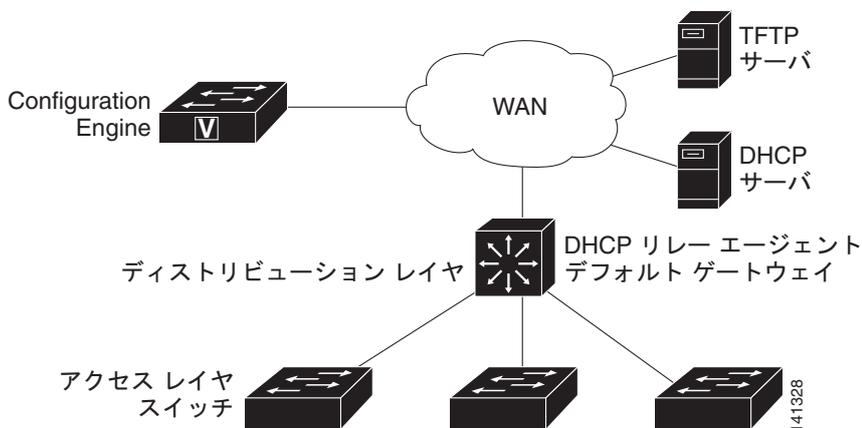
スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol (DHCP) 要求をブロードキャストすることで IP アドレスを取得しようとしています。サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバの IP アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。DHCP リレー エージェントは、この応答をスイッチに転送します。

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

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

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

図 5-2 初期設定の概要



差分（部分）設定

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

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

同期設定

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

Cisco IOS エージェントの設定

スイッチの Cisco IOS ソフトウェアに組み込まれた Cisco IOS エージェントによって、スイッチを接続して自動的に設定できます（「[自動 CNS 設定のイネーブル化](#)」(P.5-7) を参照）。設定を変更する場合、またはカスタム コンフィギュレーションをインストールする場合は次の手順を参照してください。

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

自動 CNS 設定のイネーブル化

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

表 5-1 自動設定イネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定（コンフィギュレーション ファイルなし）
ディストリビューション スイッチ	<ul style="list-style-type: none"> IP ヘルパー アドレス DHCP リレー エージェントのイネーブル化 IP ルーティング（デフォルト ゲートウェイとして使用する場合）
DHCP サーバ	<ul style="list-style-type: none"> IP アドレスの割り当て TFTP サーバの IP アドレス TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス デフォルト ゲートウェイの IP アドレス
TFTP サーバ	<ul style="list-style-type: none"> スイッチと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル （デフォルトのホスト名の代わりに）スイッチ MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたスイッチ スイッチにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。



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

CNS イベント エージェントのイネーブル化



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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns event { <i>hostname</i> <i>ip-address</i> } [<i>port-number</i>] [backup] [failover-time seconds] [keepalive seconds] <i>retry-count</i>] [reconnect time] [source ip-address]	<p>イベント エージェントをイネーブルにして、ゲートウェイ パラメータを入力します。</p> <ul style="list-style-type: none"> • {<i>hostname</i> <i>ip-address</i>} に、イベント ゲートウェイのホスト名または IP アドレスを入力します。 • (任意) <i>port number</i> に、イベント ゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • (任意) バックアップ ゲートウェイであることを示す場合は、backup を入力します (省略した場合は、プライマリ ゲートウェイになります)。 • (任意) failover-time seconds に、バックアップ ゲートウェイが確立された後にスイッチがプライマリ ゲートウェイ ルートを待つ時間を入力します。 • (任意) keepalive seconds に、スイッチがキープアライブ メッセージを送信する間隔を入力します。 <i>retry-count</i> に、キープアライブ メッセージへの応答がない場合に接続を終了するまでのメッセージ送信回数を入力します。デフォルト値はいずれも 0 です。 • (任意) reconnect time に、スイッチがイベント ゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • (任意) source ip-address に、このデバイスの送信元 IP アドレスを入力します。 <p>(注) encrypt キーワードおよび clock-timeout time キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show cns event connections	イベント エージェントに関する情報を確認します。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

Cisco IOS CNS エージェントのイネーブル化

CNS イベント エージェントをイネーブルにした後、スイッチ上で Cisco IOS CNS エージェントを起動します。次のコマンドを使用して、Cisco IOS エージェントをイネーブルにできます。

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

初期設定のイネーブル化

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns template connect name	CNS テンプレート接続コンフィギュレーション モードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 3	cli config-text	CNS 接続テンプレートにコマンドラインを入力します。テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 4		別の CNS 接続テンプレートを設定する場合は、ステップ 2 ~ 3 を繰り返します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]	<p>CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイルの名前を指定し、プロファイル パラメータを定義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。</p> <ul style="list-style-type: none"> • CNS 接続プロファイルの名前を入力します。 • (任意) retries number に、接続のリトライ回数を入力します。指定できる範囲は 1 ~ 30 です。デフォルトは 3 です。 • (任意) retry-interval seconds に、Configuration Engine への連続する接続の試行間隔を入力します。指定できる範囲は 1 ~ 40 秒です。デフォルト値は 10 秒です。 • (任意) sleep seconds に、最初の接続試行を実行するまで待機する時間を入力します。指定できる範囲は 0 ~ 250 秒です。デフォルトは 0 です。 • (任意) timeout seconds に、接続が終了しようとした後に待機する時間を入力します。指定できる範囲は 10 ~ 2000 秒です。デフォルトは 120 です。

コマンド	目的
ステップ 7 discover { controller <i>controller-type</i> dcli [subinterface <i>subinterface-number</i>] interface [<i>interface-type</i>] line <i>line-type</i> }	CNS 接続プロファイル内のインターフェイス パラメータを入力します。 <ul style="list-style-type: none"> • controller <i>controller-type</i> に、コントローラ タイプを入力します。 • dcli に、アクティブな Data-Link Connection Identifier (DLCI; データリンク接続識別子) を入力します。 (任意) subinterface <i>subinterface-number</i> に、アクティブな DLCI の検索に使用するポイントツーポイント サブインターフェイス番号を指定します。 • interface [<i>interface-type</i>] に、インターフェイスのタイプを入力します。 • line <i>line-type</i> に、ライン タイプを入力します。
ステップ 8 template <i>name</i> [... <i>name</i>]	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 9	ステップ 7 ~ 8 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイス パラメータと CNS 接続テンプレートを指定します。
ステップ 10 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 11 hostname <i>name</i>	スイッチのホスト名を入力します。
ステップ 12 ip route <i>network-number</i>	(任意) IP アドレスが <i>network-number</i> の Configuration Engine へのスタティック ルートを確立します。

コマンド	目的
ステップ 13 cns id interface num {dns-reverse ipaddress mac-address} [event] [image] または cns id {hardware-serial hostname string string udi} [event] [image]	<p>(任意) Configuration Engine が使用する一意の EventID または ConfigID を設定します。</p> <ul style="list-style-type: none"> <i>interface num</i> に、インターフェイスの種類 (たとえば、ethernet、group-async、loopback、virtual-template) を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 {dns-reverse ipaddress mac-address} では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには dns-reverse を入力し、IP アドレスを使用するには ipaddress を入力し、MAC アドレスを一意の ID として使用するには mac-address を入力します。 (任意) ID をスイッチの識別に使用する event-id 値になるように設定するには、event を入力します。 (任意) ID をスイッチの識別に使用する image-id 値になるように設定するには、image を入力します。 <p>(注) event と image キーワードの両方を省略した場合は、スイッチの識別には image-id 値が使用されます。</p> <ul style="list-style-type: none"> {hardware-serial hostname string string udi} で、hardware-serial を入力してスイッチのシリアル番号を一意の ID として設定するか、hostname (デフォルト) を入力してスイッチのホスト名を一意の ID として選択するか、string string に任意のテキストストリングを一意の ID として入力するか、または udi を入力して Unique Device Identifier (UDI; 一意のデバイス ID) を一意の ID として設定します。

コマンド	目的
ステップ 14 cns config initial {hostname ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]	Cisco IOS をイネーブルにし、初期設定を開始します。 <ul style="list-style-type: none"> • {ip-address hostname} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • (任意) port number に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • (任意) 設定が完了したときの設定の成功、失敗、または警告のメッセージ用に event をイネーブルにします。 • (任意) cns config initial グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、no-persist を入力します。no-persist キーワードを入力しない場合、cns config initial コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • (任意) page page に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • (任意) 送信元 IP アドレスに使用するには、source ip-address を入力します。 • (任意) このパラメータを使用したときの構文をチェックするには、syntax-check をイネーブルにします。 (注) encrypt キーワード、 status キーワード、 url キーワードおよび inventory キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 15 end	特権 EXEC モードに戻ります。
ステップ 16 show cns config connections	コンフィギュレーション エージェントに関する情報を確認します。
ステップ 17 show running-config	設定を確認します。

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

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

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

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

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

部分設定のイネーブル化

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	cns config partial { <i>ip-address</i> <i>hostname</i> } [<i>port-number</i>] [<i>source ip-address</i>]	<p>コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。</p> <ul style="list-style-type: none"> {<i>ip-address</i> <i>hostname</i>} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 (任意) <i>port number</i> に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 (任意) 送信元 IP アドレスに使用するには、source ip-address を入力します。 <p>(注) encrypt キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。</p>
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show cns config stats または show cns config outstanding	コンフィギュレーション エージェントに関する情報を確認します。
ステップ5	show running-config	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

CNS 設定の表示

表 5-2 特権 EXEC 表示コマンド

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



CHAPTER 6

スイッチのクラスタ化

この章では、IE 3000 スイッチ クラスタの作成と管理に関する概念と手順について説明します。Cisco Network Assistant アプリケーション（以降、Network Assistant）、コマンドライン インターフェイス (CLI) または SNMP を使用してスイッチ クラスタを作成、管理できます。具体的な手順については、オンラインヘルプを参照してください。CLI クラスタコマンドについては、スイッチ コマンドリファレンスを参照してください。

この章では、IE 3000 スイッチ クラスタを中心に説明します。クラスタ内に他のクラスタに対応した Catalyst スイッチが混在している場合の注意事項や制限事項も紹介しますが、これらのスイッチに対するクラスタ機能の詳細な説明は割愛します。特定の Catalyst プラットフォームにおけるクラスタの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

この章で説明する内容は、次のとおりです。

- 「スイッチ クラスタの概要」(P.6-1)
- 「スイッチ クラスタのプランニング」(P.6-4)
- 「CLI によるスイッチ クラスタの管理」(P.6-16)
- 「SNMP によるスイッチ クラスタの管理」(P.6-17)



(注)

特定のホストまたはネットワークに対してアクセスを制限する場合、**ip http access-class** グローバル コンフィギュレーション コマンドは使用しないことを推奨します。アクセスをコントロールするには、クラスタ コマンド **スイッチ** を使用するか、または IP アドレスが設定されているインターフェイス上に Access Control List (ACL; アクセス コントロール リスト) を適用します。ACL の詳細については、[第 38 章「ACL によるネットワーク セキュリティの設定」](#) を参照してください。

スイッチ クラスタの概要

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

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

スイッチのクラスタ化には次のような利点があります。

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

クラスタ メンバは、「クラスタ候補およびクラスタ メンバの自動検出」(P.6-4) で説明している接続方法に従ってクラスタ コマンド スイッチに接続します。ここでは、Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL スイッチに対する管理 VLAN (仮想 LAN) の検討事項を説明します。スイッチクラスタ環境におけるこれらのスイッチの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

- クラスタ コマンドスイッチに冗長性を持たせることで、コマンド スイッチに障害が発生した場合でも対応できます。1 つまたは複数のスイッチをスタンバイ クラスタ コマンドに指定すると、クラスタ メンバ間の競合を回避できます。クラスタ スタンバイ グループは、スタンバイ クラスタ コマンド スイッチのグループです。
- さまざまなスイッチを、1 つの IP アドレスで管理できます。これは、特に IP アドレスの数が限られている場合に効果があります。スイッチ クラスタとの通信はすべてクラスタ コマンド スイッチの IP アドレスで行われます。

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

表 6-1 スイッチ ソフトウェアおよびクラスタへの対応性

スイッチ	Cisco IOS リリース	クラスタへの対応性
IE 3000 スイッチ	12.2(40)EX 以降	メンバまたはコマンド スイッチ
Catalyst 3750-X または Catalyst 3560-X	12.2(53)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750-E または Catalyst 3560-E	12.2(35)SE2 以降	メンバまたはコマンド スイッチ
Catalyst 3750	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバまたはコマンド スイッチ
Catalyst 3550	12.1(4)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2975	12.2(46)EX 以降	メンバまたはコマンド スイッチ
Catalyst 2970	12.1(11)AX 以降	メンバまたはコマンド スイッチ
Catalyst 2960-S	12.2(53)SE 以降	メンバまたはコマンド スイッチ
Catalyst 2960	12.2(25)FX 以降	メンバまたはコマンド スイッチ
Catalyst 2955	12.1(12c)EA1 以降	メンバまたはコマンド スイッチ
Catalyst 2950	12.0(5.2)WC(1) 以降	メンバまたはコマンド スイッチ

表 6-1 スイッチ ソフトウェアおよびクラスタへの対応性 (続き)

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 2950 LRE	12.1(11)JY 以降	メンバまたはコマンドスイッチ
Catalyst 2940	12.1(13)AY 以降	メンバまたはコマンドスイッチ
Catalyst 3500 XL	12.0(5.1)XU 以降	メンバまたはコマンドスイッチ
Catalyst 2900 XL (8 MB スイッチ)	12.0(5.1)XU 以降	メンバまたはコマンドスイッチ
Catalyst 2900 XL (4 MB スイッチ)	11.2(8.5)SA6 (推奨)	メンバスイッチのみ
Catalyst 1900 および Catalyst 2820	9.00 (-A または -EN) 以降	メンバスイッチのみ

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS Release 12.2(40)EX 以降を実行している。
- IP アドレスが指定されている。
- Cisco Discovery Protocol (CDP) バージョン 2 がイネーブル (デフォルト) に設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。
- 管理 VLAN を介してスタンバイ クラスタ コマンド スイッチに、共通 VLAN を介してクラスタ メンバ スイッチに接続されている。

スタンバイ クラスタ コマンド スイッチの特性

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

- Cisco IOS 12.2(40)EX 以降を実行している。
- IP アドレスが指定されている。
- CDP バージョン 2 がイネーブルに設定されている。
- 管理 VLAN を介してコマンド スイッチに接続されていて、なおかつ他のスタンバイ コマンド スイッチに接続されている。
- 共通 VLAN を介して (クラスタ コマンド スイッチおよびスタンバイ コマンド スイッチを除く) 他のすべてのクラスタ メンバ スイッチに接続されている。
- クラスタ メンバ スイッチとの接続能力を維持するために、クラスタに冗長接続されている。
- 他のクラスタのコマンド スイッチまたはメンバ スイッチではない。

候補スイッチおよびクラスタ メンバ スイッチの特性

候補スイッチとは、クラスタ対応ですが、クラスタにまだ追加されていないスイッチを意味します。クラスタ メンバ スイッチは、スイッチ クラスタにすでに追加されているスイッチです。候補スイッチまたはクラスタ メンバ スイッチには必須ではありませんが、専用の IP アドレスおよびパスワードを指定できます (「IP アドレス」(P.6-14) および「パスワード」(P.6-15) を参照してください)。

クラスタに加入する候補スイッチは、次の要件を満たしている必要があります。

- クラスタ対応のソフトウェアが稼働している。
- CDP バージョン 2 がイネーブルに設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。
- **ip http server** グローバル コンフィギュレーション コマンドはスイッチで設定する必要があります。
- クラスタ スタンバイ グループが存在する場合、少なくとも 1 つの共通 VLAN を介して、すべてのスタンバイ クラスタ コマンド スイッチに接続されている。各スタンバイ クラスタ コマンド スイッチに対応する VLAN は、異なる場合があります。
- 少なくとも 1 つの共通 VLAN を介して、クラスタ コマンド スイッチに接続されている。



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

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

スイッチ クラスタのプランニング

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

- 「クラスタ候補およびクラスタ メンバの自動検出」(P.6-4)
- 「HSRP およびスタンバイ クラスタ コマンド スイッチ」(P.6-11)
- 「IP アドレス」(P.6-14)
- 「ホスト名」(P.6-14)
- 「パスワード」(P.6-15)
- 「SNMP コミュニティ ストリング」(P.6-15)
- 「TACACS+ および RADIUS」(P.6-15)
- 「LRE プロファイル」(P.6-16)

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

クラスタ候補およびクラスタ メンバの自動検出

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



(注)

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

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

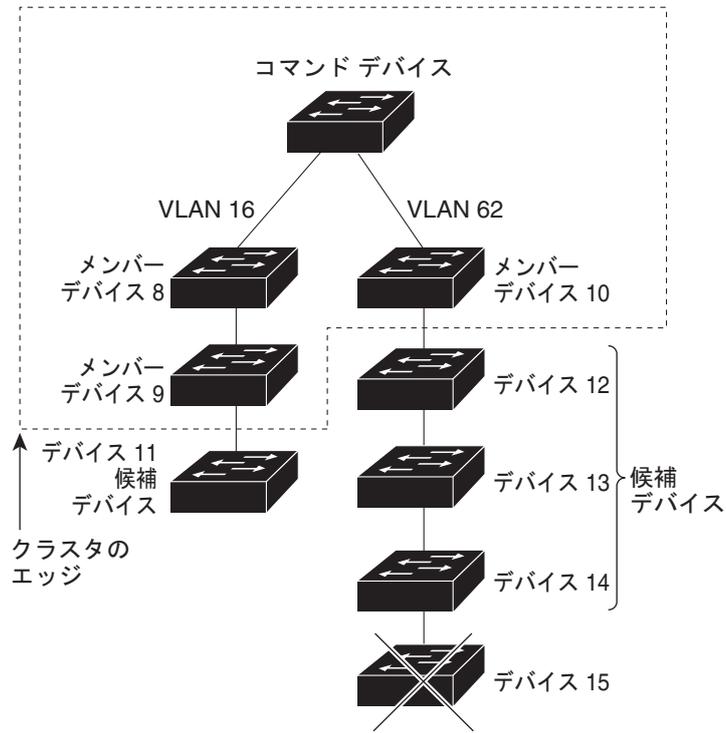
- 「CDP ホップを使用しての検出」(P.6-5)
- 「CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出」(P.6-7)
- 「異なる VLAN からの検出」(P.6-7)
- 「異なる管理 VLAN からの検出」(P.6-8)
- 「RP による検出」(P.6-9)
- 「新しく設置したスイッチの検出」(P.6-10)

CDP ホップを使用しての検出

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

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

図 6-1 CDP ホップを使用しての検出

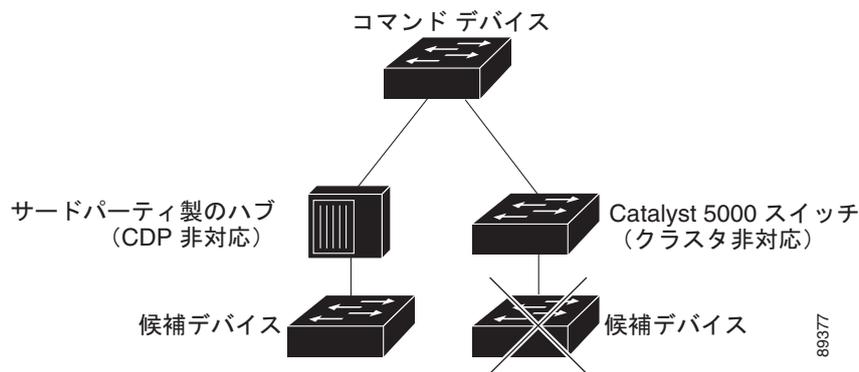


CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

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

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

図 6-2 CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

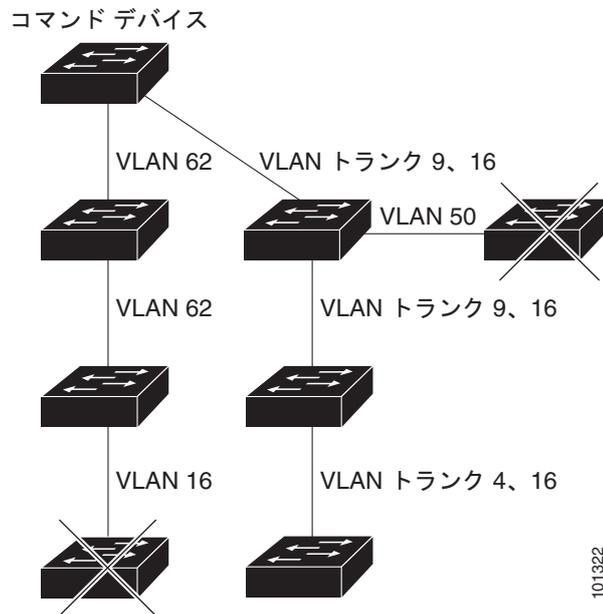


異なる VLAN からの検出

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

Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL のクラスタ メンバ スイッチは、それぞれの管理 VLAN を介してクラスタ コマンド スイッチに接続する必要があります。管理 VLAN からの検出については、「異なる管理 VLAN からの検出」(P.6-8) を参照してください。VLAN の詳細については、第 16 章「VLAN の設定」を参照してください。

図 6-3 異なる VLAN からの検出



異なる管理 VLAN からの検出

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



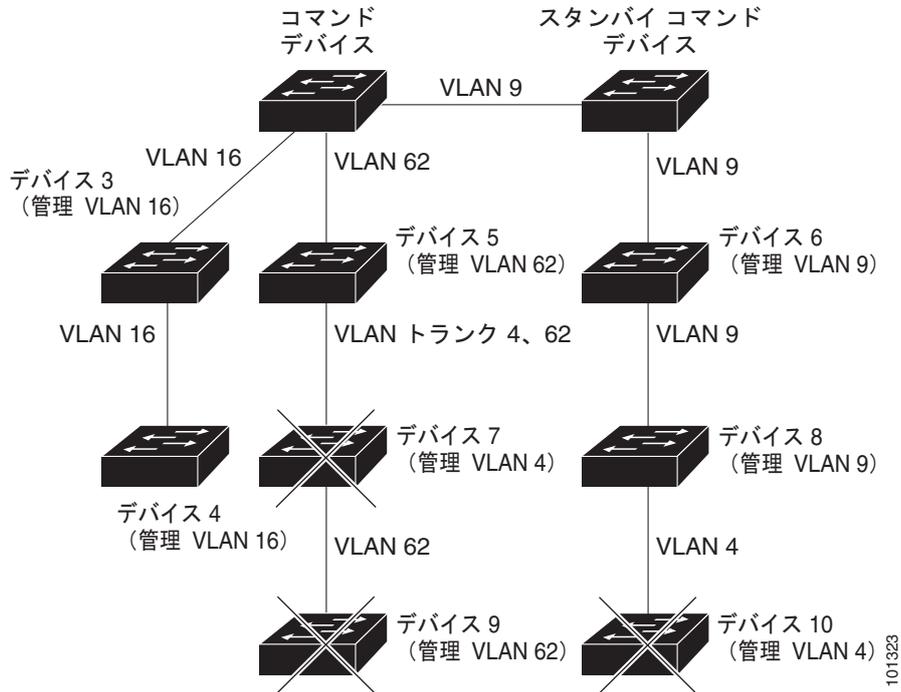
(注)

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

図 6-4 に示されているクラスタ コマンド スイッチおよびスタンバイ コマンド スイッチ (Catalyst 2960、Catalyst 2970、Catalyst 2975、Catalyst 3550、Catalyst 3560、Catalyst 3750 と想定します) のポートには、VLAN 9、16、および 62 が割り当てられています。クラスタ コマンド スイッチの管理 VLAN は VLAN 9 です。各クラスタ コマンド スイッチは、次の例外を除き、異なる管理 VLAN のスイッチを検出します。

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

図 6-4 レイヤ3 クラスタ コマンド スイッチを使用して異なる管理 VLAN から検出

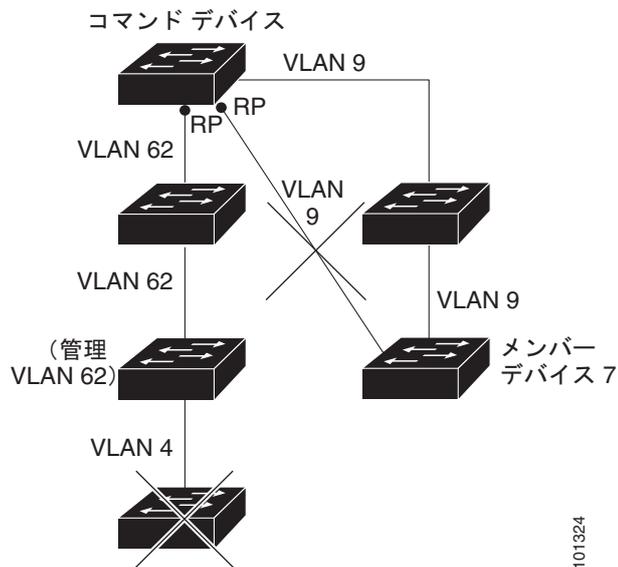


RP による検出

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

図 6-5 のレイヤ 3 クラスタ コマンド スイッチにより、VLAN 9 および 62 のスイッチは検出されますが、VLAN 4 のスイッチは検出されません。クラスタ コマンド スイッチとクラスタ メンバー スイッチ 7 間の RP パスが損失している場合、VLAN 9 を介する冗長パスがあるため、クラスタ メンバー スイッチ 7 との接続は維持されます。

図 6-5 RP による検出



101324

新しく設置したスイッチの検出

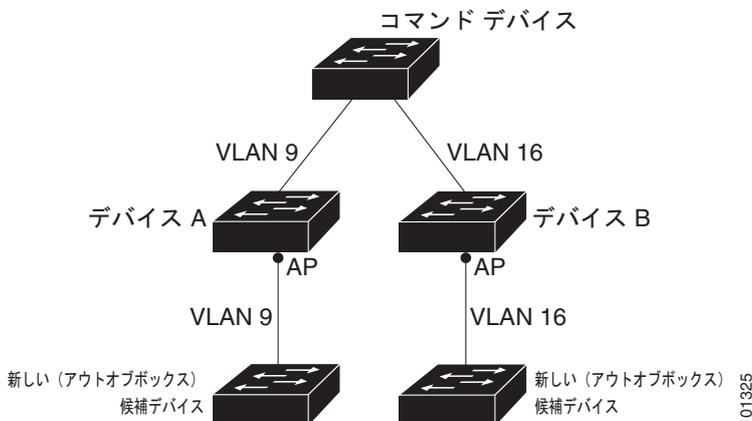
新しいアウトオブボックス スイッチをクラスタに加入させるには、アクセスポートの 1 つにクラスタを接続する必要があります。Access Port (AP; アクセス ポート) は 1 つの VLAN にのみ属し、そのトラフィックを転送します。デフォルトでは、新しいスイッチとそのアクセス ポートに対して VLAN 1 が割り当てられます。

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

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

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

図 6-6 新しく設置したスイッチの検出



101325

HSRP およびスタンバイ クラスタ コマンド スイッチ

スイッチはホットスタンバイ ルータ プロトコル (HSRP) をサポートしているためスタンバイ クラスタ コマンド スイッチのグループを設定できます。クラスタ コマンド スイッチは、すべての通信の転送と、すべてのクラスタ メンバ スイッチの設定情報を管理しているため、次のような環境設定を推奨します。

- クラスタ コマンドのスイッチ スタックには、スイッチ スタック全体に障害が発生する場合に備えて、スタンバイ クラスタ コマンド スイッチが必要です。ただし、コマンド スイッチのスタック マスターだけに障害が発生した場合は、スイッチ スタックで新しいスタック マスターを選出し、クラスタ コマンド スイッチ スタックとしての機能を引き継がせることができます。
- スタンドアロンのクラスタ コマンド スイッチの場合、プライマリ クラスタ コマンド スイッチの障害に備え、スタンバイ クラスタ コマンド スイッチを設定してその機能を引き継がせるようにします。

クラスタ スタンバイ グループは、「[スタンバイ クラスタ コマンド スイッチの特性](#)」(P.6-3) で説明している要件を満たしたコマンド対応スイッチのグループです。クラスタごとに、1つのクラスタ スタンバイ グループのみ割り当てることができます。



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

クラスタ スタンバイ グループのスイッチは、HSRP プライオリティに基づいてランク付けされています。グループ内でプライオリティの高いスイッチは、*Active Cluster Command Switch* (AC; アクティブ クラスタ コマンド スイッチ) です。グループ内で次にプライオリティの高いスイッチは、*Standby Cluster Command Switch* (SC; スタンバイ クラスタ コマンド スイッチ) です。クラスタ スタンバイ グループの他のスイッチは、*Passive Cluster Command Switch* (PC; パッシブ クラスタ コマンド スイッチ) です。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時にディセーブルになった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。自動検出の制限事項については、「[クラスタ設定の自動回復](#)」(P.6-13) を参照してください。HSRP プライオリティ値の変更については、「[HSRP のプライオリティの設定](#)」(P.46-8) を参照してください。クラスタ スタンバイ グループのメンバーおよびルータ冗長グループのメンバーのプライオリティの変更には、同じ HSRP **standby priority** インターフェイス コンフィギュレーション コマンドを使用します。



(注) HSRP のスタンバイ中止間隔は、hello タイム間隔の3倍以上必要です。デフォルトの HSRP スタンバイ中止間隔は10秒です。デフォルトの HSRP スタンバイ hello タイム インターバルは3秒です。スタンバイ中止間隔およびスタンバイ hello タイム間隔の詳細については、「[HSRP 認証およびタイマーの設定](#)」(P.46-11) を参照してください。

次の接続に関する注意事項に従って、スイッチ クラスタ、クラスタ候補、接続されたスイッチ クラスタ、ネイバー エッジ デバイスを自動検出してください。これらのトピックでもスタンバイ クラスタ コマンド スイッチの詳細について説明します。

- 「[仮想 IP アドレス](#)」(P.6-12)
- 「[クラスタ スタンバイ グループに関する他の考慮事項](#)」(P.6-12)
- 「[クラスタ設定の自動回復](#)」(P.6-13)

仮想 IP アドレス

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

アクティブ クラスタ コマンド スイッチに障害が発生すると、スタンバイ クラスタ コマンド スイッチが仮想 IP アドレスを使用して、アクティブ クラスタ コマンド スイッチになります。クラスタ スタンバイ グループのパッシブ スイッチは、それぞれ割り当てられたプライオリティを比較し、新しいスタンバイ クラスタ コマンド スイッチを選出します。その後、プライオリティの一番高いパッシブ スタンバイ スイッチがスタンバイ クラスタ コマンド スイッチになります。前回アクティブ クラスタ コマンド スイッチだったスイッチが再びアクティブになると、アクティブ クラスタ コマンド スイッチの役割を再開します。そのため、現在アクティブ クラスタ コマンド スイッチを担当しているスイッチは再びスタンバイ クラスタ コマンド スイッチになります。スイッチ クラスタの IP アドレスの詳細については、「IP アドレス」(P.6-14) を参照してください。

クラスタ スタンバイ グループに関する他の考慮事項

次の要件も満たす必要があります。

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

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

- クラスタごとに、1 つのクラスタ スタンバイ グループのみ割り当てることができます。ルータ冗長スタンバイ グループは複数作成できます。

1 つの HSRP グループをクラスタ スタンバイ グループとルータ冗長構成グループの両方にすることができます。ただし、ルータ冗長構成グループがクラスタ スタンバイ グループになった場合、そのグループ上でのルータ冗長構成はディセーブルになります。CLI を使用すれば、冗長構成を再びイネーブルにすることができます。HSRP およびルータ冗長構成の詳細については、第 46 章「HSRP および VRRP の設定」を参照してください。

- すべてのスタンバイグループ メンバはそのクラスタのメンバである必要があります。



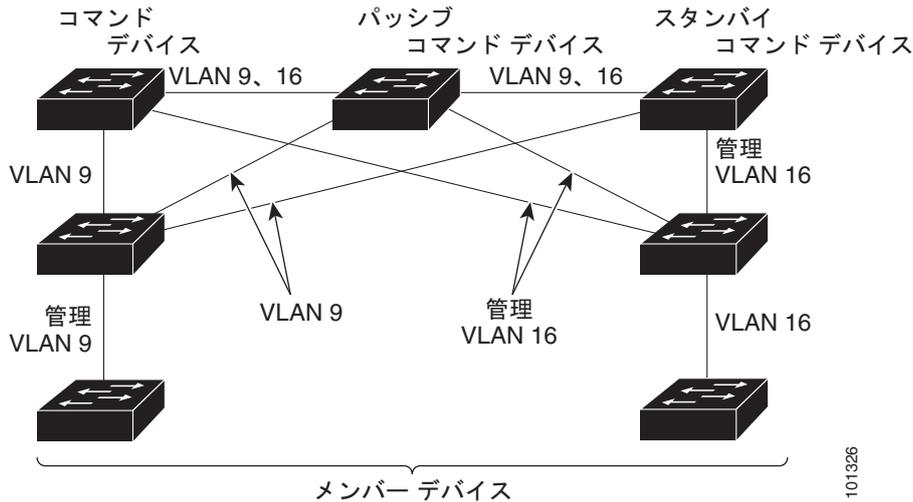
(注) スタンバイ クラスタ コマンド スイッチとして割り当てることができるスイッチ数に制限はありません。ただし、クラスタのスイッチの総数 (アクティブ クラスタ コマンド スイッチ、スタンバイ グループ メンバ、およびクラスタ メンバ スイッチを含む) は 16 以内にする必要があります。

- 各スタンバイグループのメンバ (図 6-7 を参照) は、同じ VLAN を介してクラスタ コマンド スイッチに接続されている必要があります。この例のクラスタ コマンド スイッチとスタンバイ クラスタ コマンド スイッチには Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 が該当します。各スタンバイグループのメンバも、スイッチ クラスタと同じ VLAN を最低 1 つは介在させて、冗長性を持たせながら相互接続する必要があります。

Catalyst 1900、Catalyst 2820、Catalyst 2900 XL、Catalyst 2950、Catalyst 3500 XL クラスタ メンバスイッチは、それぞれの管理 VLAN を介してクラスタ スタンバイ グループに接続する必要があります。スイッチ クラスタの VLAN の詳細については、次の各項を参照してください。

- 「異なる VLAN からの検出」(P.6-7)
- 「異なる管理 VLAN からの検出」(P.6-8)

図 6-7 スタンバイグループメンバとクラスタメンバ間の VLAN 接続



101926

クラスタ設定の自動回復

アクティブ クラスタ コマンド スイッチは、クラスタ設定情報をスタンバイ クラスタ コマンド スイッチに継続的に送信します (デバイス設定情報は送信しません)。アクティブ クラスタ コマンド スイッチに障害が発生した場合は、この情報をもとに、スタンバイ クラスタ コマンド スイッチが即座にクラスタを引き継ぎます。

自動検出には次のような制限があります。

- この制限は、Catalyst 2950、Catalyst 3550、Catalyst 3560、Catalyst 3750 のコマンド スイッチおよびスタンバイ クラスタ スイッチを含むクラスタのみに該当します。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時にディセーブルになった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。ただし、前回パッシブ スタンバイ クラスタ コマンド スイッチだったため、以前のクラスタ コマンド スイッチはクラスタ設定情報を送信していません。アクティブ クラスタ コマンド スイッチは、スタンバイ クラスタ コマンド スイッチにクラスタ設定情報のみ送信します。そのため、クラスタを再設定する必要があります。
- クラスタ スタンバイ グループに複数のスイッチを持つアクティブ クラスタ コマンド スイッチに障害が発生した場合、新しいクラスタ コマンド スイッチは、いかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL のクラスタ メンバ スイッチも検出しません。これらのクラスタ メンバ スイッチをクラスタにもう一度追加する必要があります。
- アクティブ クラスタ コマンド スイッチに障害が発生してダウンした後、再びアクティブになった場合、そのスイッチはいかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL クラスタ メンバ スイッチも検出しません。これらのクラスタ メンバ スイッチをクラスタにもう一度追加する必要があります。

以前アクティブ クラスタ コマンド スイッチだったスイッチが再びアクティブになった場合、そのスイッチは最新のクラスタ設定のコピー（ダウン中に追加されたメンバを含む）をアクティブ クラスタ コマンド スイッチから受信します。アクティブ クラスタ コマンド スイッチは、クラスタ スタンバイ グループにクラスタ設定のコピーを送信します。

IP アドレス

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

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

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

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

ホスト名

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

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

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

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

パスワード

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

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

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

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

SNMP コミュニティ スtring

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

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

クラスタコマンドスイッチに複数の Read-Only または Read-Write コミュニティ スtringがある場合、クラスタメンバスイッチには最初の Read-Only または Read-Write スtringのみ伝播されます。

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

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

TACACS+ および RADIUS

Terminal Access Controller Access Control System Plus (TACACS+) をクラスタメンバに設定する場合、すべてのクラスタメンバに設定する必要があります。同様に、RADIUS をクラスタメンバに設定する場合、すべてのクラスタメンバに設定する必要があります。また、TACACS+ を設定したメンバと RADIUS を設定した他のメンバを同じスイッチ クラスタには追加できません。

TACACS+ の詳細については、「[TACACS+ によるスイッチ アクセスの制御](#)」(P.11-11)を参照してください。RADIUS の詳細については、「[RADIUS によるスイッチ アクセスの制御](#)」(P.11-19)を参照してください。

LRE プロファイル

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

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

CLI によるスイッチ クラスタの管理

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

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

```
switch# rcommand 3
```

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

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

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

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

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

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



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

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

SNMP によるスイッチ クラスタの管理

スイッチの最初の起動時にセットアッププログラムを使用して IP 情報を入力し、提示されたコンフィギュレーションを採用した場合、SNMP はイネーブルに設定されています。セットアッププログラムを使用して IP 情報を入力していない場合は、SNMP はイネーブルではありません。その場合は、「SNMP の設定」(P.36-6) の説明に従って、SNMP をイネーブルに設定します。Catalyst 1900 および Catalyst 2820 スイッチでは、SNMP はデフォルトでイネーブルに設定されています。

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



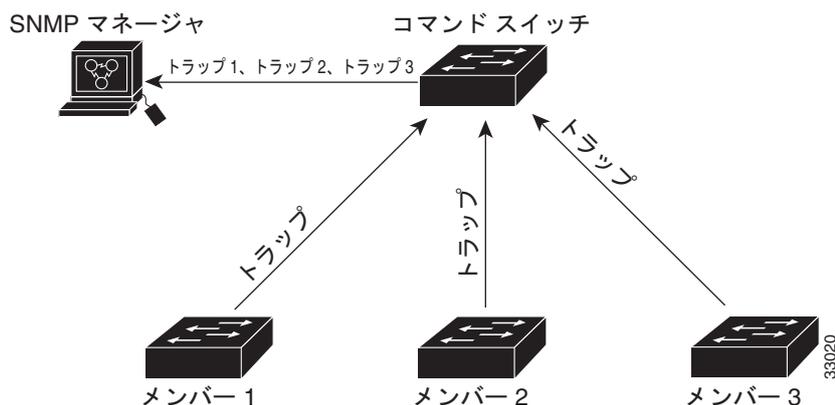
(注)

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

クラスタ メンバ スイッチに IP アドレスが割り当てられていない場合、図 6-8 に示すように、クラスタ コマンド スイッチはクラスタ メンバ スイッチからのトラップを管理ステーションにリダイレクトします。クラスタ メンバ スイッチに専用の IP アドレスおよびコミュニティ ストリングが割り当てられている場合、そのクラスタ メンバ スイッチはクラスタ コマンド スイッチを経由せず、管理ステーションに直接トラップを送信できます。

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

図 6-8 SNMP によるクラスタ管理





CHAPTER 7

スイッチの管理

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

- 「システム日時の管理」(P.7-1)
- 「システム名およびプロンプトの設定」(P.7-7)
- 「バナーの作成」(P.7-10)
- 「MAC アドレス テーブルの管理」(P.7-12)
- 「ARP テーブルの管理」(P.7-24)

システム日時の管理

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



(注)

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

ここでは、次の設定について説明します。

- 「システム クロックの概要」(P.7-1)
- 「NTP の概要」(P.7-2)
- 「NTP バージョン 4」(P.7-3)
- 「手動での日時の設定」(P.7-4)

システム クロックの概要

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

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

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

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

システム クロックは、時刻に**信頼性**があるかどうか (つまり、信頼できると見なされるタイムソースによって時刻が設定されているか) を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。設定の詳細については、「**手動での日時の設定**」(P.7-4) を参照してください。

NTP の概要

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

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

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

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

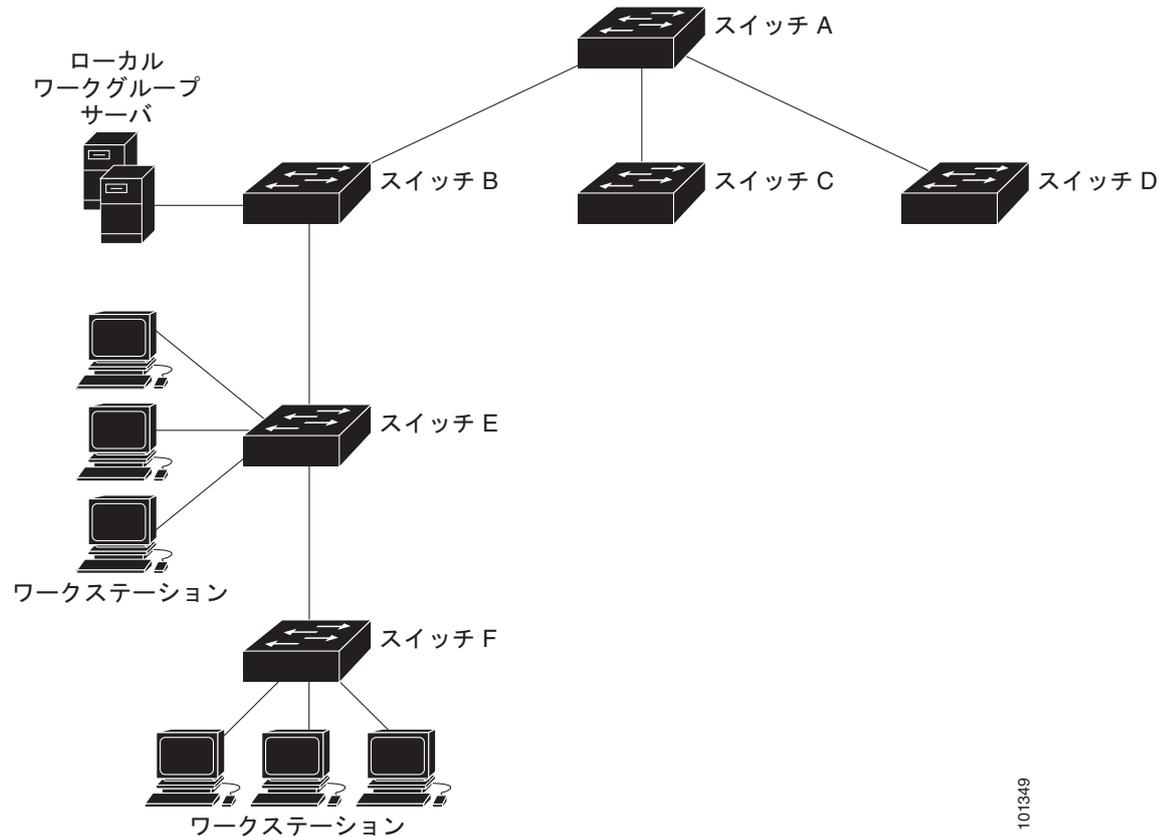
NTP が稼働するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られません。

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤ってあるいは意図的に設定されることを防止してください。アクセスリストを使用して制限する方式および暗号化認証メカニズムの、2 種類のメカニズムを使用できます。

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

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

図 7-1 一般的な NTP ネットワークの構成



101349

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

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

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

NTP バージョン 4

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

NTPv4 は次の互換性を提供します。

- IPv6 のサポート。

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

NTPv4 の設定の詳細については、『Cisco IOS IPv6 Configuration Guide, Release 12.4T』を参照してください。

手動での日時の設定

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

ここでは、次の設定について説明します。

- 「システム クロックの設定」(P.7-4)
- 「日時設定の表示」(P.7-5)
- 「タイム ゾーンの設定」(P.7-5)
- 「夏時間の設定」(P.7-6)

システム クロックの設定

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

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

コマンド	目的
ステップ1 <code>clock set hh:mm:ss day month year</code> または <code>clock set hh:mm:ss month day year</code>	次のいずれかの書式で、手動でシステム クロックを設定します。 <ul style="list-style-type: none"> • <code>hh:mm:ss</code> には、時刻を時間 (24 時間形式)、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • <code>day</code> には、当月の日付で日を指定します。 • <code>month</code> には、月を名前で指定します。 • <code>year</code> には、年を指定します (常に 4 桁で指定)。

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

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

日時設定の表示

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

システム クロックは、信頼性がある（正確であると信じられる）かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミグ ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていない場合は、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

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

タイム ゾーンの設定

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	clock timezone zone hours-offset [minutes-offset]	タイム ゾーンを設定します。 スイッチは内部時刻を UTC で管理するので、このコマンドは表示目的の場合および手動で時刻を設定した場合に限って使用します。 <ul style="list-style-type: none"> • <i>zone</i> には、標準時間が施行されているときに表示されるタイムゾーンの名前を入力します。デフォルトは UTC です。 • <i>hours-offset</i> には、UTC からの時差を入力します。 • (任意) <i>minutes-offset</i> には、UTC からの分差を入力します。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

夏時間の設定

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	clock summer-time zone recurring [<i>week day month hh:mm week day month</i> <i>hh:mm [offset]</i>]	毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで clock summer-time zone recurring を指定すると、夏時間のルールは米国のルールをデフォルトにします。 <ul style="list-style-type: none"> • <i>zone</i> には、夏時間が施行されているときに表示されるタイムゾーンの名前（たとえば PDT）を入力します。 • (任意) <i>week</i> には、月の何週目かを指定します（1～5、または last）。 • (任意) <i>day</i> には、曜日を指定します（Sunday、Monday など）。 • (任意) <i>month</i> には、月を指定します（January、February など）。 • (任意) <i>hh:mm</i> には、時刻を時間（24 時間形式）と分で指定します。 • (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルトは 60 です。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]] または clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]	最初の日付で夏時間開始の日付を、2 番目の日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 <ul style="list-style-type: none"> • zone には、夏時間が施行されているときに表示されるタイム ゾーンの名前（たとえば PDT）を入力します。 • (任意) week には、月の何週目かを指定します（1 ~ 5、または last）。 • (任意) day には、曜日を指定します（Sunday、Monday など）。 • (任意) month には、月を指定します（January、February など）。 • (任意) hh:mm には、時刻を時間（24 時間形式）と分で指定します。 • (任意) offset には、夏時間の間、追加する分の数を指定します。デフォルトは 60 です。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

システム名およびプロンプトの設定

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

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

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

ここでは、次の設定について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.7-8)
- 「システム名の設定」(P.7-8)
- 「DNS の概要」(P.7-8)

デフォルトのシステム名およびプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは *Switch* です。

システム名の設定

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

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

システム名を設定すると、システム プロンプトとしても使用されます。

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

DNS の概要

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

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

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

ここでは、次の設定について説明します。

- 「DNS のデフォルト設定」 (P.7-9)
- 「DNS の設定」 (P.7-9)
- 「DNS の設定の表示」 (P.7-10)

DNS のデフォルト設定

表 7-1 に、DNS のデフォルト設定を示します。

表 7-1 DNS のデフォルト設定

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

DNS の設定

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip domain-name name</code>	未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 起動時にはドメイン名は設定されていませんが、BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバからスイッチ コンフィギュレーションを取得している場合は、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（サーバにこの情報が設定されている場合）。
ステップ3	<code>ip name-server server-address1 [server-address2 ... server-address6]</code>	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。スイッチは、最初にプライマリ サーバに DNS クエリーを送信します。そのクエリーが失敗した場合は、バックアップ サーバにクエリーが送信されます。

	コマンド	目的
ステップ4	ip domain-lookup	(任意) スイッチ上で、DNS ベースのホスト名のアドレスへの変換をイネーブ ルにします。この機能は、デフォルトでイネーブにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワ ーク内のデバイスと接続する必要がある場合、グローバルなインターネットの ネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバ イス名を動的に割り当てることができます。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

DNS の設定の表示

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

バナーの作成

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

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



(注)

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

ここでは、次の設定について説明します。

- 「バナーのデフォルト設定」(P.7-11)
- 「MoTD ログイン バナーの設定」(P.7-11)
- 「ログイン バナーの設定」(P.7-12)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

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

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

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

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

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

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

次に、前の設定により表示されたバナーの例を示します。

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

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

User Access Verification

Password:
```

ログイン バナーの設定

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

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

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

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

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

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

MAC アドレス テーブルの管理

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

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

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



(注)

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

ここでは、次の設定について説明します。

- 「アドレス テーブルの作成」 (P.7-13)
- 「MAC アドレスおよび VLAN」 (P.7-13)
- 「MAC アドレス テーブルのデフォルト設定」 (P.7-14)
- 「アドレス エージング タイムの変更」 (P.7-14)
- 「ダイナミック アドレス エントリの削除」 (P.7-15)
- 「MAC アドレス変更通知トラップの設定」 (P.7-15)
- 「MAC アドレス移動通知トラップの設定」 (P.7-17)
- 「MAC しきい値通知トラップの設定」 (P.7-19)
- 「スタティック アドレス エントリの追加および削除」 (P.7-20)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.7-21)
- 「VLAN の MAC アドレス ラーニングのディセーブル化」 (P.7-22)
- 「アドレス テーブル エントリの表示」 (P.7-24)

アドレス テーブルの作成

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

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

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

MAC アドレスおよび VLAN

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

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

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

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

MAC アドレス テーブルのデフォルト設定

表 7-2 に、MAC アドレス テーブルのデフォルト設定を示します。

表 7-2 MAC アドレス テーブルのデフォルト設定

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

アドレス エージング タイムの変更

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

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

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

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

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

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

ダイナミック アドレス エントリの削除

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

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

MAC アドレス変更通知トラップの設定

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。<code>snmp-server host</code> コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、<code>snmp-server community</code> コマンドを使用し、次に <code>snmp-server host</code> コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ3	<code>snmp-server enable traps mac-notification change</code>	スイッチが MAC アドレス変更通知を NMS に送信できるようにします。
ステップ4	<code>mac address-table notification change</code>	MAC アドレス変更通知機能をイネーブルにします。
ステップ5	<code>mac address-table notification change [interval value] [history-size value]</code>	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> (任意) interval value には、NMS に対して生成される各トラップセット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。 (任意) history-size value には、MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ~ 500 です。デフォルトは 1 です。
ステップ6	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンド	目的
ステップ7	<code>snmp trap mac-notification change {added removed}</code>	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 <ul style="list-style-type: none"> MAC アドレスがインターフェイスに追加された (added) 場合にトラップをイネーブルにします。 MAC アドレスがインターフェイスから削除された (removed) 場合に MAC 通知トラップをイネーブルにします。
ステップ8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ9	<code>show mac address-table notification change interface</code> <code>show running-config</code>	設定を確認します。
ステップ10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

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

MAC アドレス移動通知トラップの設定

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。<code>snmp-server host</code> コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ3	<code>snmp-server enable traps mac-notification move</code>	スイッチが MAC アドレス移動通知トラップを NMS に送信できるようにします。
ステップ4	<code>mac address-table notification mac-move</code>	MAC アドレス移動通知機能をイネーブルにします。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show mac address-table notification mac-move</code> <code>show running-config</code>	設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

`show mac address-table notification mac-move` 特権 EXEC コマンドを入力すれば、設定を確認することができます。

MAC しきい値通知トラップの設定

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できませんが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ3	<code>snmp-server enable traps mac-notification threshold</code>	スイッチが MAC しきい値通知トラップを NMS に送信できるようにします。
ステップ4	<code>mac address-table notification threshold</code>	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ5	<code>mac address-table notification threshold [limit percentage] [interval time]</code>	<p>MAC アドレスしきい値の使用状況モニタのしきい値を入力します。</p> <ul style="list-style-type: none"> (任意) <code>limit percentage</code> に、MAC アドレス テーブルの使用率を指定します。有効値は 1 ~ 100% です。デフォルト値は 50% です。 (任意) <code>interval time</code> に、通知の間隔を指定します。有効値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show mac address-table notification threshold</code> <code>show running-config</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

show mac address-table notification threshold 特権 EXEC コマンドを入力すれば、設定を確認することができます。

スタティック アドレス エントリの追加および削除

スタティック アドレスには、次の特性があります。

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

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

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

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

プライベート VLAN のプライマリまたはセカンダリ VLAN 内にスタティック MAC アドレスを設定した場合、同じスタティック MAC アドレスをすべての関連 VLAN に設定する必要があります。プライベート VLAN のプライマリまたはセカンダリ VLAN に設定されたスタティック MAC アドレスは関連 VLAN には複製されません。プライベート VLAN の詳細については、[第 19 章「プライベート VLAN の設定」](#)を参照してください。

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mac address-table static mac-addr vlan vlan-id interface interface-id</code>	MAC アドレス テーブルにスタティック アドレスを追加します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。 <code>interface-id</code> には、受信したパケットの転送先インターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポートチャンネルです。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mac address-table static</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

ユニキャスト MAC アドレス フィルタリングの設定

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

この機能を使用する場合は、次の注意事項に従ってください。

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

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

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

- CPU に転送されるパケットもサポートされません。

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

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

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

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mac address-table static mac-addr vlan vlan-id drop</code>	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットをドロップするように設定します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットはドロップされます。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mac address-table static</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

VLAN の MAC アドレス ラーニングのディセーブル化

デフォルトでは、MAC アドレス ラーニングは、スイッチのすべての VLAN でイネーブルです。VLAN で MAC アドレス ラーニングを制御すると、MAC アドレスを学習できる VLAN、さらにポートを制御することで、利用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス

ラーニングをディセーブルにする前に、ネットワーク トポロジとスイッチ システム設定に詳しいことを確認してください。VLAN で MAC アドレス ラーニングをディセーブルにすると、ネットワークでフラッドিংを引き起こす可能性があります。

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

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

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

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

VLAN で MAC アドレス ラーニングを再びイネーブルにするには、**default mac address-table learning vlan vlan-id** グローバル コンフィギュレーション コマンドを使用します。**mac address-table learning vlan vlan-id** グローバル コンフィギュレーション コマンドを使用しても、VLAN で MAC ア

ドレス ラーニングを再びイネーブルにできます。最初の (**default**) コマンドを使用するとデフォルト状態に戻るため、**show running-config** コマンドからの出力に設定が表示されません。2 番目のコマンドを使用すると、**show running-config** 特権 EXEC コマンド出力に設定が表示されます。

次に、VLAN 200 で MAC アドレス ラーニングをディセーブルにする例を示します。

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

show mac-address-table learning [vlan vlan-id] 特権 EXEC コマンドを入力すると、すべての VLAN、または指定した VLAN の MAC アドレス ラーニングのステータスを表示できます。

アドレス テーブル エントリの表示

表 7-3 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 7-3 MAC アドレス テーブル表示用のコマンド

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

ARP テーブルの管理

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

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

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



(注)

CLI の手順の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] にある Cisco IOS Release 12.2 のマニュアルを参照してください。



CHAPTER 8

PTP の設定

- 「高精度時間プロトコルの概要」 (P.8-1)
- 「PTP の設定」 (P.8-2)
- 「PTP 設定の表示」 (P.8-4)

高精度時間プロトコルの概要

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

PTP ネットワークのクロックは、マスター/スレーブ階層で構成されています。グランドマスター クロックはベスト マスタークロック (BMC) と呼ばれ、マスター/スレーブ クロック階層のルートです。PTP は、マスタークロックとなる最も正確なクロックを持つデバイスに接続されたスイッチ ポートを識別する、BMC アルゴリズムを使用します。

マスタークロックは、グローバル ポジショニング システム (GPS) 時間からクロック ソースを受信します。スレーブは、マスタークロックに自分のクロックを同期する他のネットワーク デバイスです。親は、メンバのスレーブ クロックが同期するクロックです。マスタークロックとスレーブクロック間のタイミング メッセージは、継続的な同期を保証します。

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

境界モードのスイッチ クロックは、最も正確なマスター クロックの選択に参加します。より正確なクロックが検出されない場合、そのスイッチ クロックがマスター クロックになります。スレーブ クロック間でより正確なクロックが検出された場合、スイッチはそのクロックに同期し、スレーブ クロックになります。最初の同期のあと、スイッチと接続済み装置は、タイミング メッセージを交換して、クロックのオフセットとネットワークの遅延による時間の変更を修正します。

エンドツーエンド トランスペアレント モードのスイッチ クロックは、すべてのスイッチ ポートをマスター クロックに同期します。このスイッチは、マスター クロックの選択に参加せず、すべてのポートでデフォルト PTP クロック モードを使用します。

転送モードのスイッチ クロックにより、受信 PTP パケットがスイッチを通常のマルチキャスト トラフィックとしてパススルーできるようにします。

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

スイッチのグローバル コンフィギュレーションを実行することによって、PTP パススルー処理をイネーブルにできます。PTP パススルーをイネーブルにすると、すべての PTP メッセージは、パケットを受信する VLAN 内の拡張モジュールのポートとの間で受け渡されます。

PTP パススルー機能には、仮想ルーティングおよび転送 (VRF)、ポリシーベース ルーティング (PBR)、および PVLAN (プライベート仮想ローカル エリア ネットワーク) 機能との互換性はありません。

PTP の設定

- 「[デフォルト コンフィギュレーション](#)」 (P.8-2)
- 「[PTP の設定](#)」 (P.8-3)

デフォルト コンフィギュレーション

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

表 8-1 デフォルトの PTP 設定

機能	デフォルト設定
PTP 境界モード	ディセーブル
PTP 転送モード	ディセーブル
PTP エンドツーエンド トランスペアレント モード	イネーブル
PTP プライオリティ 1 および PTP プライオリティ 2	デフォルトのプライオリティ番号は 128 です。
PTP アナウンス間隔	2 秒
PTP アナウンス タイムアウト	8 秒
PTP 遅延要求間隔	32 秒
PTP 同期間隔	1 秒
PTP 同期制限	500000000 ナノ秒
PTP パススルー	ディセーブル

PTP の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ptp {mode {boundary e2transparent forward} priority1 value priority2 value passthrough}</code>	<p>同期クロックを指定します。</p> <ul style="list-style-type: none"> mode boundary : すべての接続デバイスに対するグラウンドマスター クロックおよび親クロックとして動作します。最も正確なマスター クロックの選択に参加するスイッチをイネーブルにします。 このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。 mode e2transparent (エンドツーエンド トランスペアレント) : すべてのスイッチ ポートをマスター クロックに同期化します。これがデフォルトのクロック モードです。 ジッタとエラーの累積を減らすには、このモードを使用します。 mode forward : 受信 PTP パケットが通常のマルチキャスト トラフィックとしてスイッチをパススルーすることを許可します。 スイッチ ポートが境界モードの場合に、クロック プライオリティのプロパティを指定します。 priority1 value : 最も正確なマスター クロックを選択するために、デフォルトの条件 (クロック品質、クロック クラスなど) を上書きします。低い値が優先されます。有効な範囲は 0 ~ 255 です。デフォルトは 128 です。 priority2 value : 2 つのスイッチがデフォルトの条件に一致する場合に、一方が選択されるようにします。たとえば、プライオリティ 2 値を使用して、同等のスイッチにスイッチ プライオリティを付与することができます。有効な範囲は 0 ~ 255 です。デフォルトは 128 です。 <p>PTP パススルー オプションを指定します。</p> <ul style="list-style-type: none"> passthrough : 拡張モジュール ポート上で PTP メッセージをイネーブルにします。 このオプションは、スイッチ ポートが境界モードまたはトランスペアレント モードの場合に使用できます。
ステップ3	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始します。

PTP 設定の表示

	コマンド	目的
ステップ 4	<code>ptp {announce {interval value timeout value} delay-req interval value enable sync {interval value limit value}}</code>	<p>タイミング メッセージの設定を指定します。これらのオプションは、スイッチが境界モードの場合にのみ使用できます。</p> <ul style="list-style-type: none"> • announce interval value : アナウンス メッセージを送信する時間を設定します。指定できる範囲は 0 ~ 4 秒です。デフォルトは 1 (2 秒) です。 • announce timeout value : タイムアウト メッセージをアナウンスする時間を設定します。指定できる範囲は 2 ~ 10 秒です。デフォルトは 3 (8 秒) です。 • delay-req interval value : ポートがマスター クロック状態の場合に、スレーブ デバイスが遅延要求メッセージを送信する時間を設定します。指定できる範囲は -1 ~ 6 秒です。デフォルトは 5 (32 秒) です。 • enable : ポート ベースのモジュールで PTP をイネーブルにします。 • sync interval value : 同期メッセージを送信する時間を設定します。入力できる範囲は -1 ~ 1 秒です。デフォルトは 1 秒です。 • sync limit value : PTP が再同期を試みるまでの、最大クロック オフセット値を設定します。範囲は 50 ~ 500000000 ナノ秒です。デフォルトは 500000000 ナノ秒です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

PTP 設定の表示

表 8-2 PTP 設定を表示するためのコマンド

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



CHAPTER 9

PROFINET の設定

この章では、Cisco IE 3000 スイッチで PROFINET 機能を設定する手順について説明します。

- 「PROFINET の概要」 (P.9-1)
- 「PROFINET の設定」 (P.9-4)
- 「PROFINET 設定の表示」 (P.9-5)
- 「PROFINET のトラブルシューティング」 (P.9-5)

PROFINET の概要

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

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



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

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

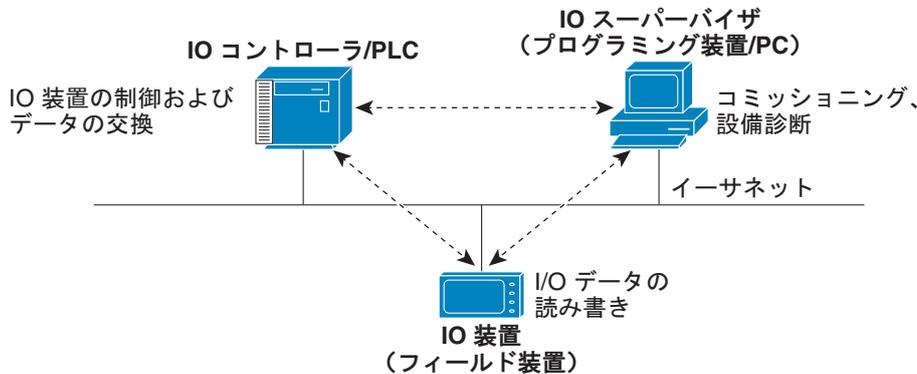
PROFINET IO は、次の 3 つのクラスの装置を認識します。

- IO 装置
- IO コントローラ
- IO スーパーバイザ

PROFINET 装置の役割

図 9-1 に、3 種類の装置の役割を示します。

図 9-1 PROFINET 装置の役割



276394

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

PROFINET は、唯一またはプライマリの管理システムとして使用するよう設計されています。IO コントローラは Discovery and Configuration Protocol (DCP; 検出/コンフィギュレーション プロトコル) でスイッチを検出し、装置名と IP アドレスを設定するため、基本的な設定に Cisco IOS コマンドは必要ありません。拡張設定 (QoS や DHCP などの機能) を行うには、スイッチ上で Cisco IOS コマンドを使用する必要があります。PROFINET を使用して、これらの機能の設定はできません。

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

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



(注)

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

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

PROFINET 装置のデータ交換

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

表 9-1 PROFINET IO スイッチ属性

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

表 9-2 PROFINET IO ポート属性

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

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

- 装置 ID 情報 (装置 ID、ベンダー ID およびベンダー名、製品ファミリー、ポート数)。
- 着脱可能モジュールの数およびタイプ。
- Cisco IE 3000 8 ポート拡張モジュールはホットスワップ可能ではありません。拡張モジュールの接続や切断を行う前に、スイッチをオフにしてください。
- 診断情報のエラー テキスト。
- IO 装置の通信パラメータ (最小サイクルタイム、リダクション比率、ウォッチ ドッグ タイムなど)。



(注) Cisco IE 3000 スイッチのデフォルトのリダクション比率は 128 ms ですが、スイッチに複雑な設定を使用する場合は、スイッチの CPU に対する負荷を減らすため、リダクション比率を 256 ms または 512 ms にすることを推奨します。

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

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



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

PROFINET の設定

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

- 「[デフォルト コンフィギュレーション](#)」 (P.9-4)
- 「[PROFINET のイネーブル化](#)」 (P.9-5)

デフォルト コンフィギュレーション

Cisco IOS ソフトウェア リリース 12.2(52)SE 以降、PROFINET はすべてのベース スイッチ モジュールおよび拡張ユニットのイーサネット ポート上で、デフォルトによりイネーブルになっています。PROFINET がディセーブルになっている場合は、「[PROFINET のイネーブル化](#)」 (P.9-5) の手順に従ってください。

PROFINET のイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>profinet</code>	スイッチ上で PROFINET をイネーブルにします。
ステップ3	<code>profinet id line</code>	(任意) Cisco IOS ソフトウェアを使用して PROFINET 装置 ID を設定します。 最大長は 240 文字です。使用可能な特殊文字はピリオド (.) とハイフン (-) のみです。これらの文字は ID 文字列内の特定のオプションでのみ使用可能です。文字列内には複数のラベルを含めることができます。各ラベルに使用できる文字数は 1 ~ 63 文字です。複数のラベルはピリオド (.) で区切る必要があります。文字列内の末尾文字はゼロ (0) にしないでください。 PROFINET ID の設定の詳細については、PROFINET の仕様、文書番号 TC2-06-0007a、ファイル名 PN-AL-protocol_2722_V22_Oct07 を参照してください (PROFIBUS から入手できます)。
ステップ4	<code>profinet vlan vlan id</code>	(任意) VLAN 番号を変更します。デフォルトの VLAN 番号は 1 です。指定できる VLAN ID の範囲は 1 ~ 4094 です。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show running-config</code>	入力内容を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチ上で PROFINET をディセーブルにするには、`no profinet` グローバル コンフィギュレーション コマンドを使用します。

PROFINET 設定の表示

`show profinet` 特権 EXEC コマンドを使用し、表 9-3 に示すキーワードのいずれかを指定します。

表 9-3 PROFINET の設定を表示するためのコマンド

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

PROFINET のトラブルシューティング

PLC の LED はアラームが発生すると赤になり、IO スーパーバイザのソフトウェアはこれらのアラームを反映します。

PROFINET のトラブルシューティングを行うには、`debug profinet` 特権 EXEC コマンドを使用し、表 9-4 に示すキーワードを指定します。`debug` コマンドの出力により、シリアルリンクにエラーが発生する可能性があるので注意してください。これらのコマンドを使用する際には、必ずシスコのテクニ

カル サポートのエンジニアの指示に従ってください。このコマンドの使用時には、シリアルポートではなくイーサネットを使用して、Telnet で Cisco IOS のコマンドライン インターフェイス (CLI) にアクセスしてください。

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

コマンド	目的
<code>debug profinet alarm</code>	アラーム ステータス (オンまたはオフ) と PROFINET アラームの内容を表示します。
<code>debug profinet cyclic</code>	タイム サイクル ベースの PROFINET イーサネット フレームに関する情報を表示します。
<code>debug profinet error</code>	PROFINET セッション エラーを表示します。
<code>debug profinet packet ethernet</code>	PROFINET イーサネット パケットに関する情報を表示します。
<code>debug profinet packet udp</code>	PROFINET Upper Layer Data Protocol (UDP) パケットに関する情報を表示します。
<code>debug profinet platform</code>	Cisco IOS と PROFINET 間の連携に関する情報を表示します。
<code>debug profinet topology</code>	受信した PROFINET トポロジ パケットを表示します。
<code>debug profinet trace</code>	追跡されたデバッグ出力ログのグループを表示します。



CHAPTER 10

SDM テンプレートの設定

SDM テンプレートの概要

Switch Database Management (SDM) テンプレートは、スイッチ上で特定の機能をサポートするために、システム ハードウェア リソースを割り当てます。特定の機能に関して、システム使用率を最大にする SDM テンプレートを選択できます。たとえば、デフォルトのテンプレートを使用してシステム リソースを均衡化し、LAN ベース ルーティング テンプレートを使用することにより、スイッチ仮想インターフェイス (SVI) 上のスタティック ルートの数を最大にできます。

SDM テンプレートを選択すると、次に示す機能を最大限にサポートできます。

- デフォルト：すべてのレイヤ 2 機能を均等に動作させます。
- LAN ベース ルーティング：スタティック ルーティング SVI を設定するための IPv4 ユニキャスト ルートをサポートします。
- デュアル IPv4/IPv6：IPv4 と IPv6 の両方のトラフィックをサポートするデュアル スタック環境でスイッチを使用できます。IPv4 トラフィックだけを転送する場合は、このテンプレートを使用すべきではありません。「[デュアル IPv4/IPv6 SDM テンプレート](#)」(P.10-2) を参照してください。
- QoS：Quality of Service (QoS) アクセス コントロール エントリ (ACE) のためのシステム リソースを最大にします。
- ルーティング：ルーティング テンプレートは、一般的に、ネットワークの中心にあるルータまたはアグリゲータが必要となります。IPv4 ユニキャスト ルーティングに対して、システム リソースを最大化します。ルーティング テンプレートを設定するには、スイッチ上で IP サービス イメージが稼働している必要があります。



(注)

スイッチでルーティング テンプレートを設定するには、Cisco IOS Release 12.2(52)SE 以降を実行している必要があります。

表 10-1 IPv4 テンプレートによって許容される機能リソースの概算

リソース	デフォルト	LAN ベース	QoS	ルーティング
ユニキャスト MAC アドレス	8 K	8 K	8 K	2 K
IGMP グループとマルチキャスト ルート	256	256	256	1 K
ユニキャスト ルート	0	750		4 K
• ホストに直接接続	0	750		2 K
• 間接ルート	0	16		2 K

表 10-1 IPv4 テンプレートによって許容される機能リソースの概算 (続き)

リソース	デフォルト	LAN ベース	QoS	ルーティング
ポリシーベース ルーティング ACE	0	0		512
QoS 分類 ACE	375	375	625	625
セキュリティの ACE	375	375	125	375
レイヤ 2 VLAN	1 K	1 K	1 K	1 K

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

デュアル IPv4/IPv6 SDM テンプレート

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

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



(注)

デュアル IPv4/IPv6 テンプレートは、IP サービス イメージを稼働しているスイッチ上でだけ使用できます。



(注)

このソフトウェア リリースは、IPv4 ポリシーベース ルーティング (PBR) だけをサポートします。IPv6 トラフィックの転送時は、PBR をサポートしません。

表 10-2 デュアル IPv4/IPv6 テンプレート¹によって許容される機能リソースの概算

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 のルーティング
ユニキャスト MAC アドレス	8 K	1 K
IPv4 IGMP グループおよびマルチキャスト ルート	0.25 K	0.5 K
IPv4 ユニキャスト ルートの合計	0	2 K
• IPv4 ホストに直接接続	0	1 K
• 間接 IPv4 ルート	0	1 K
IPv6 マルチキャスト グループ	0.375 K	0.625 K

表 10-2 デュアル IPv4/IPv6 テンプレート¹によって許容される機能リソースの概算 (続き)

リソース	IPv4 および IPv6 のデフォルト	IPv4 および IPv6 のルーティング
IPv6 ユニキャスト ルートの合計	0	1.375 K
• 直接接続された IPv6 アドレス	0	1 K
• 間接 IPv6 ユニキャスト ルート	0	0.375 K
IPv4 ポリシー ベース ルーティング ACE	0	0.125 K
IPv4 または MAC QoS ACE (合計)	0.375 K	0.375 K
IPv4 または MAC セキュリティの ACE (合計)	0.375 K	0.125 K
IPv6 ポリシー ベース ルーティング ACE ²	0	0.125 K
IPv6 QoS ACE	0	0.125 K
IPv6 セキュリティの ACE	0.125 K	0.125 K

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

スイッチ SDM テンプレートの設定

ここでは、次の設定について説明します。

- 「[デフォルトの SDM テンプレート](#)」 (P.10-3)
- 「[SDM テンプレートの設定時の注意事項](#)」 (P.10-3)
- 「[SDM テンプレートの設定](#)」 (P.10-4)

デフォルトの SDM テンプレート

デフォルト テンプレートは、デフォルトの SDM テンプレートです。

SDM テンプレートの設定時の注意事項

SDM テンプレートを選択および設定する場合は、次の注意事項に従ってください。

- SDM テンプレートの選択と設定を行う際、設定を有効にするため、スイッチをリロードする必要があります。
- ルーティングをサポートしていないレイヤ 2 スイッチング専用スイッチ上でのみ、**sdm prefer vlan** グローバル コンフィギュレーション コマンドを使用してください。VLAN テンプレートを使用する場合、システム リソースはルーティング エントリに予約されません。ルーティングはソフトウェアで実行されます。これにより、CPU は過負荷となり、ルーティング パフォーマンスは大幅に低下します。
- スイッチ上でルーティングがイネーブルになっていない場合、ルーティング テンプレートを使用しないでください。**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用して、他の機能にルーティング テンプレートのユニキャスト ルーティングに割り当てたメモリを使用させないようにします。

- IP サービス イメージをダウンロードして、レイヤ 3 機能を使用する場合は、ルーティング SDM テンプレートを使用する必要があります。
- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 機能を設定しようとする、警告メッセージが生成されます。
- デュアル IPv4/IPv6 テンプレートにより、各リソースに割り当てられる Ternary Content Addressable Memory (TCAM) がより少なくなります。これにより、ハードウェアで転送されるエントリ数が減少します。IPv4 トラフィックだけを転送する場合は、これらのテンプレートを使用しないでください。



(注) スイッチで lanbase-routing テンプレートを設定するには、Cisco IOS Release 15.0(2)SE 以降を実行している必要があります。

SDM テンプレートの設定

SDM テンプレートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>sdm prefer {default lanbase-routing dual-ipv4-and-ipv6 {default routing} qos routing}</code>	<p>スイッチで使用する SDM テンプレートを指定します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • default : すべての機能に均等にリソースを割り当てます。 • lanbase-routing : SVI 上で IPv4 スタティック ルーティングを設定するためのシステム リソースを最大化します。 • dual-ipv4-and-ipv6 : IPv4/IPv6 ルーティングの両方をサポートするテンプレートを選択します。 <ul style="list-style-type: none"> – default : IPv4/IPv6 のレイヤ 2 およびレイヤ 3 機能を均衡化します。 – routing : IPv4 ポリシーベース ルーティングを含む IPv4/IPv6 ルーティングを最大限に使用します。 • qos : QoS ACE 用のシステム リソースを最大にします。 • routing : スイッチでの IPv4 ルーティングを最大化します。 <p>スイッチをデフォルト テンプレートに設定するには、no sdm prefer コマンドを使用します。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>reload</code>	オペレーティング システムをリロードします。

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

次は、テンプレートを変更後にスイッチをリロードしなかった場合の出力表示の一例です。

```
Switch# show sdm prefer
```

```
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 1024 VLANs.
```

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

```
On next reload, template will be "routing" template.
```

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

次に、ルーティング テンプレートを持つスイッチの設定例を示します。

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

次に、スイッチ上でデフォルトのデュアル IPv4/IPv6 テンプレートを設定する例を示します。

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

SDM テンプレートの表示

アクティブ テンプレートを表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。

指定したテンプレートでサポートされているリソース数を表示するには、特権 EXEC コマンドで **show sdm prefer [default | dual-ipv4-and-ipv6 {default | routing} | qos | routing]** コマンドを使用します。

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

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

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

number of unicast mac addresses:          2K
  number of IPv4 IGMP groups + multicast routes: 1K
  number of IPv4 unicast routes:          4K
    number of directly-connected IPv4 hosts: 2K
    number of indirect IPv4 routes:        2K
  number of IPv4 policy based routing aces: 0.5K
  number of IPv4/MAC qos aces:            0.625k
  number of IPv4/MAC security aces:       0.375k
```




CHAPTER 11

スイッチ ベース認証の設定

この章では、IE 3000 スイッチでのスイッチベース認証の設定方法について説明します。この章で説明する内容は、次のとおりです。

- 「スイッチへの不正アクセスの防止」(P.11-1)
- 「特権 EXEC コマンドへのアクセスの保護」(P.11-2)
- 「TACACS+ によるスイッチ アクセスの制御」(P.11-11)
- 「RADIUS によるスイッチ アクセスの制御」(P.11-19)
- 「Kerberos によるスイッチ アクセスの制御」(P.11-41)
- 「スイッチのローカル認証および許可の設定」(P.11-46)
- 「SSH のためのスイッチの設定」(P.11-47)
- 「SSL HTTP のためのスイッチの設定」(P.11-51)
- 「SCP のためのスイッチの設定」(P.11-57)

スイッチへの不正アクセスの防止

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

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

- 最低限のセキュリティとして、各スイッチポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。詳細については、「[特権 EXEC コマンドへのアクセスの保護](#)」(P.11-2) を参照してください。
- 追加のセキュリティレイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユー

ザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。詳細については、「[ユーザ名とパスワードのペアの設定](#)」(P.11-7) を参照してください。

- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーク デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。詳細については、「[TACACS+ によるスイッチ アクセスの制御](#)」(P.11-11) を参照してください。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、次の URL の『Cisco IOS Login Enhancements』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

特権 EXEC コマンドへのアクセスの保護

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



(注)

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

ここでは、次の設定について説明します。

- 「[デフォルトのパスワードおよび権限レベル設定](#)」(P.11-3)
- 「[スタティック イネーブル パスワードの設定または変更](#)」(P.11-3)
- 「[暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護](#)」(P.11-4)
- 「[パスワード回復のディセーブル化](#)」(P.11-5)
- 「[端末回線に対する Telnet パスワードの設定](#)」(P.11-6)
- 「[ユーザ名とパスワードのペアの設定](#)」(P.11-7)
- 「[複数の権限レベルの設定](#)」(P.11-9)

デフォルトのパスワードおよび権限レベル設定

表 11-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 11-1 デフォルトのパスワードおよび権限レベル設定

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	enable password <i>password</i>	<p>特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>デフォルトでは、パスワードは定義されません。</p> <p><i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符 (?) は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。</p> <p>abc を入力します。</p> <p>Ctrl+v を入力します。</p> <p>?123 を入力します。</p> <p>システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p> <p>イネーブル パスワードは暗号化されず、スイッチのコンフィギュレーション ファイル内では読み取ることができる状態です。</p>

パスワードを削除するには、**no enable password** グローバル コンフィギュレーション コマンドを使用します。

次に、イネーブルパスワードを `11u2c3k4y5` に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password 11u2c3k4y5
```

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

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

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

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

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	enable password [level level] {password encryption-type encrypted-password} または enable secret [level level] {password encryption-type encrypted-password}	特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。 または シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。 <ul style="list-style-type: none"> （任意）<i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルトレベルは 15 です（特権 EXEC モード権限）。 <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できませんが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 （任意）<i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。 <p>(注) 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。</p>

	コマンド	目的
ステップ3	<code>service password-encryption</code>	(任意) パスワードを定義するとき、または設定を保存するときに、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したら、そのレベルでアクセスする必要のあるユーザだけにそのパスワードを渡してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「[複数の権限レベルの設定 \(P.11-9\)](#)」を参照してください。

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

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

次に、権限レベル 2 に対して暗号化パスワード `1FaD0$Xyti5Rkls3LoyxzS8` を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

パスワード回復のディセーブル化

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

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



(注)

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

ピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」(P.53-3) を参照してください。

パスワードの回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no service password-recovery	パスワードの回復をディセーブルにします。 この設定は、フラッシュ メモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show version	コマンド出力の最後の数行をチェックすることによって、設定を確認します。

パスワードの回復を再びイネーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。



(注)

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

端末回線に対する Telnet パスワードの設定

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

スイッチを Telnet アクセス用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアを備えた PC またはワークステーションとスイッチのコンソール ポートを接続します。 コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトが表示されるまで、Return キーを何回か押す必要があります。
ステップ 2	enable password <i>password</i>	特権 EXEC モードを開始します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ4	<code>line vty 0 15</code>	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ5	<code>password password</code>	1 つまたは複数の回線に対応する Telnet パスワードを入力します。 <i>password</i> には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できませんが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show running-config</code>	設定を確認します。 コマンド <code>line vty 0 15</code> の下にパスワードが表示されます。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

パスワードを削除するには、`no password` グローバル コンフィギュレーション コマンドを使用します。

次に、Telnet パスワードを `let45me67in89` に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

ユーザ名とパスワードのペアの設定

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

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムでは、ログインユーザ名とパスワードが要求されます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	username name [privilege level] { password encryption-type password }	各ユーザのユーザ名、権限レベル、パスワードを入力します。 <ul style="list-style-type: none"> <i>name</i> には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 (任意) <i>level</i> には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 <i>encryption-type</i> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 <i>password</i> には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 3	line console 0 または line vty 0 15	ライン コンフィギュレーション モードを開始し、コンソール ポート (回線 0) または VTY 回線 (回線 0 ~ 15) を設定します。
ステップ 4	login local	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、**no username name** グローバル コンフィギュレーション コマンドを使用します。パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアはデフォルトで、2 種類のパスワードセキュリティ モードを使用します。ユーザ EXEC および特権 EXEC です。モードごとに、コマンドの階層レベルを 16 まで設定できます。複数のパスワードを設定することにより、さまざまなユーザ グループに対して特定のコマンドへのアクセスを許可できます。

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

ここでは、次の設定について説明します。

- 「コマンドの権限レベルの設定」 (P.11-9)
- 「回線に対するデフォルトの権限レベルの変更」 (P.11-10)
- 「権限レベルへのログインおよび終了」 (P.11-11)

コマンドの権限レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	privilege mode level level command	コマンドの権限レベルを設定します。 <ul style="list-style-type: none"> • <i>mode</i> には、グローバル コンフィギュレーション モードの場合は configure を、EXEC モードの場合は exec を、インターフェイス コンフィギュレーション モードの場合は interface を、ライン コンフィギュレーション モードの場合は line をそれぞれ入力します。 • <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、enable パスワードによって許可されるアクセス レベルです。 • <i>command</i> には、アクセスを制限したいコマンドを指定します。
ステップ3	enable password level level password	権限レベルに対応するイネーブルパスワードを指定します。 <ul style="list-style-type: none"> • <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show running-config または show privilege	設定を確認します。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。 show privilege コマンドは、権限レベルの設定を表示します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

回線に対するデフォルトの権限レベルの変更

回線に対するデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	line vty line	アクセスを制限する仮想端末回線を選択します。
ステップ 3	privilege level level	回線のデフォルトの権限レベルを変更します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、 enable パスワードによって許可されるアクセス レベルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config または show privilege	設定を確認します。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。 show privilege コマンドは、権限レベルの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>enable level</code>	指定した権限レベルにログインします。 <i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ2	<code>disablelevel</code>	指定した権限レベルを終了します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

TACACS+ によるスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus (TACACS+) をイネーブルにして設定する方法について説明します。TACACS+ は、詳細なアカウント情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントing) 機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

Cisco IOS Release 12.2(58)SE 以降、スイッチは IPv6 対応の TACACS+ をサポートしています。この機能の設定については、『*Cisco IOS XE IPv6 Configuration Guide, Release 2*』の「Implementing ADSL for IPv6」の章を参照してください。



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

ここでは、次の設定について説明します。

- 「TACACS+ の概要」(P.11-11)
- 「TACACS+ の動作」(P.11-13)
- 「TACACS+ の設定」(P.11-14)
- 「TACACS+ 設定の表示」(P.11-19)

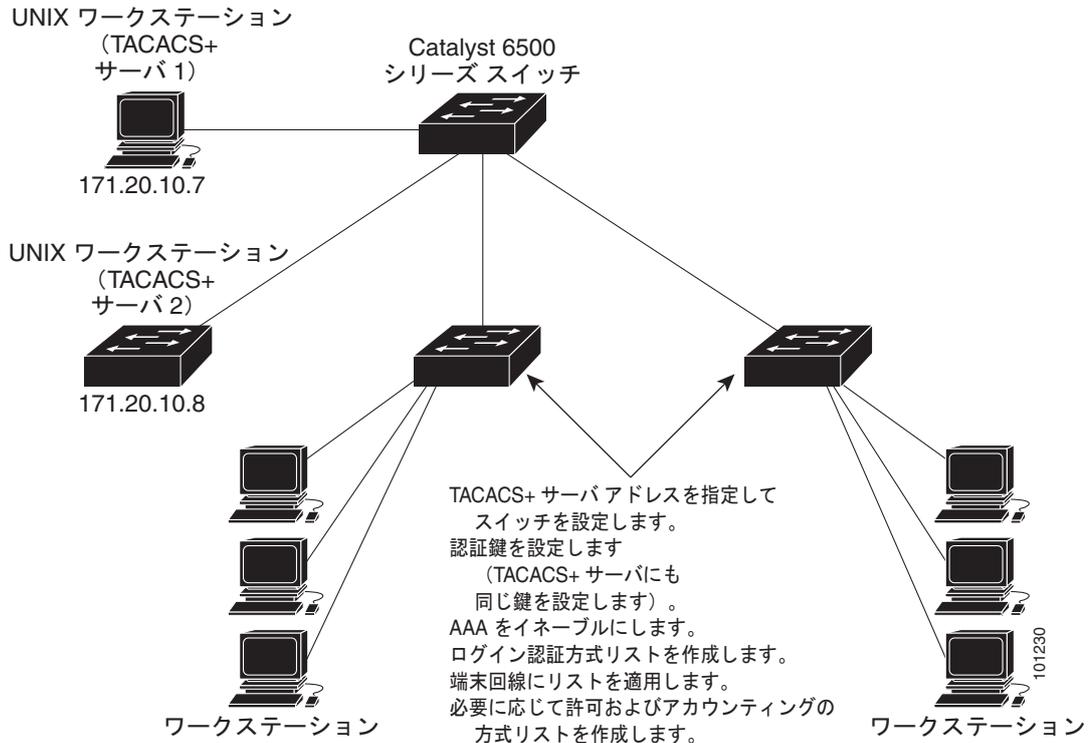
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、個別の、およびモジュールでの認証、認可、およびアカウントing機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ (TACACS+ デーモン) が各サービス (認証、許可、およびアカウントing) を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できません。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。ネットワーク アクセス サーバは、個々のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します (図 11-1 を参照)。

図 11-1 一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

認証機能は、ユーザとの対話を実行できます (たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを確認します)。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。
- 許可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザ セッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド (PPP など)、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワードプロンプトを取得します。スイッチによってパスワードプロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。
TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。
2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
 - **ACCEPT** : ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
 - **REJECT** : ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログインシーケンスを再試行するように求められます。
 - **ERROR** : デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。**ERROR** 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
 - **CONTINUE** : ユーザは、さらに認証情報の入力を求められます。認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが **ACCEPT** または **REJECT** の許可応答を返します。**ACCEPT** 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、**EXEC** または **NETWORK** セッション宛ての属性の形式でデータが含まれています。
 - Telnet、Secure Shell (SSH; セキュア シェル)、rlogin、または特権 EXEC サービス
 - 接続パラメータ (ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む)

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウントिंगの方式リストを定義することもできます。方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定について説明します。

- 「TACACS+ のデフォルト設定」(P.11-14)
- 「TACACS+ サーバ ホストの特定および認証キーの設定」(P.11-14)
- 「TACACS+ ログイン認証の設定」(P.11-15)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」(P.11-17)
- 「TACACS+ アカウンティングの起動」(P.11-18)

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されます。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。



(注) TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定および認証キーの設定

認証用に 1 つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 tacacs-server host <i>hostname</i> [<i>port integer</i>] [<i>timeout integer</i>] [<i>key string</i>]	TACACS+ サーバを維持する IP ホスト (1 つまたは複数) を特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <ul style="list-style-type: none"> <i>hostname</i> には、ホストの名前または IP アドレスを指定します。 (任意) port integer には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ~ 65535 です。 (任意) timeout integer には、スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチはタイムアウトしてエラーを宣言します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 秒です。 (任意) key string には、スイッチと TACACS+ デーモン間のすべてのトラフィックを暗号化および暗号解除するための暗号キーを指定します。暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。
ステップ3 aaa new-model	AAA をイネーブルにします。
ステップ4 aaa group server tacacs+ <i>group-name</i>	(任意) グループ名で AAA サーバグループを定義します。 このコマンドによって、スイッチはサーバグループサブコンフィギュレーションモードになります。
ステップ5 server <i>ip-address</i>	(任意) 特定の TACACS+ サーバを定義済みサーバグループに対応付けます。AAA サーバグループの各 TACACS+ サーバに対してこのステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ6 end	特権 EXEC モードに戻ります。
ステップ7 show tacacs	設定を確認します。
ステップ8 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host *hostname*** グローバル コンフィギュレーション コマンドを使用します。設定リストからサーバグループを削除するには、**no aaa group server tacacs+ *group-name*** グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server *ip-address*** サーバグループサブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト (偶然に *default* と名前が付けられている) です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためにクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • list-name には、作成するリストの名前として使用する文字列を指定します。 • method1... には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • enable : イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • group tacacs+ : TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバホストの特定および認証キーの設定」(P.11-14) を参照してください。 • line : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。password password ライン コンフィギュレーション コマンドを使用します。 • local : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。username password グローバル コンフィギュレーション コマンドを使用します。 • local-case : 大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。username name password グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • none : ログインに認証を使用しません。

	コマンド	目的
ステップ4	<code>line [console tty vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ5	<code>login authentication {default list-name}</code>	回線または回線セットに対して、認証リストを適用します。 <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • list-name には、aaa authentication login コマンドで作成したリストを指定します。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show running-config</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login {default | list-name} method1 [method2...]** グローバル コンフィギュレーション コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするかデフォルト値に戻す場合は、**no login authentication {default | list-name}** ライン コンフィギュレーション コマンドを使用します。



(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Security Command Reference, Release 12.2』を参照してください。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 認証によってユーザが利用できるサービスが制限されます。AAA 認証がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドに **tacacs+** キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



(注)

許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization network tacacs+	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可を、スイッチに設定します。
ステップ 3	aaa authorization exec tacacs+	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ TACACS+ 許可をスイッチに設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization {network | exec} method1** グローバル コンフィギュレーション コマンドを使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa accounting network start-stop tacacs+	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	aaa accounting exec start-stop tacacs+	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting {network | exec} {start-stop} method1...** グローバル コンフィギュレーション コマンドを使用します。

AAA サーバが到達不能な場合のルータとのセッションの確立

`aaa accounting system guarantee-first` コマンドは、システム アカウンティングが最初のレコードになることを保証します。これはデフォルトの状態です。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、`no aaa accounting system guarantee-first` コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、`show tacacs` 特権 EXEC コマンドを使用します。

RADIUS によるスイッチ アクセスの制御

ここでは、RADIUS をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は、AAA を介して実装され、AAA コマンドを使用するのみイネーブルにできます。

Cisco IOS Release 12.2(58)SE 以降、スイッチは IPv6 対応の RADIUS をサポートしています。この機能の設定については、『[Cisco IOS XE IPv6 Configuration Guide, Release 2](#)』の「Implementing ADSL for IPv6」を参照してください。



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

ここでは、次の設定について説明します。

- 「RADIUS の概要」 (P.11-19)
- 「RADIUS の動作」 (P.11-21)
- 「RADIUS 許可の変更」 (P.11-21)
- 「RADIUS の設定」 (P.11-28)
- 「RADIUS の設定の表示」 (P.11-41)

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。RADIUS ホストは、通

常、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

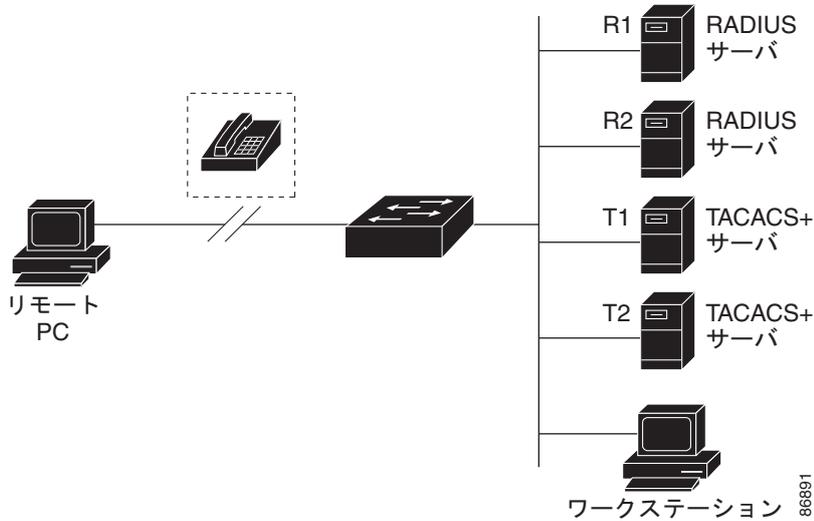
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カードアクセス コントロール システムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースへのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備の Cisco スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。図 11-2 (P.11-21) を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 12 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース (時間、パケット、バイトなど) の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できません。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

図 11-2 RADIUS サービスから TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス コントロールされるスイッチに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは RADIUS サーバから、次のいずれかの応答を受信します。
 - a. ACCEPT : ユーザが認証されたことを表します。
 - b. REJECT : ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が必要されるか、またはアクセスが拒否されます。
 - c. CHALLENGE : ユーザに追加データを要求します。
 - d. CHALLENGE PASSWORD : ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります (イネーブルに設定されている場合)。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ (ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む)

RADIUS 許可の変更

ここでは、使用可能なプリミティブおよびそれらの Change of Authorization (CoA) での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- 「概要」 (P.11-22)
- 「Change-of-Authorization 要求」 (P.11-22)

- 「CoA 要求応答コード」 (P.11-24)
- 「CoA 要求コマンド」 (P.11-25)
- 「セッション再認証」 (P.11-25)

概要

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。Catalyst スイッチは、通常プッシュ モデルで使用される RFC 5176 で規定された RADIUS Change of Authorization (CoA) 拡張機能をサポートし、外部の認証、許可、およびアカウントिंग (AAA) またはポリシーサーバからのセッションのダイナミック再設定ができるようにします。

Cisco IOS Release 12.2(52)SE 以降では、これらのセッションごとの CoA 要求がスイッチにサポートされています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。ACS の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html

Catalyst スイッチで、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、一部の基本的な設定では次の属性が必要です。

- セキュリティおよびパスワード : 『*Catalyst 3750 Switch Software Configuration Guide, Cisco Release 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「[Preventing Unauthorized Access to Your Switch](#)」を参照してください。
- アカウントिंग : 『*Catalyst 3750 Switch Software Configuration Guide 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「[Starting RADIUS Accounting](#)」を参照してください。

Change-of-Authorization 要求

Change of Authorization (CoA) 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用するによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求 (CoA-Request) と 2 つの可能な応答コードで構成されています。

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA non-acknowledgement (NAK) [CoA-NAK]

要求は CoA クライアント (通常は RADIUS またはポリシー サーバ) から発信されて、リスナーとして動作するスイッチに送信されます。

ここでは、次の内容について説明します。

- [CoA 要求応答コード](#)
- [CoA 要求コマンド](#)
- [セッション再認証](#)

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect (POD) と呼ばれますが、セッション終了に対してスイッチでサポートされています。

表 11-2 には、この機能でサポートされている IETF 属性を示します。

表 11-2 サポートされている IETF 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 11-3 には、Error-Cause 属性で取ることができる値を示します。

表 11-3 Error-Cause の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット (無視)
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求 (プロキシ)
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされていない

前提条件

CoA インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。サポートされているコマンドを表 11-4 (P.11-25) に示します。

セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Calling-Station-Id (ホストの MAC アドレスを含む IETF 属性 31)
- Audit-Session-Id VSA (シスコの Vendor-Specific Attribute (VSA; ベンダー固有属性))
- Acct-Session-Id (IETF 属性 44)

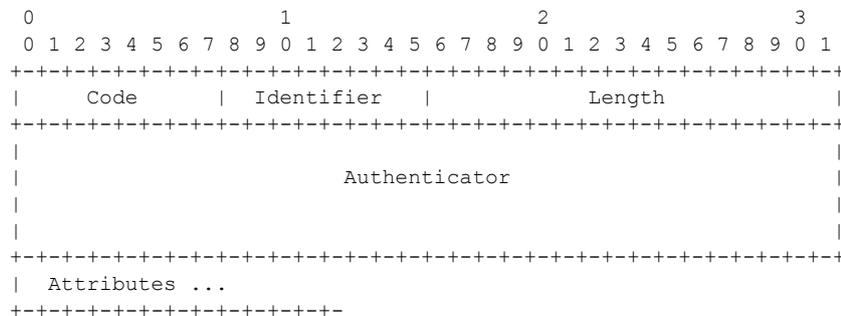
CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しないかぎり、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

特定のセッションに対する接続解除および CoA 要求の場合、次のいずれかのセッション ID を使用できます。

- Calling-Station-ID (MAC アドレスを含む IETF 属性 31)
- Audit-Session-ID (シスコのベンダー固有属性)
- Accounting-Session-ID (IETF 属性 44)

メッセージに複数のセッション ID 属性が含まれる場合、すべての属性がセッションと一致する必要があります。一致しない場合は、スイッチが「Invalid Attribute Value」エラー コードを含む Disconnect-Negative Acknowledgement (NAK; 否定確認応答) または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、および Type Length Value (TLV; タイプ、長さ、値) 形式の属性から構成されます。



属性フィールドは、Cisco Vendor-Specific Attribute (VSA; ベンダー固有属性) を送信するために使用します。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答 (ACK) が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定確認応答 (NAK) は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

この項では、次の内容について説明します。

- セッション再認証
- セッションの終了
- CoA 接続解除要求
- CoA 要求：ホスト ポートのディセーブル化
- CoA 要求：バウンス ポート

Cisco IOS Release 12.2(52)SE 以降では、表 11-4 に示されるコマンドがスイッチにサポートされています。

表 11-4 スイッチでサポートされる CoA コマンド

コマンド ¹	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があります。

セッション再認証

不明な ID またはポストチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは

Cisco:Avpair="subscriber:command=reauthenticate" の形式でシスコのベンダー固有属性（VSA）と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは Extensible Authentication Protocol over LAN (EAPOL; LAN 経由の拡張認証プロトコル) RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC Authentication Bypass (MAB; MAC 認証バイパス) で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されていない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホストポートをディセーブルにせずセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステート マシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、

`Cisco:Avpair="subscriber:command=disable-host-port"` VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサブリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホストポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。このコマンドはセッション指向であるため、「[セッションの識別](#)」(P.11-24) で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは `Disconnect-NAK` メッセージと「`Session Context Not Found`」エラー コード属性を返します。セッションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるたびに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、`Disconnect-ACK` と「`Session Context Not Found`」エラー コード属性が送信されます。

CoA 要求 : ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

このコマンドはセッション指向であるため、「[セッションの識別](#)」(P.11-24) で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合は、`CoA-NAK` メッセージと「`Session Context Not Found`」エラー コード属性が返されます。このセッションがある場合は、スイッチはホストポートをディセーブルにし、`CoA-ACK` メッセージを返します。

スイッチが `CoA-ACK` をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるたびに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが `CoA-ACK` メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。



(注)

再送信コマンドの後に接続解除要求が失敗すると、(接続解除 ACK が送信されていない場合に) チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

CoA 要求 : バウンス ポート

このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

このコマンドはセッション指向であるため、「セッションの識別」(P.11-24) で示される 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合は、CoA-NAK メッセージと「Session Context Not Found」エラー コード属性が返されます。このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし (ポート バウンス)、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるたびに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

RADIUS の設定

ここでは、スイッチが RADIUS をサポートするように設定する方法について説明します。最低限、RADIUS サーバソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウントिंगの方式リストを定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコル（TACACS+、ローカル ユーザ名検索など）を 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合は、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。

- 「RADIUS のデフォルト設定」(P.11-28)
- 「RADIUS サーバ ホストの識別」(P.11-29) (必須)
- 「RADIUS ログイン認証の設定」(P.11-31) (必須)
- 「AAA サーバ グループの定義」(P.11-33) (任意)
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」(P.11-35) (任意)
- 「RADIUS アカウントिंगの起動」(P.11-36) (任意)
- 「すべての RADIUS サーバの設定」(P.11-37) (任意)
- 「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(P.11-37) (任意)
- 「ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定」(P.11-39) (任意)
- 「スイッチ上での CoA の設定」(P.11-40)
- 「CoA 機能のモニタリングおよびトラブルシューティング」(P.11-41)
- 「RADIUS サーバ ロード バランシングの設定」(P.11-41) (任意)

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバホストの識別

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー ストリング
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー） ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。スイッチと通信するすべての RADIUS サーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。



(注)

スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、「[すべての RADIUS サーバの設定](#)」(P.11-37) を参照してください。

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。詳細については、「[AAA サーバ グループの定義](#)」(P.11-33) を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> • (任意) <code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。 • (任意) <code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。 • (任意) <code>timeout seconds</code> には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。 <code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。 • (任意) <code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。 • (任意) <code>key string</code> には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 <p>(注) <code>key</code> は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。キーは常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、<code>key</code> の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーをそれぞれ設定してください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、`no radius-server host {hostname | ip-address}` グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウント用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
```

```
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウントングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```



(注) RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ3 <code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。 • <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> - enable : イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 - group radius : RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別」(P.11-29) を参照してください。 - line : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。password password ライン コンフィギュレーション コマンドを使用します。 - local : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。username name password グローバル コンフィギュレーション コマンドを使用します。 - local-case : 大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。username password グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 - none : ログインに認証を使用しません。
ステップ4 <code>line [console tty vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ5 <code>login authentication {default list-name}</code>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • <i>list-name</i> には、aaa authentication login コマンドで作成したリストを指定します。
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ7 <code>show running-config</code>	設定を確認します。
ステップ8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login {default | list-name} method1 [method2...]** グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication {default | list-name}** ライン コンフィギュレーション コマンドを使用します。



(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Security Command Reference, Release 12.2』を参照してください。

AAA サーバ グループの定義

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意的 ID (IP アドレスと UDP ポート番号の組み合わせ) を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス (たとえばアカウントिंग) を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> （任意）<code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。 （任意）<code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。 （任意）<code>timeout seconds</code> には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。 （任意）<code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。 （任意）<code>key string</code> には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 <p>(注) <code>key</code> は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。キーは常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、<code>key</code> の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーをそれぞれ設定してください。</p>
ステップ 3	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa group server radius group-name</code>	<p>AAA サーバ グループを、特定のグループ名で定義します。</p> <p>このコマンドを使用すると、スイッチはサーバ グループ コンフィギュレーション モードになります。</p>
ステップ 5	<code>server ip-address</code>	<p>特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。</p> <p>グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定を確認します。

コマンド	目的
ステップ8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ9	RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」(P.11-31) を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host {hostname | ip-address}** グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server radius group-name** グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ (*group1* および *group2*) を認識するようにスイッチを設定しています。*group1* では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 認証によってユーザが利用できるサービスが制限されます。AAA 認証をイネーブルにすると、スイッチは (ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する) ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定するには、**radius** キーワードを指定して **aaa authorization** グローバル コンフィギュレーション コマンドを使用します。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注)

許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、スイッチに設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可を、スイッチに設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop radius</code>	ネットワーク関連のすべてのサービス要求について、RADIUS アカウンティングをイネーブルにします。
ステップ 3	<code>aaa accounting exec start-stop radius</code>	RADIUS アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止アカウンティング通知を送信するように設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、`no aaa accounting {network | exec} {start-stop} method1...` グローバル コンフィギュレーション コマンドを使用します。

AAA サーバが到達不能な場合のルータとのセッションの確立

`aaa accounting system guarantee-first` コマンドは、システム アカウンティングが最初のレコードになることを保証します。これはデフォルトの状態です。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、`no aaa accounting system guarantee-first` コマンドを使用します。

すべての RADIUS サーバの設定

スイッチとすべての RADIUS サーバ間でグローバルに通信を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server key string</code>	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。 (注) key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 3	<code>radius-server retransmit retries</code>	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 4	<code>radius-server timeout seconds</code>	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間 (秒) を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 です。
ステップ 5	<code>radius-server deadtime minutes</code>	認証要求に応答しない RADIUS サーバをスキップする時間 (分) を指定し、要求がタイムアウトするまで待機することなく、次に設定されているサーバを試行できるようにします。デフォルトは 0 です。指定できる範囲は 0 ~ 1440 分です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定値を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数、タイムアウト、および待機時間の設定をデフォルトに戻すには、これらのコマンドの `no` 形式を使用します。

ベンダー固有の RADIUS 属性を使用するスイッチ設定

Internet Engineering Task Force (IETF) ドラフト規格に、ベンダー固有の属性 (属性 26) を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨される

フォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダー タイプ 1 (名前は *cisco-avpair*) です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の許可タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な Attribute Value (AV; 属性値) ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 許可で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアを指定すると、IP 許可時 (PPP の IPCP アドレスの割り当て時) に、シスコの複数の名前付き IP アドレス プール機能が有効になります。

```
cisco-avpair= "ip:addr-pool=first"
```

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバ データベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-id(#81)=vlanid"
```

次に、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

スイッチが VSA を認識して使用するようには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server vsa send [accounting authentication]</code>	<p>スイッチが VSA (RADIUS IETF 属性 26 で定義) を認識して使用できるようにします。</p> <ul style="list-style-type: none"> (任意) 認識されるベンダー固有属性の集合をアカウント属性だけに限定するには、accounting キーワードを使用します。 (任意) 認識されるベンダー固有属性の集合を認証属性だけに限定するには、authentication キーワードを使用します。 <p>キーワードを指定せずにこのコマンドを入力すると、アカウントおよび認証のベンダー固有属性の両方が使用されます。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定値を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) RADIUS 属性の詳細なリストまたはベンダー固有属性 26 の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Security Configuration Guide, Release 12.2』の付録「RADIUS Attributes」を参照してください。

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバ デーモンが稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト スtring を指定する必要があります。RADIUS ホストおよびシークレット テキスト スtring を指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト スtring を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host {hostname ip-address} non-standard	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、そのホストが、ベンダーが独自に実装した RADIUS を使用していることを指定します。
ステップ 3	radius-server key string	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト スtring を指定します。スイッチおよび RADIUS サーバは、このテキスト スtring を使用して、パスワードの暗号化および応答の交換を行います。 (注) key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定値を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、**no radius-server host {hostname | ip-address} non-standard** グローバル コンフィギュレーション コマンドを使用します。キーをディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次に、ベンダー独自仕様の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* という秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

スイッチ上での CoA の設定

スイッチ上で CoA を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。
ステップ 3	aaa server radius dynamic-author	スイッチを認証、許可、およびアカウントिंग (AAA) サーバに設定し、外部ポリシーサーバとの相互作用を実行します。
ステップ 4	client {ip-address name} [vrf vrfname] [server-key string]	ダイナミック認証ローカル サーバ コンフィギュレーション モードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 5	server-key [0 7] string	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	port port-number	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 7	auth-type {any all session-key}	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 8	ignore session-key	(任意) セッション キーを無視するようにスイッチを設定します。 ignore コマンドの詳細については、Cisco.com の『 Cisco IOS Intelligent Services Gateway Command Reference 』を参照してください。
ステップ 9	ignore server-key	(任意) サーバ キーを無視するようにスイッチを設定します。 ignore コマンドの詳細については、Cisco.com の『 Cisco IOS Intelligent Services Gateway Command Reference 』を参照してください。
ステップ 10	authentication command bounce-port ignore	(任意) CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサブリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 11	authentication command disable-port ignore	(任意) セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにスイッチを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 12	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 13	<code>show running-config</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。スイッチ上の AAA サーバ機能をディセーブルにするには、`no aaa server radius dynamic authorization` グローバル コンフィギュレーション コマンドを使用します。

CoA 機能のモニタリングおよびトラブルシューティング

次の Cisco IOS コマンドを使用して、スイッチ上の CoA 機能をモニタおよびトラブルシューティングします。

- `debug radius`
- `debug aaa coa`
- `debug aaa pod`
- `debug aaa subsys`
- `debug cmdhd [detail | error | events]`
- `show aaa attributes protocol radius`

RADIUS サーバ ロード バランシングの設定

この機能を使用すると、アクセス要求および認証要求を、サーバ グループ内のすべての RADIUS サーバに対して均等に送信できます。詳細については、『Cisco IOS Security Configuration Guide, Release 12.2』の「RADIUS Server Load Balancing」の章を参照してください。URL は次のとおりです。
http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrldbl.html

RADIUS の設定の表示

RADIUS の設定を表示するには、`show running-config` 特権 EXEC コマンドを使用します。

Kerberos によるスイッチ アクセスの制御

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。この機能を使用するには、スイッチにスイッチ ソフトウェアの暗号化バージョンをインストールする必要があります。

この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「Kerberos の概要」 (P.11-42)
- 「Kerberos の動作」 (P.11-44)
- 「Kerberos の設定」 (P.11-45)

Kerberos の設定例については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Security Server Protocols」の章の「Kerberos Configuration Examples」を参照してください。

ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Security Command Reference, Release 12.2』の「Security Server Protocols」の章の「Kerberos Commands」を参照してください。



(注) Kerberos 設定例および『Cisco IOS Security Command Reference, Release 12.2』では、信頼できるサードパーティは、Kerberos をサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos の概要

Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密キーによるネットワーク認証プロトコルです。Data Encryption Standard (DES; データ暗号化規格) という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティを *Key Distribution Center* (KDC; キー発行局) と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC (つまり信頼できる Kerberos サーバ) がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。



(注) Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ クレデンシャルが有効な間は (他のパスワードの暗号化を行わずに) セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、(UNIX サーバや PC などの) 他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

このソフトウェア リリースでは、Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh (リモート シェル プロトコル)

表 11-5 に、一般的な Kerberos 関連用語とその定義を示します。

表 11-5 Kerberos の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシヤル	認証チケット (TGT ¹ やサービス クレデンシヤルなど) を表す総称。 Kerberos クレデンシヤルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。クレデンシヤルの有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、 <i>user@REALM</i> という形式です (たとえば、 <i>smith@EXAMPLE.COM</i>)。Kerberos インスタンスのある Kerberos プリンシパルは、 <i>user/instance@REALM</i> という形式です (たとえば、 <i>smith/admin@EXAMPLE.COM</i>)。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 (注) Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 (注) Kerberos レルム名はすべて大文字でなければなりません。
KDC ²	ネットワーク ホストで稼働する Kerberos サーバおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシヤルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 (注) Kerberos レルム名はすべて大文字でなければなりません。
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB ³	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシヤルを暗号解除して認証します。KEYTAB は Kerberos 5 よりも前のバージョンでは、SRVTAB ⁴ と呼ばれています。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であることを表します。 (注) Kerberos プリンシパル名はすべて小文字でなければなりません。

表 11-5 Kerberos の用語 (続き)

用語	定義
サービス クレデンシヤル	ネットワーク サービスのクレデンシヤル。KDC からクレデンシヤルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のこと、KDC が認証済みユーザに発行するクレデンシヤル。TGT を受け取ったユーザは、KDC が示した Kerberos レalm内のネットワーク サービスに対して認証を得ることができます。

1. TGT = Ticket Granting Ticket (身分証明書)
2. KDC = Key Distribution Center (キー発行局)
3. KEYTAB = key table (キー テーブル)
4. SRVTAB = server table (サーバ テーブル)

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてリモート ユーザを認証できるスイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

Kerberos サーバとしてスイッチを使用し、リモート ユーザがネットワーク サービスに対して認証を得る手順は、次のとおりです。

1. 「境界スイッチに対する認証の取得」(P.11-44)
2. 「KDC からの TGT の取得」(P.11-45)
3. 「ネットワーク サービスに対する認証の取得」(P.11-45)

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
 - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
 - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力 (Caps Lock または Num Lock のオン/オフに注意) するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番目のセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番目のセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。



(注) Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

設定については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Security Server Protocols」の章の「Kerberos Configuration Task List」を参照してください。

スイッチのローカル認証および許可の設定

ローカルモードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウント機能は使用できません。

スイッチをローカル AAA 用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login default local</code>	ローカル ユーザ名データベースを使用するようにログイン認証を設定します。 default キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 4	<code>aaa authorization exec local</code>	ユーザの AAA 認証を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 5	<code>aaa authorization network local</code>	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 認証を設定します。
ステップ 6	<code>username name [privilege level] {password encryption-type password}</code>	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 <ul style="list-style-type: none"> <i>name</i> には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 (任意) <i>level</i> には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 <i>encryption-type</i> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 <i>password</i> には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。



(注) AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、`ip http authentication aaa` グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

`ip http authentication` コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

SSH のためのスイッチの設定

ここでは、SSH 機能を設定する方法について説明します。この機能を使用するには、暗号（暗号化）ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「SSH の概要」(P.11-47)
- 「SSH の設定」(P.11-48)
- 「SSH の設定およびステータスの表示」(P.11-51)

SSH の設定例については、次の URL にある『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の「SSH Configuration Examples」を参照してください。

IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点を提供します。SSH への IPv6 の機能拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。



(注)

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。

SSH の概要

SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1 (SSHv1) および SSH バージョン 2 (SSHv2) をサポートしています。

ここでは、次の内容について説明します。

- 「SSH サーバ、統合クライアント、およびサポートされているバージョン」(P.11-47)
- 「制限事項」(P.11-48)

SSH サーバ、統合クライアント、およびサポートされているバージョン

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるアプリケーションです。SSH クライアントを使用すると、SSH サーバが稼働するスイッチに接続できます。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。また、SSH クライアントは、このリリースでサポートされている SSH サーバおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、DES 暗号化アルゴリズム、Triple DES (3DES) 暗号化アルゴリズム、およびパスワードベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+（詳細については、「[TACACS+ によるスイッチ アクセスの制御](#)」(P.11-11) を参照してください)
- RADIUS（詳細については、「[RADIUS によるスイッチ アクセスの制御](#)」(P.11-19) を参照してください)
- ローカル認証および許可（詳細については、「[スイッチのローカル認証および許可の設定](#)」(P.11-46) を参照）



(注)

このソフトウェア リリースは、IP Security (IPSec) をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman (RSA) 認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES (56 ビット) および 3DES (168 ビット) データ暗号化ソフトウェアでのみサポートされます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard (AES; 高度暗号化規格) 暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。

SSH の設定

内容は次のとおりです。

- 「[設定時の注意事項](#)」(P.11-48)
- 「[スイッチで SSH を実行するためのセットアップ](#)」(P.11-49) (必須)
- 「[SSH サーバの設定](#)」(P.11-50) (スイッチを SSH サーバとして設定する場合のみ必須)

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できません (逆の場合も同様です)。
- `crypto key generate rsa` グローバル コンフィギュレーション コマンドを入力した後、CLI エラーメッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、`crypto key generate rsa` コマンドを入力してください。詳細については、「[スイッチで SSH を実行するためのセットアップ](#)」(P.11-49) を参照してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、`hostname` グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。

- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

スイッチで SSH を実行するためのセットアップ

SSH を実行するようにスイッチをセットアップするには、次の手順を実行してください。

1. 暗号化ソフトウェア イメージを **Cisco.com** からダウンロードします。この手順は必須です。詳細については、このリリースのリリース ノートを参照してください。
2. スイッチのホスト名および IP ドメイン名を設定します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
3. スイッチが SSH を自動的にイネーブ爾にするための RSA キーのペアを生成します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
4. ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、「[スイッチのローカル認証および許可の設定](#)」(P.11-46) を参照してください。

ホスト名と IP ドメイン名を設定し、RSA キーのペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	hostname hostname	スイッチのホスト名を設定します。
ステップ3	ip domain-name domain_name	スイッチのホスト ドメインを設定します。
ステップ4	crypto key generate rsa	スイッチ上でローカルおよびリモート認証用に SSH サーバをイネーブ爾にし、RSA キーのペアを生成します。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show ip ssh または show ssh	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RSA キーのペアを削除するには、**crypto key zeroize rsa** グローバル コンフィギュレーション コマンドを使用します。RSA キーのペアを削除すると、SSH サーバは自動的にディセーブルになります。

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip ssh version [1 2]</code>	(任意) SSHv1 または SSHv2 を実行するようにスイッチを設定します。 <ul style="list-style-type: none"> 1: SSHv1 を実行するようにスイッチを設定します。 2: SSHv2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 3	<code>ip ssh {timeout seconds authentication-retries number}</code>	SSH 制御パラメータを設定します。 <ul style="list-style-type: none"> タイムアウト値は秒単位で指定します (デフォルト値は 120 秒)。指定できる範囲は 0 ~ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション (セッション 0 ~ 4) に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 <ul style="list-style-type: none"> クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ~ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 4	<code>line vty line_number [ending_line_number]</code> <code>transport input ssh</code>	(任意) 仮想端末回線設定を設定します。 <ul style="list-style-type: none"> ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。<code>line_number</code> および <code>ending_line_number</code> に対して、1 回線ペアを指定します。指定できる範囲は 0 ~ 15 です。 スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip ssh</code> または <code>show ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバの接続ステータスを表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの SSH 制御パラメータに戻すには、`no ip ssh {timeout | authentication-retries}` グローバル コンフィギュレーション コマンドを使用します。

SSH の設定およびステータスの表示

SSH サーバの設定およびステータスを表示するには、表 11-6 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 11-6 SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『Cisco IOS Security Command Reference, Cisco IOS Release 12.2』の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。

SSL HTTP のためのスイッチの設定

ここでは、HTTP 1.1 のサーバおよびクライアントに対応した Secure Socket Layer (SSL) バージョン 3.0 を設定する方法について説明します。SSL は、セキュア HTTP 通信を実現するために、HTTP クライアント認証だけでなく、サーバ認証、暗号化、およびメッセージの完全性も提供します。SSL を使用するには、暗号化ソフトウェア イメージがスイッチにインストールされている必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。暗号化イメージの詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「セキュア HTTP サーバおよびクライアントの概要」(P.11-51)
- 「セキュア HTTP サーバおよびクライアントの設定」(P.11-53)
- 「セキュア HTTP サーバおよびクライアントのステータスの表示」(P.11-57)

ここで使用する設定例やコマンドの構文および使用方法の詳細については、Cisco IOS Release 12.2(15)T の「HTTPS : HTTP Server and Client with SSL 3.0」の機能説明を参照してください。

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます（セキュアな接続の場合、URL が http:// の代わりに https:// で始まります）。

セキュア HTTP サーバ（スイッチ）の主な役割は、指定のポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答（呼び出す）します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント（Web ブラウザ）の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を（そのアプリケーションに）返すことです。

CA のトラストポイント

Certificate Authority (CA; 認証局) は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集約的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント (通常、Web ブラウザ) は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した (自己署名) 証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択 (確立または拒否) をさせる必要があります。この選択肢は内部ネットワーク トポロジ (テスト用など) に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ (またはクライアント) に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されていない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書 (一時的に) が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。



(注)

認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力 (show running-config コマンド) を例として一部示します。

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

```
<output truncated>
```

```
crypto pki trustpoint TP-self-signed-3080755072
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3080755072
  revocation-check none
  rsakeypair TP-self-signed-3080755072
!
```

```
crypto ca certificate chain TP-self-signed-3080755072
  certificate self-signed 01
    3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
```

```
<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。



(注) *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド (**ip http secure-client-auth**) を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Configuring Certification Authority Interoperability」を参照してください。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ (RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC) をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアントブラウザ (Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など) が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷 (速さ) による CipherSuite のランク (速い順) を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA : メッセージの暗号化に DES-CBC、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (RSA 公開キー暗号化)
2. SSL_RSA_WITH_RC4_128_MD5 : RC4 128 ビット暗号化、およびメッセージダイジェストに MD5 を使用した RSA のキー交換
3. SSL_RSA_WITH_RC4_128_SHA : RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA : メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (RSA 公開キー暗号化)

(暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた) RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわらず。

セキュア HTTP サーバおよびクライアントの設定

ここでは、次の設定について説明します。

- 「SSL のデフォルト設定」(P.11-54)
- 「SSL の設定時の注意事項」(P.11-54)
- 「CA のトラストポイントの設定」(P.11-54)
- 「セキュア HTTP サーバの設定」(P.11-55)
- 「セキュア HTTP クライアントの設定」(P.11-56)

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンドで終了します。クラスタメンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>hostname hostname</code>	スイッチのホスト名を指定します (以前ホスト名を設定していない場合のみ必須)。ホスト名はセキュリティ キーと証明書に必要です。
ステップ 3	<code>ip domain-name domain-name</code>	スイッチの IP ドメイン名を指定します (以前 IP ドメイン名を設定していない場合のみ必須)。IP ドメイン名はセキュリティ キーと証明書に必要です。
ステップ 4	<code>crypto key generate rsa</code>	(任意) RSA キーのペアを生成します。RSA キーのペアは、スイッチの証明書を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。
ステップ 5	<code>crypto ca trustpoint name</code>	CA のトラストポイントにローカルの設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	<code>enrollment url url</code>	証明書の要求の送信先スイッチの URL を指定します。
ステップ 7	<code>enrollment http-proxy host-name port-number</code>	(任意) HTTP プロキシ サーバを経由して CA から証明書を入手するようにスイッチを設定します。
ステップ 8	<code>crl query url</code>	ピアの証明書が取り消されていないかを確認するために、Certificate Revocation List (CRL; 証明書失効リスト) を要求するようにスイッチを設定します。
ステップ 9	<code>primary</code>	(任意) トラストポイントが CA 要求に対してプライマリ (デフォルト) トラストポイントとして使用されるように指定します。
ステップ 10	<code>exit</code>	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	<code>crypto ca authentication name</code>	CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。

	コマンド	目的
ステップ 12	<code>crypto ca enroll name</code>	指定の CA のトラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show crypto ca trustpoints</code>	設定を確認します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`no crypto ca trustpoint name` グローバル コンフィギュレーション コマンドを使用して、CA に関連するすべての ID 情報および証明書を削除できます。

セキュア HTTP サーバの設定

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセス リスト、最大接続数、またはタイムアウト ポリシー）を設定できます。

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>show ip http server status</code>	(任意) HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。 <code>HTTP secure server capability: Present</code> <code>or</code> <code>HTTP secure server capability: Not present</code>
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>ip http secure-server</code>	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。
ステップ 4	<code>ip http secure-port port-number</code>	(任意) HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ~ 65535 の範囲で指定できます。
ステップ 5	<code>ip http secure-ciphersuite</code> {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}	(任意) HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ 6	<code>ip http secure-client-auth</code>	(任意) HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	<code>ip http secure-trustpoint name</code>	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。 (注) このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。

	コマンド	目的
ステップ 8	<code>ip http path path-name</code>	(任意) HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します (通常、システムのフラッシュ メモリを指定します)。
ステップ 9	<code>ip http access-class access-list-number</code>	(任意) HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	<code>ip http max-connections value</code>	(任意) HTTP サーバへの同時最大接続数を指定します。指定できる範囲は 1 ~ 16 です。デフォルトは 5 です。
ステップ 11	<code>ip http timeout-policy idle seconds life seconds requests value</code>	(任意) 指定の状況下における、HTTP サーバへの接続最大時間を指定します。 <ul style="list-style-type: none"> • idle : データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ~ 600 秒です。デフォルト値は 180 秒 (3 分) です。 • life : 接続を確立している最大時間。指定できる範囲は 1 ~ 86400 秒 (24 時間) です。デフォルト値は 180 秒です。 • requests : 永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip http server secure status</code>	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

標準の HTTP サーバをディセーブルにするには、**no ip http server** グローバル コンフィギュレーション コマンドを使用します。セキュア HTTP サーバをディセーブルにするには、**no ip http secure-server** グローバル コンフィギュレーション コマンドを使用します。デフォルトの設定に戻すには、**no ip http secure-port** および **no ip http secure-ciphersuite** グローバル コンフィギュレーション コマンドを使用します。クライアント認証の要件を削除するには、**no ip http secure-client-auth** グローバル コンフィギュレーション コマンドを使用します。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、`https://URL` を入力します (URL は IP アドレス、またはサーバ スイッチのホスト名)。デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

セキュア HTTP クライアントの設定

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip http client secure-trustpoint name</code>	(任意) リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリのトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ3	<code>ip http client secure-ciphersuite</code> { <code>[3des-ede-cbc-sha]</code> <code>[rc4-128-md5]</code> <code>[rc4-128-sha]</code> <code>[des-cbc-sha]</code> }	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴリズム) を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これはデフォルトです。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show ip http client secure status</code>	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

クライアントのトラストポイントの設定を削除するには、`no ip http client secure-trustpoint name` コマンドを使用します。クライアントにすでに設定されている CipherSuite 仕様を削除するには、`no ip http client secure-ciphersuite` コマンドを使用します。

セキュア HTTP サーバおよびクライアントのステータスの表示

SSL セキュア サーバおよびクライアントのステータスを表示するには、表 11-7 に記載された特権 EXEC コマンドを使用します。

表 11-7 SSL セキュア サーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
<code>show ip http client secure status</code>	セキュア HTTP クライアントの設定を表示します。
<code>show ip http server secure status</code>	セキュア HTTP サーバの設定を表示します。
<code>show running-config</code>	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

SCP のためのスイッチの設定

Secure Copy Protocol (SCP) 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供します。SCP には、Berkeley r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルであるセキュア シェル (SSH) が必要です。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंगを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。



(注) SCP を使用する場合、`copy` コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

Secure Copy に関する情報

Secure Copy 機能を設定するには、次の概念を理解する必要があります。

SCP は一連の Berkeley の `r-tools` に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol (RCP) と類似しています。また、SCP の設定には AAA の許可も必要のため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。

適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System (IFS) のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには `copy` コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

SCP の設定および検証方法の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』の「Secure Copy Protocol」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_ps6350_TSD_Products_Configuration_Guide_Chapter.html



CHAPTER 12

IEEE 802.1x ポートベース認証の設定

IEEE 802.1x ポートベース認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。IE 3000 スイッチのコマンド リファレンスと、『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」に、コマンドの構文と使用方法の情報が 있습니다。

この章で説明する内容は、次のとおりです。

- 「IEEE 802.1x ポートベース認証の概要」 (P.12-1)
- 「802.1x 認証の設定」 (P.12-32)
- 「802.1x の統計情報およびステータスの表示」 (P.12-65)

IEEE 802.1x ポートベース認証の概要

IEEE 802.1x 規格では、一般の人がアクセス可能なポートからクライアントが LAN に接続しないように規制する、クライアント/サーバベースのアクセス コントロールおよび認証プロトコルを規定しています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスを利用できるようにします。

IEEE 802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL)、Cisco Discovery Protocol (CDP)、および Spanning-Tree Protocol (STP; スパニングツリー プロトコル) トラフィックしか許可されません。認証後、通常のトラフィックをポート経由で送受信できます。

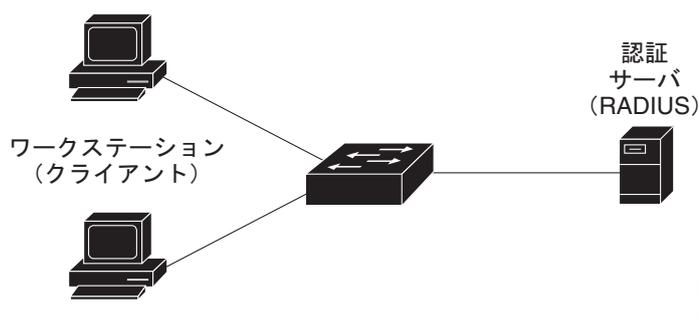
- 「デバイスの役割」 (P.12-2)
- 「認証プロセス」 (P.12-3)
- 「認証の開始およびメッセージ交換」 (P.12-5)
- 「認証マネージャ」 (P.12-7)
- 「許可ステートおよび無許可ステートのポート」 (P.12-10)
- 「802.1x のホスト モード」 (P.12-11)
- 「マルチドメイン認証」 (P.12-12)
- 「802.1x 複数認証モード」 (P.12-13)
- 「MAC Move」 (P.12-13)
- 「MAC 置換」 (P.12-14)
- 「802.1x アカウンティング」 (P.12-14)
- 「802.1x アカウンティング属性値ペア」 (P.12-15)
- 「802.1x 準備状態チェック」 (P.12-16)

- 「VLAN 割り当てを使用した 802.1x 認証」 (P.12-16)
- 「ユーザ単位 ACL を使用した 802.1x 認証の使用」 (P.12-17)
- 「ゲスト VLAN を使用した 802.1x 認証」 (P.12-21)
- 「制限付き VLAN を使用した 802.1x 認証」 (P.12-22)
- 「アクセス不能認証バイパスを使用した 802.1x 認証」 (P.12-23)
- 「音声 VLAN ポートを使用した 802.1x 認証」 (P.12-25)
- 「ポートセキュリティを使用した 802.1x 認証」 (P.12-25)
- 「Wake-on-LAN を使用した 802.1x 認証」 (P.12-25)
- 「MAC 認証バイパスによる 802.1x 認証」 (P.12-26)
- 「802.1x ユーザ ディストリビューション」 (P.12-27)
- 「Network Admission Control レイヤ 2 802.1x 検証」 (P.12-28)
- 「柔軟な認証の順序設定」 (P.12-28)
- 「Open1x 認証」 (P.12-29)
- 「音声認識 802.1x セキュリティの使用」 (P.12-29)
- 「Network Edge Access Topology (NEAT) を使用した 802.1x サプリカントおよびオーセンティケータ」 (P.12-29)
- 「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証」 (P.12-19)
- 「ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用」 (P.12-31)
- 「コモン セッション ID」 (P.12-31)

デバイスの役割

802.1X ポートベースの認証での装置の役割：

図 12-1 802.1x におけるデバイスの役割



101229

- クライアント: LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス (ワークステーション)。ワークステーションでは、Microsoft Windows XP OS (オペレーティング システム) に付属しているような 802.1x 準拠のクライアント ソフトウェアを実行する必要があります (クライアントは、802.1x 標準ではサブリカントといえます)。



(注) Windows XP のネットワーク接続と 802.1x 認証の問題を解決するには、次の URL にある「Microsoft Knowledge Base」を参照してください。
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- 認証サーバ: クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対して透過的に行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol (EAP) 拡張機能を備えた Remote Authentication Dial-In User Service (RADIUS) セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- スイッチ (エッジ スイッチまたはワイヤレス アクセス ポイント): クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス (プロキシ) として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています (スイッチは、802.1x 標準ではオーセンティケータといえます)。

スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われなため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

仲介装置として動作できる装置は、IE 3000、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 の各スイッチや、ワイヤレス アクセス ポイントなどです。これらのデバイスでは、RADIUS クライアントおよび 802.1x 認証をサポートするソフトウェアが稼働している必要があります。

認証プロセス

802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。

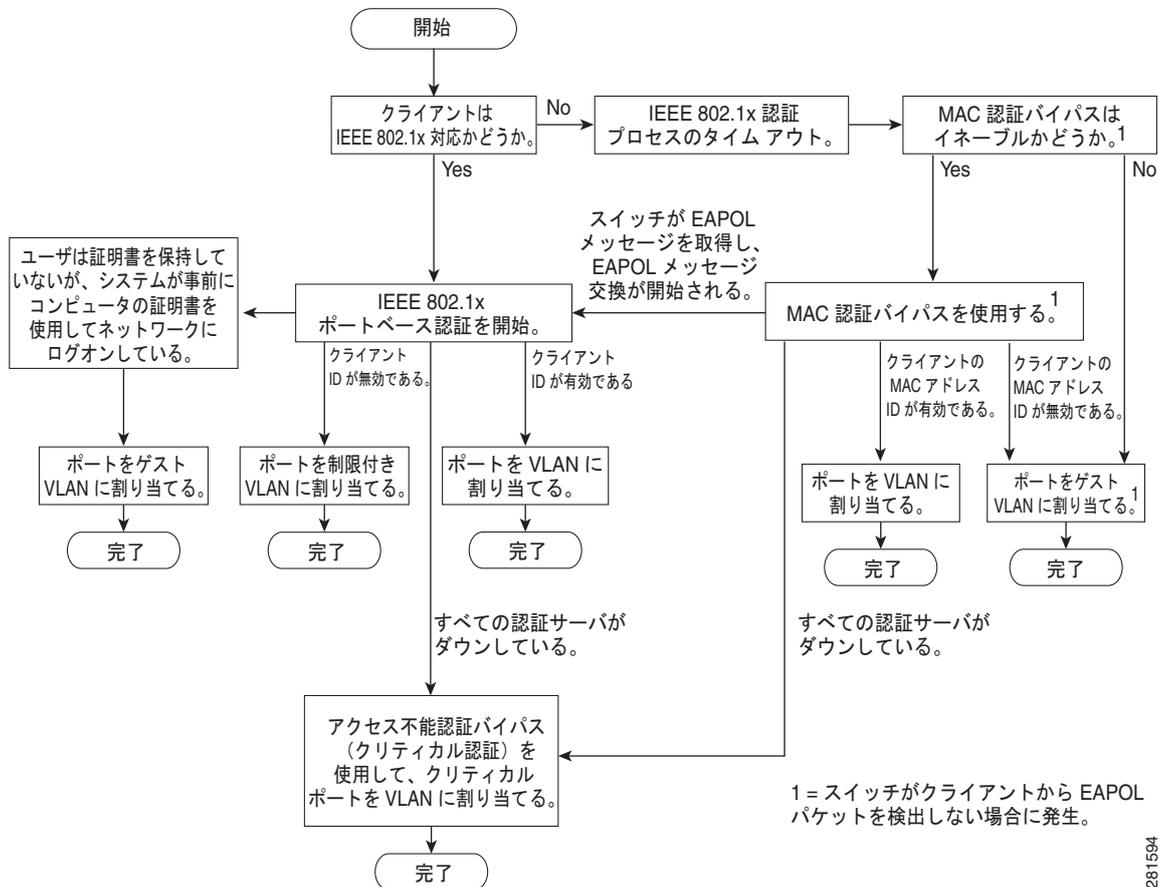
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証状態にして、クライアントにネットワークのアクセスを許可します。



(注) アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントング) 失敗ポリシーとも呼ばれます。

図 12-2 に、認証プロセスを示します。

図 12-2 認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

RADIUS サーバを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性（属性 [27]）、および Termination-Action RADIUS 属性（属性 [29]）に基づいてタイマーを使用します。

Session-Timeout RADIUS 属性（属性 [27]）には再認証が行われるまでの時間を指定します。

Termination-Action RADIUS 属性 (Attribute[29]) には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize* (属性値は *DEFAULT*) を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate* (属性値は *RADIUS-Request*) を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface interface-id** 特権 EXEC コマンドを入力します。

Multidomain Authentication (MDA; マルチドメイン認証) がポートでイネーブルにされている場合、このフローが使用されます。ただし、音声許可の場合はいくつかの例外があります。MDA の詳細については、「[マルチドメイン認証](#)」(P.12-12) を参照してください。

認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンク ステータスがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチから EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。



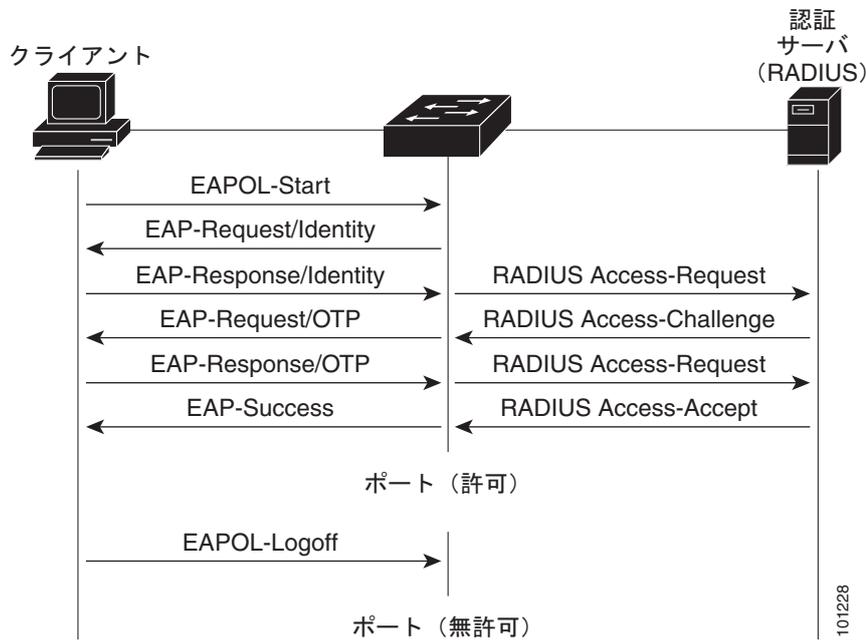
(注)

ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステータスであるものとしてフレームを送信します。ポートが許可ステータスであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「[許可ステータスおよび無許可ステータスのポート](#)」(P.12-10) を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステータスになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「[許可ステータスおよび無許可ステータスのポート](#)」(P.12-10) を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 12-3 に、クライアントが RADIUS サーバとの間で OTP (ワンタイム パスワード) 認証方式を使用する際に行われるメッセージ交換を示します。

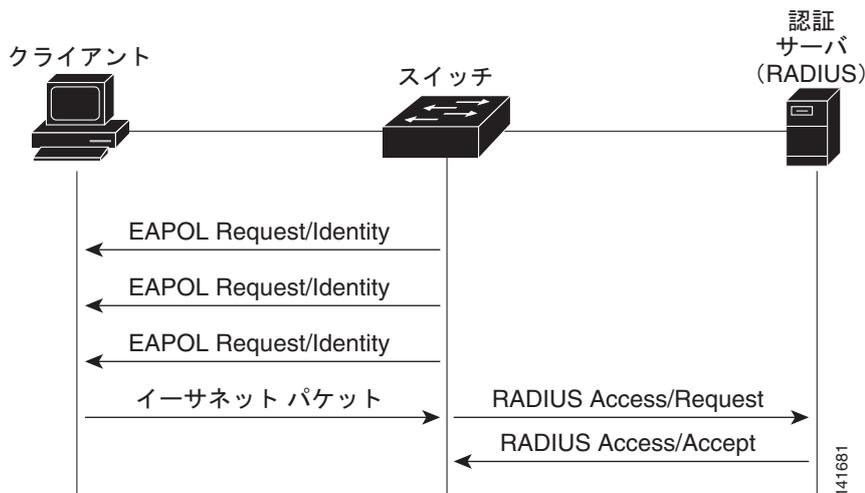
図 12-3 メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証できません。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネットパケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパスプロセスを停止して、802.1x 認証を停止します。

図 12-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 12-4 MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、スイッチ上および Catalyst 6000 などの他のネットワーク デバイス上で、CLI コマンドおよびメッセージなど、同じ認証方法を使用することができず、異なる認証設定を使用する必要がありました。Cisco IOS Release 12.2(50)SE 以降では、ネットワークのすべての Catalyst スイッチで同じ認証方法を使用できます。

Cisco IOS Release 12.2(55)SE は、認証マネージャからの冗長なシステム メッセージのフィルタリングをサポートします。詳細については、「[認証マネージャ CLI コマンド](#)」(P.12-9)を参照してください。

- 「[ポートベースの認証方法](#)」(P.12-7)
- 「[ユーザ単位 ACL および Filter-Id](#)」(P.12-8)
- 「[認証マネージャ CLI コマンド](#)」(P.12-9)

ポートベースの認証方法

表 12-1 に、これらのホスト モードでサポートされている認証方法を示します。

- シングル ホスト：ポートで認証できるデータまたは音声ホスト（クライアント）は 1 つだけです。
- マルチ ホスト：同じポートで複数のデータ ホストを認証できます（ポートがマルチ ホスト モードで無許可になると、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します）。
- マルチドメイン認証（MDA）：同じスイッチ ポートでデータ デバイスと音声デバイスの両方を認証できます。ポートはデータ ドメインと音声ドメインに分割されます。
- 複数認証：複数のホストがデータ VLAN で認証できます。このモードでは、音声 VLAN が設定されている場合、VLAN で 1 クライアントだけ使用できます。

表 12-1 802.1x の機能

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ⁴ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
スタンドアロン Web 認証 ⁴	プロキシ ACL、Filter-Id 属性、ダウンロード可能な ACL ²			

表 12-1 802.1x の機能 (続き)

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²
NAC レイヤ 2 IP 検証	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性 ³ ダウンロード可能 ACL ³ リダイレクト URL ³
フォールバック メソッドとしての Web 認証 ⁵	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL Filter-Id 属性 ³ ダウンロード可能 ACL ³	Proxy ACL ³ Filter-Id 属性 ³ ダウンロード可能 ACL ³

1. MDA = マルチドメイン認証。
2. *multiauth* と呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされています。
5. 802.1x 認証をサポートしていないクライアントの場合。

ユーザ単位 ACL および Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id がサポートされているのは、シングル ホスト モードだけでした。Cisco IOS Release 12.2(50) では、MDA および複数認証 (multiauth) をイネーブルにしたポートのサポートが追加されました。12.2(52)SE 以降では、マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、Catalyst 6000 スイッチなど、Cisco IOS ソフトウェアを実行する別のデバイスで設定された ACL と互換性がありませんでした。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行する他のデバイスで設定された ACL と互換性があります。



(注) **any** は、ACL の発信元としてだけ設定できます。



(注) マルチ ホスト モードで設定された ACL では、ステートメントの発信元部分は **any** でなければなりません (たとえば、**permit icmp any host 10.10.1.1**)。

定義された ACL の発信元ポートには **any** を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。

マルチ ホスト ポートで認証されるホストが 1 つだけで、他のホストが認証なしでネットワーク アクセスを取得する場合、発信元アドレスに **any** を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパス および Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation** および **authentication timer** インターフェイス コンフィギュレーション コマンドがあります。

802.1x 専用コマンドは、頭に **dot1x** または **authentication** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。



(注) 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは、以前の 802.1x コマンドと同じ機能を提供します。

表 12-2 認証マネージャ コマンドおよび以前の 802.1x コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {both in}	dot1x control-direction {both in}	Wake-on-LAN (WoL) 機能を使用した認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	dot1x auth-fail vlan dot1x critical (インターフェイス コンフィギュレーション) dot1x guest-vlan6	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback <i>fallback-profile</i>	dot1x fallback <i>fallback-profile</i>	認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
authentication host-mode [multi-auth multi-domain multi-host single-host]	dot1x host-mode {single-host multi-host multi-domain}	認可ポートでシングル ホスト (クライアント) またはマルチ ホストを許可します。
authentication order	dot1x mac-auth-bypass	使用される認証方法の順序を柔軟に定義できるようにします。
authentication periodic	dot1x reauthentication	クライアントの定期的再認証をイネーブルにします。
authentication port-control {auto force-authorized force-unauthorized}	dot1x port-control {auto force-authorized force-unauthorized}	ポートの許可ステータスの手動制御をイネーブルにします。

表 12-2 認証マネージャ コマンドおよび以前の 802.1x コマンド (続き)

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
<code>authentication timer</code>	<code>dot1x timeout</code>	タイマーを設定します。
<code>authentication violation {protect restrict shutdown}</code>	<code>dot1x violation-mode {shutdown restrict protect}</code>	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に発生する違反モードを設定します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、認証マネージャで生成された冗長なシステム メッセージをフィルタリングできます。通常、フィルタリングされた内容は、認証の成功と関係していません。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの冗長なメッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の冗長なメッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC Authentication Bypass (MAB; MAC 認証バイパス) の冗長なメッセージをフィルタリングします。

詳細については、このリリースのコマンド リファレンスを参照してください。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN (仮想 LAN) ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコル パケットが許可された後クライアントが正常に認証されます。

802.1x 認証をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に回答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized** : 802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- **force-unauthorized** : クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチはポートを介してクライアントに認証サービスを提供できません。

- **auto** : 802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから **Accept** フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。指定された回数試行してもサーバから応答が得られない場合は、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

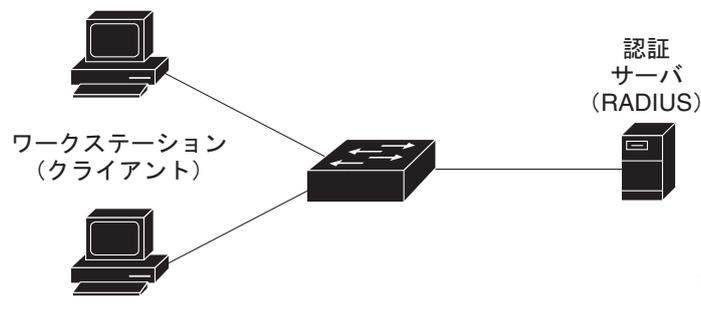
ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1x のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モード (図 12-1 (P.12-2) を参照) では、802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。図 12-5 (P.12-11) に、ワイヤレス LAN における 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 12-5 マルチ ホスト モードの例



(注)

ポートベース認証が設定された場合は、認可の前に、すべてのホスト モードに対してライン プロトコルがアップ状態になります。

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方を同じスイッチ ポートに接続できます。詳細については、「[マルチドメイン認証](#)」(P.12-12) を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定するには、「[ホスト モードの設定](#)」(P.12-42) を参照してください。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、[第 16 章「VLAN の設定」](#)を参照してください。
- 音声デバイスを許可するには、値 `device-traffic-class=voice` の Cisco Attribute Value (AV; 属性値) ペア属性を送信するように AAA サーバを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、`errordisable` になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック方法として MAC 認証バイパスを使用して、IEEE 802.1x 認証をサポートしていないデバイスにスイッチポートを接続できます。詳細については、「[MAC 認証バイパス](#)」(P.12-36) を参照してください。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは `errdisable` になります。
- ポートのホスト モードがシングル ホストまたはマルチホストからマルチドメイン モードに変更される場合、許可済みのデータ デバイスはポートで許可済みのままになります。ただし、ポート音声 VLAN の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。
- ポートがシングルまたはマルチ ホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック方法は設定されたままになります。
- マルチドメイン モードからシングル ホストまたはマルチ ホスト モードにポートを切り替えると、ポートからすべての認証済みデバイスが削除されます。

- データ ドメインがまず許可されてゲスト VLAN に配置された場合、IEEE 802.1x 非対応音声デバイスは認証をトリガーするために音声 VLAN 上のパケットにタグを付ける必要があります。電話機はタグ付きトラフィックを送信する必要はありません (802.1x 対応電話の場合も同様です)。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーがある許可済みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。使用する場合、ポート上の 1 デバイスだけでユーザ単位 ACL が実行されます。

詳細については、「[ホストモードの設定](#)」(P.12-42) を参照してください。

802.1x 複数認証モード

複数認証 (multiauth) モードでは、データ VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは、VLAN で 1 クライアントだけ認証できます (ポートが他の音声クライアントを検出すると、これらはポートから廃棄されますが、違反エラーは発生しません)。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。

802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 台だけです。ホスト制限がないため、定義された違反はトリガーされません。たとえば、別の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガーされません。

音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取った VSA に応じて、認証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。



(注) ポートがマルチ認証モードの場合、ゲスト VLAN、および認証失敗 VLAN 機能はアクティブになりません。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「[アクセス不能認証バイパスを使用した 802.1x 認証](#)」(P.12-23) を参照してください。

ポートでのマルチ認証モードの設定の詳細については、「[ホストモードの設定](#)」(P.12-42) を参照してください。

MAC Move

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチ ポート間に別のデバイス (ハブまたは IP Phone など) がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC Move をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。

MAC Move はすべてのホスト モードでサポートされます（認証ホストは、ポートでイネーブルにされているホスト モードに関係なく、スイッチの任意のポートに移動できます）。

MAC アドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。

MAC Move の機能は、音声およびデータ ホストの両方に適用されます。



(注)

オープン認証モードでは、MAC アドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「[MAC Move のイネーブル化](#)」(P.12-47) を参照してください。

MAC 置換

Cisco IOS Release 12.2(55)SE 以降のリリースでは、MAC 置換機能を設定して、事前に別のホストが認証されたポートにホストが接続を試みるときに発生する違反に対処できるようになりました。



(注)

違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ ホストの MAC アドレスを、新しい MAC アドレスで置き換えます。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MAC アドレスはただちに MAC アドレス テーブルに追加されます。

詳細については、「[MAC 置換のイネーブル化](#)」(P.12-48) を参照してください。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1x アカウンティング情報を記録しません。その代わりに、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティングメッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、Attribute Value (AV; 属性値) ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます (たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です)。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START : 新規ユーザセッションが始まると送信されます。
- INTERIM : 既存のセッションが更新されると送信されます。
- STOP : セッションが終了すると送信されます。

次の表 12-3 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 12-3 アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信 ¹	条件に応じて送信 ¹
属性 [25]	Class	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	常時送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	常時送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	常時送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol (DHCP) バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にのみ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。

AV ペアの詳細については、RFC 3580『802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサブリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

802.1x 準備状態チェックのスイッチの設定については、「[802.1x 準備状態チェックの設定](#)」(P.12-36)を参照してください。

VLAN 割り当てを使用した 802.1x 認証

RADIUS サーバは、VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバデータベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声装置が認可され、RADIUS サーバが認可済みの VLAN を返した場合、ポート上の音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されます。音声 VLAN 割り当ては、マルチドメイン認証 (MDA) 対応のポートでのデータ VLAN 割り当てと同じように機能します。詳細については、「[マルチドメイン認証](#)」(P.12-12)を参照してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッドポートの VLAN、間違った VLAN ID、存在しないまたは内部 (ルーテッドポート) VLAN ID、RSPAN VLAN、シャットダウンまたは一時停止している VLAN の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行 (またはその逆) のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。

- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN (RADIUS サーバにより指定) に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
 - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
 - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可 (force-authorized) ステート、強制無許可 (force-unauthorized) ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server (VMPS; VLAN メンバーシップ ポリシー サーバ) によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。(アクセス ポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
 - [64] Tunnel-Type = VLAN
 - [65] Tunnel-Medium-Type = 802
 - [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID または VLAN-Group
 - [83] Tunnel-Preference

属性 [64] は、値 *VLAN* (タイプ 13) でなければなりません。属性 [65] は、値 *802* (タイプ 6) でなければなりません。属性 [81] は、802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(P.11-37) を参照してください。

ユーザ単位 ACL を使用した 802.1x 認証の使用

ユーザ単位 Access Control List (ACL; アクセス コントロール リスト) をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザ セッションの期間中、その属性を 802.1x ポート

に適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。発信するルーテッドパケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバに保存するユーザプロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。Vendor-Specific Attribute (VSA; ベンダー固有属性) は、オクテットストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、第 38 章「ACL によるネットワークセキュリティの設定」を参照してください。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す `.in` または `.out` が含まれています。RADIUS サーバが `.in` または `.out` 構文を許可しない場合、アクセスリストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセスリストに関するサポートが制限されているため、Filter-ID 属性は 1 ~ 199 および 1300 ~ 2699 の IP ACL (IP 標準 ACL および IP 拡張 ACL) に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

ベンダー固有属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」(P.11-37) を参照してください。ACL の設定の詳細については、第 38 章「ACL によるネットワークセキュリティの設定」を参照してください。



(注)

ユーザ単位 ACL がサポートされるのはシングルホストモードだけです。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザプロファイルと VSA を設定します。
- 802.1x ポートをシングルホストモードに設定します。

設定の詳細については、「認証マネージャ」(P.12-7) を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。



(注) ダウンロード可能な ACL は *dACL* と呼ばれます。

複数のホストが認証され、それらのホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト ACL が作成され、dACL がダウンロードされて適用される前にポリシーが実施されます。



(注) 認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト ACL は、**ip access-list extended auth-default-acl** グローバル コンフィギュレーション コマンドを使用して作成できます。



(注) 認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol (CDP) バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック ACL を設定する必要があります。

802.1x および MAB 認証方式では、オープンおよびクローズの 2 つの認証方式がサポートされます。クローズ認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

オープン認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブは、ポートから提供されるアク

セスにトラフィックを従わせませす。ディレクティブは、AAA サーバ上のユーザ プロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバ上でディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチ上でディレクティブを設定するには、**epm access-control open** グローバル コンフィギュレーション コマンドを使用します。



(注) ディレクティブのデフォルト値は *default* です。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、次のようになります。

- ポートがオープン認証モードの場合、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト ACL が作成されます。

フォールバック ACL のアクセス コントロール エントリ (ACE) は、ユーザ単位のエントリに変換されます。設定されたフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストはポートに関連付けられた認証デフォルト ACL に従います。



(注) Web 認証でカスタム ログを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

Cisco Secure ACS およびリダイレクト URL の属性と値のペア

スイッチはこれらの *cisco-av-pair* VSA を使用します。

- *url-redirect* は HTTP to HTTPS URL です。
- *url-redirect-acl* はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL 属性値ペアを使用して、エンドポイントデバイスからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS の *url-redirect* 属性値ペアには、Web ブラウザがリダイレクトされる URL が含まれます。*url-redirect-acl* 属性値ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL の permit ACE と一致するトラフィックがリダイレクトされます。



(注) スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

Cisco Secure ACS およびダウンロード可能な ACL の属性と値のペア

RADIUS の *cisco-av-pair Vendor-Specific Attribute* (VSA; ベンダー固有属性) を使用すると、Cisco Secure ACS で CiscoSecure-Defined-ACL Attribute Value (AV; 属性値) ペアを設定できます。このペアは、*#ACL#-IP-name-number* 属性を使って、Cisco Secure ACS でダウンロード可能な ACL の名前を指定します。

- *name* は ACL の名前です。
- *number* はバージョン番号 (たとえば 3f783768) です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこのポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

設定の詳細については、「[認証マネージャ](#)」(P.12-7) および「[ダウンロード可能 ACL およびダイレクト URL を使用した 802.1x 認証の設定](#)」(P.12-60) を参照してください。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スイッチにスタティック VLAN ポリシーが設定されていると、認証する各ホストの MAC アドレスとともに VLAN の情報が IAS (Microsoft) RADIUS サーバに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

この機能を使用すると、STP によりモニタリングおよび処理される VLAN の数も制限されます。ネットワークは、固定 VLAN として管理できます。



(注)

この機能は Cisco ACS Server ではサポートされていません (ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います)。

設定の詳細については、「[VLAN ID ベース MAC 認証の設定](#)」(P.12-62) を参照してください。追加設定は、同様の MAC 認証バイパスです («[MAC 認証バイパスの設定](#)」(P.12-56) を参照してください)。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます (802.1x クライアントのダウンロードなど)。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。ポートは、マルチホスト モードに自動的に設定されます。

スイッチは EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンドシーケンスを使用します。

- **authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。



(注)

インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステータスに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステータスになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッド ポート) またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは MAC 認証バイパスをサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます (指定されていない場合)。詳細については、「[MAC 認証バイパスによる 802.1x 認証](#)」(P.12-26) を参照してください。

詳細については、「[ゲスト VLAN の設定](#)」(P.12-49) を参照してください。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチの各 802.1x ポートに対して制限付き VLAN (認証失敗 VLAN と呼ばれることもあります) を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシャルを持っていないユーザ (通常、企業にアクセスするユーザ) に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。



(注)

両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパンニングツリーのブロッキング ステータスから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し (デフォルト値は 3 回)、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1x ポート上でシングル ホスト モードの場合だけサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッドポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

ダイナミック ARP インспекション、DHCP スヌーピング、および IP 送信元ガードのような他のセキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「[制限付き VLAN の設定](#)」（P.12-50）を参照してください。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、*クリティカル認証*または *AAA 失敗ポリシー*とも呼ばれます。これらのホストを *クリティカル ポート*に接続するようにスイッチを設定できます。

新しいホストが *クリティカル ポート*に接続しようとする時、そのホストはユーザ指定のアクセス VLAN、*クリティカル VLAN*に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、*クリティカル ポート*に接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースである *クリティカル認証*ステートにします。

複数認証ポートのサポート

ポートが任意のホスト モードで設定されていて、AAA サーバを使用できない場合、ポートはマルチホスト モードに設定され、*クリティカル VLAN*に移動されます。マルチ認証（*multiauth*）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan *vlan-id*** コマンドを使用します。新しいホストが *クリティカル ポート*に接続しようとする時、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイムアウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカル ポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。詳細については、このリリースのコマンドリファレンスおよび「[アクセス不能認証バイパス機能の設定](#)」(P.12-52) を参照してください。

機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- **ゲスト VLAN** : アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 802.1x ポートでイネーブルの場合、この機能は次のように相互に作用します。
 - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- **制限付き VLAN** : ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- **802.1x アカウンティング** : RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- **プライベート VLAN** : プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- **音声 VLAN** : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異ならなければなりません。
- **Remote Switched Port Analyzer (RSPAN)** : アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを送送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータトラフィックを送送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サブリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サブリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。



(注)

音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、第 18 章「音声 VLAN の設定」を参照してください。

ポート セキュリティを使用した 802.1x 認証

通常、IEEE 802.1x がイネーブルの場合に、ポート セキュリティをイネーブルにすることは推奨されません。IEEE 802.1x がポートごとに（または IP テレフォニーに MDA が設定されている場合は VLAN ごとに）単一の MAC アドレスを強制するため、ポート セキュリティが冗長になり、正常な IEEE 802.1x 操作が妨害される場合もあります。

Wake-on-LAN を使用した 802.1x 認証

802.1x 認証の Wake-on-LAN (WoL) 機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1x ポートを通じて接続され、ホストの電源がオフになると、802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。



(注)

PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに変わります。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスによる 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス (図 12-2 (P.12-4) を参照) に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サブリカントであることを確認し、(MAC 認証バイパス機能ではなく) 802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1x サブリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。Termination-Action RADIUS 属性の値が DEFAULT であるという理由で直前のセッションが終了した場合、スイッチは再認証時に、802.1x 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性 (属性 [27])、および Termination-Action RADIUS 属性 (属性 [29]) に基づいて行われるときに、Termination-Action RADIUS 属性 (属性 [29]) のアクションが Initialize (属性値は DEFAULT) である場合、MAC 認証バイパスセッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能がイネーブルで、802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。AV ペアの詳細については、RFC 3580 『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1x 認証：802.1x 認証がポートでイネーブルの場合にだけ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1x 認証」(P.12-25) を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1x 認証」(P.12-25) を参照してください。
- VLAN メンバーシップ ポリシー サーバ (VMPS)：802.1x および VMPS は相互に排他的です。
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- シスコ ネットワーク アドミッションコントロール (NAC) レイヤ 2 IP 検証：この機能は、802.1X ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。
- Network Edge Access Topology (NEAT)：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT がイネーブルの場合は、MAB をイネーブルにできません。また、インターフェイス上で MAB がイネーブルの場合は、NEAT をイネーブルにできません。

設定の詳細については、「認証マネージャ」(P.12-7) を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。「認証マネージャ CLI コマンド」(P.12-9) を参照してください。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。



(注) RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされることを確認してください。

- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

詳細については、「[802.1x ユーザ ディストリビューションの設定](#)」(P.12-56) を参照してください。

Network Admission Control レイヤ 2 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャをチェックする Network Admission Control (NAC) レイヤ 2 802.1x 検証をサポートしています。NAC レイヤ 2 802.1x 検証を使用すると、次の作業を実行できます。

- Session-Timeout RADIUS 属性 (属性 [27]) と Termination-Action RADIUS 属性 (属性 [29]) を認証サーバからダウンロードします。
- Session-Timeout RADIUS 属性 (属性 [27]) の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性 (属性 [29]) を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID (属性 [81]) の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference (属性 [83]) の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID (属性 [81]) 属性がリストから選択されます。
- **show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、802.1x ポートベース認証と似ています。NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「[NAC レイヤ 2 802.1x 検証の設定](#)」(P.12-57) および「[定期的な再認証の設定](#)」(P.12-43) を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

設定の詳細については、「[認証マネージャ](#)」(P.12-7) を参照してください。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法的順序を設定できます。MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。詳細については、「[柔軟な認証順序の設定](#)」(P.12-63) を参照してください。

Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセスコントロール リスト (ACL) に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングル ホスト モードでのオープン認証：1 人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの 1 人のユーザだけ、およびデータ ドメインの 1 人のユーザだけが許可されます。
- マルチ ホスト モードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDA の場合と似ていますが、複数のホストを認証できます。

詳細については、「[ホスト モードの設定](#)」(P.12-42) を参照してください。



(注)

オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

音声認識 802.1x セキュリティの使用

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、データ クライアントを認証しようとしてセキュリティ違反が発生すると、ポート全体がシャットダウンされ、接続が完全に切断されていました。

この機能は、PC が IP Phone に接続されている場合に使用できます。この機能を使用した場合、データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされ、音声 VLAN のトラフィックは中断することなく処理を続行できます。

音声認識 802.1x セキュリティの設定については、「[音声対応 802.1x セキュリティの設定](#)」(P.12-37) を参照してください。

Network Edge Access Topology (NEAT) を使用した 802.1x サブリカントおよびオーセンティケータ

Network Edge Access Topology (NEAT) 機能は、ワイヤリング クローゼット (会議室など) 外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サブリカント：802.1x サブリカント機能を使用することで、別のスイッチのサブリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランク ポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サブリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。

サブリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されます。

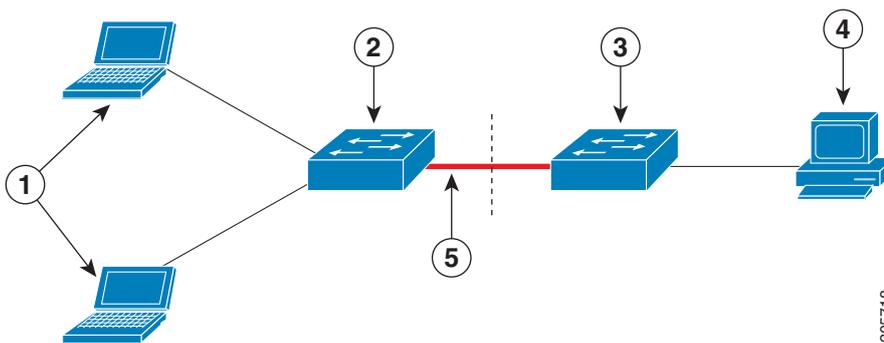
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

1 つ以上のサブリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または **multiauth** モードをイネーブルにできます。マルチホスト モードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

すべてのホスト モードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology (NEAT) のサブリカント スイッチで使用します。

- ホスト許可：許可済み (サブリカントでスイッチに接続する) ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol (CISP) を使用して、サブリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します (図 12-6 を参照してください)。
- 自動イネーブル化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的にイネーブル化します。これにより、サブリカント スイッチから着信する複数の VLAN のユーザートラフィックが許可されます。ACS で **cisco-av-pair** を *device-traffic-class=switch* として設定します (この設定は *group* または *user* 設定で行うことができます)。

図 12-6 CISP を使用したオーセンティケータまたはサブリカント スイッチ



1	ワークステーション (クライアント)	2	サブリカント スイッチ (ワイヤリング クローゼット外)
3	オーセンティケータ スイッチ	4	Access Control Server (ACS)
5	トランク ポート		

注意事項

- NEAT ポートは、他の認証ポートと同じコンフィギュレーションで設定できます。サブリカント スイッチが認証すると、ポート モードはベンダー固有属性 (VSA) に基づいてアクセスからトランクに変更されます (*device-traffic-class=switch*)。
- VSA はオーセンティケータ スイッチ ポート モードをアクセスからトランクに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします (任意の VLAN がネイティブ トランク VLAN に変換される場合)。VSA はサブリカントのポート コンフィギュレーションは変更しません。

- ホスト モードを変更して、オーセンティケータ スイッチ ポートの標準ポート コンフィギュレーションを適用するには、スイッチ VSA ではなく、Auto Smartport ユーザ定義マクロを使用することもできます。これにより、オーセンティケータ スイッチ ポートでサポートされていないコンフィギュレーションを削除して、ポート モードをアクセスからトランクに変更できます。詳細については、『*AutoSmartports Configuration Guide*』を参照してください。

詳細については、「NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定」(P.12-58) を参照してください。

ACL および RADIUS Filter-Id 属性を使用した IEEE 802.1x 認証の使用

スイッチは、入力ポートの IP 標準および IP 拡張ポートの Access Control List (ACL; アクセス コントロール リスト) の両方をサポートします。

- 設定する ACL
- Access Control Server (ACS) からの ACL

シングル ホスト モードでの IEEE 802.1x ポートは、ACS からの ACL を使用して、異なるレベルのサービスを IEEE 802.1x 認証ユーザに提供します。RADIUS サーバは、このタイプのユーザおよびポートを認証する場合、ユーザ ID に基づいた ACL 属性をスイッチに送信します。送信された属性は、ユーザ セッション期間中、ポートに適用されます。セッションが終了、認証が失敗、またはリンクで故障が発生した場合、ポートは無許可になり、スイッチは ACL をポートから削除します。

ACS からの IP 標準および IP 拡張ポート ACL だけが Filter-Id 属性をサポートします。これは ACL の名前または番号を指定します。Filter-id 属性は、方向 (インバウンドまたはアウトバウンド)、およびユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id 属性は、グループの Filter-Id 属性よりも優先されます。
- ACS からの Filter-Id 属性が、すでに設定されている ACL を指定する場合、これは、ユーザ設定 ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id 属性を送信する場合、最後の属性だけが適用されます。

Filter-Id 属性がスイッチで定義されていない場合、認証が失敗し、ポートが無許可ステートに戻ります。

コモン セッション ID

認証マネージャは、使用する認証方式に関係なく、クライアント用にただ 1 つのセッション ID (共通セッション ID と呼ばれます) を使用します。この ID は、表示コマンドや Management Information Base (MIB; 管理情報ベース) などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されます。

セッション ID には、次の情報が含まれます。

- Network Access Device (NAD; ネットワーク アクセス デバイス) の IP アドレス
- 一意の 32 ビット整数 (機械的に増加します)
- セッション開始タイム スタンプ (32 ビット整数)

次に、**show authentication** コマンドの出力にセッション ID が表示される例を示します。この例では、セッション ID は 1600000500000000B288508E5 です。

```
Switch# show authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Fa4/0/4	0000.0000.0203	mab	DATA	Authz Success	1600000500000000B288508E5

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

802.1x 認証の設定

ここでは、次の設定について説明します。

- 「802.1x 認証のデフォルト設定」 (P.12-33)
- 「802.1x 認証設定時の注意事項」 (P.12-34)
- 「802.1x 準備状態チェックの設定」 (P.12-36) (任意)
- 「音声対応 802.1x セキュリティの設定」 (P.12-37) (任意)
- 「802.1x 違反モードの設定」 (P.12-38) (任意)
- 「スイッチおよび RADIUS サーバ間の通信の設定」 (P.12-41) (必須)
- 「ホストモードの設定」 (P.12-42) (任意)
- 「定期的な再認証の設定」 (P.12-43) (任意)
- 「ポートに接続するクライアントの手動での再認証」 (P.12-44) (任意)
- 「待機時間の変更」 (P.12-44) (任意)
- 「スイッチからクライアントへの再送信時間の変更」 (P.12-45) (任意)
- 「スイッチからクライアントへのフレーム再送信回数の設定」 (P.12-46) (任意)
- 「再認証回数の設定」 (P.12-46) (任意)
- 「802.1X アカウンティングの設定」 (P.12-48) (任意)
- 「MAC Move のイネーブル化」 (P.12-47) (任意)
- 「MAC 置換のイネーブル化」 (P.12-48) (任意)
- 「ゲスト VLAN の設定」 (P.12-49) (任意)
- 「制限付き VLAN の設定」 (P.12-50) (任意)
- 「アクセス不能認証バイパス機能の設定」 (P.12-52) (任意)
- 「WoL を使用した 802.1x 認証の設定」 (P.12-55) (任意)
- 「MAC 認証バイパスの設定」 (P.12-56) (任意)
- 「NAC レイヤ 2 802.1x 検証の設定」 (P.12-57) (任意)
- 「NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定」 (P.12-58)
- 「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定」 (P.12-60)
- 「柔軟な認証順序の設定」 (P.12-63)

- 「ポート上での 802.1x 認証のディセーブル化」(P.12-64) (任意)
- 「802.1x 認証設定のデフォルト値へのリセット」(P.12-65) (任意)

802.1x 認証のデフォルト設定

表 12-4 に、802.1x 認証のデフォルト設定を示します。

表 12-4 802.1x 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル (force-authorized) ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ	
<ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • Key 	<ul style="list-style-type: none"> • 指定なし • 1812 • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔 (秒)	3600 秒
再認証回数	2 回 (ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数)
待機時間	60 秒 (スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数)
再送信時間	30 秒 (スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数)
最大再送信回数	2 回 (スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数)
クライアント タイムアウト時間	30 秒 (認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間)
認証サーバ タイムアウト時間	30 秒 (クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間) authentication timer server インターフェイス コンフィギュレーション コマンドを使用すると、このタイムアウト時間を変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ (スイッチ) モード	指定なし

表 12-4 802.1x 認証のデフォルト設定 (続き)

機能	デフォルト設定
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1x 認証」 (P.12-34)
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」 (P.12-35)
- 「MAC 認証バイパス」 (P.12-36)
- 「ポートあたりのデバイスの最大数」 (P.12-36)

802.1x 認証

- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当てられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。
802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポートタイプではサポートされません。
 - トランク ポート：トランク ポート上で 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
 - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
 - ダイナミック アクセス ポート：ダイナミック アクセス (VLAN Query Protocol (VQP)) ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。

- EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。
- Switched Port Analyzer (SPAN; スイッチドポートアナライザ) および Remote SPAN (RSPAN; リモート SPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。「**認証マネージャ CLI コマンド**」(P.12-9) を参照してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- 802.1x 認証をプライベート VLAN ポートに設定できますが、ポートセキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた 802.1x 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN (ルーテッドポート) または トランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を軽減します (**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
 - この機能はシングルホストモードおよびマルチホストモードの 802.1x ポートでサポートされます。
 - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステータスの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
 - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカルポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
 - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカルポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポートステータスをクリティカル認証ステータスに変更し、制限付き VLAN に残ります。

- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

MAC 認証バイパス

- 特に明記していない限り、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。詳細については、「802.1x 認証」(P.12-34) を参照してください。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポートステータスに影響はありません。
- ポートが未許可ステータスであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステータスのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステータスにない場合、再認証が行われるまでポートはこのステータスを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ~ 65535 秒です。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングルホストモードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証 (MDA) モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホストモードの場合、1 台の 802.1x サブリカントだけがポートで許可されます。ただし、アクセス VLAN で許可される 802.1x 非対応ホストの数には制限はありません。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチスタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリに応答しない場合、クライアントは 802.1x に対応していません。Syslog メッセージは生成されません。

- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに回答する各クライアントに生成されます。

スイッチ上で 802.1x 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	dot1x test eapol-capable [interface interface-id]	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 (任意) <i>interface-id</i> には、802.1x 準備状態チェックを実行するポートを指定します。 (注) オプションの interface キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ1	configure terminal	(任意) グローバル コンフィギュレーション モードを開始します。
ステップ2	dot1x test timeout timeout	(任意) EAPOL 応答の待機に使用するタイムアウトを設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルトは 10 秒です。
ステップ3	end	(任意) 特権 EXEC モードに戻ります。
ステップ4	show running-config	(任意) 変更したタイムアウト値を確認します。

次の例では、スイッチ上の準備状態チェックをイネーブルにして、ポートを照会する方法を示します。また、照会済みポートから受信した応答も示し、接続しているデバイスが 802.1x 対応であることを確認します。

```
switch# dot1x test eapol-capable interface gigabitethernet1/2
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL capable
```

音声対応 802.1x セキュリティの設定

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。



(注) **shutdown vlan** キーワードを指定しない場合、errdisable ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、errdisable リカバリを設定すると、ポートは自動的に再びイネーブルにされます。errdisable リカバリがポートで設定されていない場合、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface interface-id vlan [vlan-list]** 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause security-violation shutdown vlan	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 (注) shutdown vlan キーワードを指定しない場合、すべてのポートが errdisable ステートになり、シャットダウンされます。
ステップ 3	errdisable recovery cause security-violation	(任意) 自動 VLAN 単位エラー リカバリをイネーブルにします。
ステップ 4	clear errdisable interface interface-id vlan [vlan-list]	(任意) errdisable になっている個々の VLAN を再びイネーブルにします。 <ul style="list-style-type: none"> • <i>interface-id</i> の場合、個々の VLAN を再びイネーブルにするポートを指定します。 • (任意) <i>vlan-list</i> の場合、再びイネーブルにする VLAN のリストを指定します。<i>vlan-list</i> を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	shutdown no-shutdown	(任意) errdisable の VLAN を再びイネーブルにして、すべての errdisable 指示をクリアします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show errdisable detect	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次の例では、errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet1/2 vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication dot1x {default} method1</code>	802.1x 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用方法になっている方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 <i>method1</i> には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ スtring に表示されますが、サポートされていません。
ステップ 4	<code>interface interface-id</code>	802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>switchport mode access</code>	ポートをアクセス モードにします。
ステップ 6	<code>authentication violation {shutdown restrict protect replace}</code>	違反モードを設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • shutdown : ポートを <code>errordisable</code> にします。 • restrict : Syslog エラーを生成します。 • protect : トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • replace : 現在のセッションを削除し、新しいホストで認証します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show authentication</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の設定

802.1x ポートベース認証を設定するには、認証、許可、アカウントिंग (AAA) をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリ送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

-
- ステップ 1 ユーザがスイッチのポートに接続します。
 - ステップ 2 認証が実行されます。
 - ステップ 3 RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
 - ステップ 4 スイッチが開始メッセージをアカウントング サーバに送信します。
 - ステップ 5 必要に応じて、再認証が実行されます。

- ステップ 6** スイッチが仮のアカウントリング アップデートを、再認証結果に基づいたアカウントリング サーバに送信します。
- ステップ 7** ユーザがポートから切断します。
- ステップ 8** スイッチが停止メッセージをアカウントリング サーバに送信します。

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 aaa new-model	AAA をイネーブルにします。
ステップ 3 aaa authentication dot1x {default} method1	802.1x 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用方法になっている方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 method1 には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ スtring に表示されますが、サポートされていません。
ステップ 4 dot1x system-auth-control	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5 aaa authorization network {default} group radius	(任意) ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定は、デフォルトです。
ステップ 6 radius-server host ip-address	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7 radius-server key string	(任意) RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 8 interface interface-id	802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9 switchport mode access	(任意) ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 10 authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。 機能の相互作用については、「802.1x 認証設定時の注意事項」(P.12-34) を参照してください。
ステップ 11 dot1x pae authenticator	インターフェイスのポート アクセス エンティティを、オーセンティケータとしてのみ動作し、サブリカント用のメッセージは無視するように設定します。
ステップ 12 end	特権 EXEC モードに戻ります。
ステップ 13 show authentication	設定を確認します。
ステップ 14 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host { <i>hostname</i> <i>ip-address</i> } auth-port <i>port-number</i> key <i>string</i>	<p>RADIUS サーバ パラメータを設定します。</p> <p><i>hostname</i> <i>ip-address</i> には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。</p> <p>auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 です。指定できる範囲は 0 ~ 65536 です。</p> <p>key <i>string</i> には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。</p> <p>(注) キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず radius-server host コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。</p> <p>複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバをクリアするには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、IP アドレス 172.20.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号キーを RADIUS サーバ上のキーと同じ *rad123* に設定する例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号化キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」(P.11-37) を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー スtring があります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

802.1X 認証済みポート上でシングルホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。**multi-domain** キーワードを使用して、マルチドメイン認証（MDA）を設定し、同じスイッチ ポート上の IP Phone（シスコ製品または他社製品）など、ホストと音声デバイスの両方の認証をイネーブルにします。

この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server vsa send authentication	VSA（Vendor-Specific Attribute; ベンダー固有属性）を認識し使用するために、ネットワーク アクセス サーバを設定します。
ステップ 3	interface interface-id	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	authentication host-mode [multi-auth multi-domain multi-host single-host]	<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> multi-auth : 音声 VLAN で 1 クライアント、データ VLAN で複数の認証クライアントを許可します。各ホストは個別に認証されます。 <p>(注) multi-auth キーワードを使用できるのは、authentication host-mode コマンドだけです。</p> <ul style="list-style-type: none"> multi-host : シングル ホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。 multi-domain : IP Phone（シスコ製または他社製）など、ホストおよび音声の両方のデバイスを 802.1x 許可ポートで認証できるようにします。 <p>(注) ホスト モードが multi-domain に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細については、第 18 章「音声 VLAN の設定」を参照してください。</p> <ul style="list-style-type: none"> single-host : 802.1x 許可ポートでシングル ホスト（クライアント）の接続を許可します。 <p>指定するインターフェイスで、authentication port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。</p>
ステップ 5	switchport voice vlan vlan-id	(任意) 音声 VLAN を設定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface interface-id	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートで複数のホストをディセーブルにするには、**no authentication host-mode** または **no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1x 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにして、ポートでホストおよび音声デバイスの両方を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	authentication periodic	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 (注) デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチで RADIUS-provided セッション タイムアウトを使用するには、 authentication timer reauthenticate コマンドを入力します。
ステップ4	authentication timer {{{inactivity reauthenticate}}} {restart value}}	再認証の試行の間隔（秒）を設定します。 authentication timer キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> inactivity : クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒単位）。 reauthenticate : 自動再認証が開始するまでの時間（秒単位）。 restart value : 無許可ポートの認証を試行するまでの間隔（秒単位）。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show authentication interface interface-id	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

定期的な再認証をディセーブルにするには、**no authentication periodic** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの再認証試行間隔に戻すには、**no authentication timer** インターフェイス コンフィギュレーション コマンドを使用します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 4000
```

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface interface-id 特権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「[定期的な再認証の設定](#)」(P.12-43) を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet1/2
```

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer inactivity** インターフェイス コンフィギュレーション コマンドは、アイドル時間を制御します。クライアント認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	authentication timer inactivity seconds	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの待機時間に戻すには、**no authentication timer inactivity** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Switch(config-if)# authentication timer inactivity 30
```

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。



(注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	authentication timer reauthenticate seconds	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 5 秒です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show authentication interface interface-id	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの再送信時間に戻すには、**no authentication timer reauthenticate** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

```
Switch(config-if)# authentication timer reauthenticate 60
```

スイッチからクライアントへのフレーム再送信回数の設定

(クライアントから応答が得られなかった場合に) スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。



(注)

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	dot1x max-reauth-req count	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数をデフォルトに戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 5 に設定する例を示します。

```
Switch(config-if)# dot1x max-reauth-req 5
```

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。



(注)

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	dot1x max-req count	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォルトは 2 です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show authentication interface interface-id	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再認証回数をデフォルトに戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

MAC Move のイネーブル化

MAC Move を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC Move をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	authentication mac-move permit	スイッチで MAC Move をイネーブルにします。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	(任意) 設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチで MAC Move をグローバルにイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>authentication violation {protect replace restrict shutdown}</code>	<p>インターフェイス上で MAC 置換をイネーブルにするには、replace キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。</p> <p>他のキーワードは、次のような機能があります。</p> <ul style="list-style-type: none"> • protect : ポートは、システム メッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • restrict : 違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • shutdown : ポートは、予期しない MAC アドレスを受信すると <code>errdisable</code> になります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で MAC 置換をイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# authentication violation replace
```

802.1X アカウンティングの設定

802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ログインのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```



(注)

ログインの開始、停止、仮のアップデートメッセージ、タイムスタンプなどのアカウントリングタスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のログインをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	aaa accounting dot1x default start-stop group radius	すべての RADIUS サーバのリストを使用して、802.1x アカウンティングをイネーブルにします。
ステップ4	aaa accounting system default start-stop group radius	(任意) システム アカウンティングをイネーブルにし (すべての RADIUS サーバのリストを使用)、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** 特権 EXEC コマンドを使用します。

次に、802.1x アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホストモードまたはマルチ ホストモードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1x 認証設定時の注意事項 」(P.12-34) を参照してください。

	コマンド	目的
ステップ 3	switchport mode access または switchport mode private-vlan host	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
ステップ 5	authentication event no-response action authorize vlan <i>vlan-id</i>	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface <i>interface-id</i>	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ゲスト VLAN をディセーブルにして削除するには、**no authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication event no-response action authorize vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間 (秒) を 15 に設定し、802.1x ポートの DHCP クライアント接続時に、VLAN 2 を 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# authentication timer inactivity 3
Switch(config-if)# authentication timer reauthenticate 15
Switch(config-if)# authentication event no-response action authorize vlan 2
```

制限付き VLAN の設定

スイッチ上に制限付き VLAN を設定している、認証サーバが有効なユーザ名またはパスワードを受信できない場合と、802.1X に準拠した場合クライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.12-34) を参照してください。
ステップ 3	switchport mode access または switchport mode private-vlan host	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。

	コマンド	目的
ステップ4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
ステップ5	authentication event fail action authorize <i>vlan-id</i>	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、プライマリプライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show authentication interface <i>interface-id</i>	(任意) 設定を確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

制限付き VLAN をディセーブルにして削除するには、**no authentication event fail action authorize *vlan-id*** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、*VLAN 2* を IEEE 802.1x 制限付き VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# authentication event fail action authorize 2
```

ユーザに制限付き VLAN を割り当てる前に、**authentication event retry *retry count*** インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる認証試行回数は 1 ~ 3 回です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.12-34) を参照してください。
ステップ3	switchport mode access または switchport mode private-vlan host	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
ステップ5	authentication event fail action authorize <i>vlan-id</i>	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、プライマリプライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ6	authentication event retry <i>retry count</i>	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ~ 3 です。デフォルトは 3 です。
ステップ7	end	特権 EXEC モードに戻ります。
ステップ8	show authentication interface <i>interface-id</i>	(任意) 設定を確認します。
ステップ9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、**no authentication event retry** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートを制限付き VLAN にするために、認証試行回数を 2 に設定する方法を示します。

```
Switch(config-if)# authentication event retry 2
```

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）を設定できます。

ポートをクリティカルポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server dead-criteria time time tries tries	(任意) RADIUS サーバが使用できない、または <i>dead</i> と見なされるときを判別するのに使われる条件を設定します。 指定できる <i>time</i> の範囲は 1 ~ 120 秒です。スイッチは、デフォルトの <i>seconds</i> 値を 10 ~ 60 秒の間で動的に決定します。 指定できる <i>tries</i> の範囲は 1 ~ 100 です。スイッチは、デフォルトの <i>tries</i> パラメータを 10 ~ 100 の間で動的に決定します。
ステップ 3	radius-server deadtime minutes	(任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ~ 1440 分 (24 時間) です。デフォルト値は 0 分です。

コマンド	目的
ステップ4 radius-server host <i>ip-address</i> [acct-port <i>udp-port</i> [auth-port <i>udp-port</i>] [test username <i>name</i> [idle-time <i>time</i>] [ignore-acct-port] [ignore-auth-port]] [key <i>string</i>]	<p>(任意) 次のキーワードを使用して RADIUS サーバパラメータを設定します。</p> <ul style="list-style-type: none"> • acct-port <i>udp-port</i> : RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ~ 65536 です。デフォルト値は 1646 です。 • auth-port <i>udp-port</i> : RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ~ 65536 です。デフォルト値は 1645 です。 <p>(注) RADIUS アカウンティングサーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。</p> <ul style="list-style-type: none"> • test username <i>name</i> : RADIUS サーバステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • idle-time <i>time</i> : スイッチがテストパケットをサーバに送信した後の間隔を分数で設定します。指定できる範囲は 1 ~ 35791 分です。デフォルトは 60 分 (1 時間) です。 • ignore-acct-port : RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • ignore-auth-port : RADIUS サーバ認証ポートのテストをディセーブルにします。 • key <i>string</i> : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号キーを指定します。 <p>(注) キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず radius-server host コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。</p> <p>radius-server key {0 <i>string</i> 7 <i>string</i> <i>string</i>} グローバル コンフィギュレーション コマンドを使用しても認証および暗号キーを設定できます。</p>
ステップ5 dot1x critical { eapol recovery delay <i>milliseconds</i> }	<p>(任意) アクセス不能認証バイパスのパラメータを設定します。</p> <p>eapol : スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。</p> <p>recovery delay <i>milliseconds</i> : 使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ~ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です (ポートは毎秒再初期化できます)。</p>
ステップ6 interface <i>interface-id</i>	<p>設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.12-34) を参照してください。</p>
ステップ7 authentication event server dead action [authorize reinitialize] vlan <i>vlan-id</i>	<p>これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。</p> <ul style="list-style-type: none"> • authorize : 認証しようとする新しいホストをユーザ指定のクリティカル VLAN に移動します。 • reinitialize : ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。

	コマンド	目的
ステップ 8	authentication event server dead action {authorize reinitialize} vlan <i>vlan-id</i>	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。 <ul style="list-style-type: none"> • authorize : ポートを認証します。 • reinitialize : すべての許可済みのクライアントを再初期化します。
ステップ 9	authentication server dead action authorize [vlan]	ACS サーバがダウンしている場合は、アクセス VLAN または設定された VLAN (VLAN が指定されている場合) のスイッチを許可します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show authentication interface <i>interface-id</i>	(任意) 設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスをデフォルトの設定に戻すには、**no authentication event server dead action {authorize | reinitialize}** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 1/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1x 認証設定時の注意事項 」(P.12-34) を参照してください。
ステップ3	<code>authentication control-direction {both in}</code>	<p>ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。</p> <ul style="list-style-type: none"> both : ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 in : ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show authentication interface interface-id</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

WoL を使用した 802.1x 認証をディセーブルにするには、**no authentication control-direction** インターフェイス コンフィギュレーション コマンドを使用します。

次に、WoL を使用した 802.1x 認証をイネーブルにして、ポートを双方向に設定する例を示します。

```
Switch(config-if)# authentication control-direction both
```

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1x 認証設定時の注意事項」(P.12-34) を参照してください。
ステップ 3	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
ステップ 4	authentication order [mab] {webauth}	認証方式の順序を設定します。 <ul style="list-style-type: none"> mab : 認証方式の順序に MAC Authentication Bypass (MAB; MAC 認証バイパス) を追加します。 webauth : 認証方式の順序に Web 認証を追加します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show authentication interface interface-id	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MAC 認証バイパスをディセーブルにするには、**no authentication order** インターフェイス コンフィギュレーション コマンドを使用します。

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Switch(config-if)# authentication order
```

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	vlan group vlan-group-name vlan-list vlan-list	VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。
ステップ 2	show vlan group all vlan-group-name	設定を確認します。
ステップ 3	no vlan group vlan-group-name vlan-list vlan-list	VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                Vlans Mapped
-----
eng-dept                  10
```

```
switch# show dot1x vlan-group all
Group Name                Vlans Mapped
-----
eng-dept                  10
hr-dept                   20
```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                Vlans Mapped
-----
eng-dept                  10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
```

```
switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	authentication event no-response action authorize vlan vlan-id	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ4	authentication periodic	クライアントの定期的な再認証 (デフォルトではディセーブル) をイネーブルにします。
ステップ5	authentication timer reauthenticate	クライアントに対する再認証試行を設定します (1 時間に設定)。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。

	コマンド	目的
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface <i>interface-id</i>	802.1x 認証の設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、NAC レイヤ 2 IEEE 802.1x 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate
```

NEAT を使用したオーセンティケータ スイッチおよびサブリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサブリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。

概要については、「[Network Edge Access Topology \(NEAT\) を使用した 802.1x サブリカントおよびオーセンティケータ](#)」(P.12-29) を参照してください。



(注)

cisco-av-pairs は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、サブリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cisp enable	CISP をイネーブルにします。
ステップ 3	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switchport mode access	ポート モードを access に設定します。
ステップ 5	authentication port-control auto	ポート認証モードを auto に設定します。
ステップ 6	dot1x pae authenticator	インターフェイスを Port Access Entity (PAE; ポート アクセス エンティティ) をオーセンティケータとして設定します。
ステップ 7	spanning-tree portfast	単一ワークステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show running-config interface <i>interface-id</i>	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、スイッチを 802.1x オーセンティケータとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
```

```
Switch(config)# interface gigabitethernet1/1

Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサブリカントに設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cisp enable	CISP をイネーブルにします。
ステップ 3	dot1x credentials profile	802.1x クレデンシヤル プロファイルを作成します。これは、サブリカントとして設定されるポートに接続する必要があります。
ステップ 4	username suppswitch	ユーザ名を作成します。
ステップ 5	password password	新しいユーザ名のパスワードを作成します。
ステップ 6	dot1x supplicant force-multicast	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。これにより、NEAT がすべてのホスト モードでのサブリカント スイッチで機能できるようにもなります。
ステップ 7	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	switchport trunk encapsulation dot1q	ポートをトランク モードにします。
ステップ 9	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	dot1x pae supplicant	インターフェイスをポート アクセス エンティティ (PAE) をサブリカントとして設定します。
ステップ 11	dot1x credentials profile-name	802.1x クレデンシヤル プロファイルをインターフェイスに接続します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show running-config interface interface-id	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチをサブリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Auto Smartport マクロを使用した NEAT の設定

スイッチ VSA ではなく Auto Smartport ユーザ定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。詳細については、『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。詳細については、[Cisco Secure ACS コンフィギュレーションガイド](#)を参照してください。



(注) スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、`show ip access-list` 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示します。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキング テーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip device tracking</code>	IP デバイス トラッキング テーブルを設定します。
ステップ 3	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa authorization network default group radius</code>	許可の方法をローカルに設定します。許可の方法を削除するには、 <code>no aaa authorization network default group radius</code> コマンドを使用します。
ステップ 5	<code>radius-server vsa send authentication</code>	<code>radius vsa send authentication</code> を設定します。
ステップ 6	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<code>ip access-group acl-id in</code>	ポートの入力方向のデフォルト ACL を設定します。 (注) <code>acl-id</code> はアクセス リストの名前または番号です。
ステップ 8	<code>show running-config interface interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	access-list access-list-number deny source source-wildcard log	<p>送信元アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。</p> <p>access-list-number には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。</p> <p>条件が一致した場合にアクセスを拒否する場合は deny、許可する場合は permit を指定します。</p> <p>source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。</p> <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビット長の値。 source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。 source-wildcard 値を入力する必要はありません。 source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。 <p>(任意) source-wildcard ビットを送信元アドレスに適用します。</p> <p>(任意) ログを入力して、エントリと一致するパケットに関する情報ロギング メッセージをコンソールに送信します。</p>
ステップ3	interface interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ip access-group acl-id in	<p>ポートの入力方向のデフォルト ACL を設定します。</p> <p>(注) acl-id はアクセス リストの名前または番号です。</p>
ステップ5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ6	aaa new-model	AAA をイネーブルにします。
ステップ7	aaa authorization network default group radius	許可の方法をローカルに設定します。許可の方法を削除するには、 no aaa authorization network default group radius コマンドを使用します。
ステップ8	ip device tracking	<p>IP デバイス トラッキング テーブルをイネーブルにします。</p> <p>IP デバイス トラッキング テーブルをディセーブルにするには、no ip device tracking グローバル コンフィギュレーション コマンドを使用します。</p>
ステップ9	ip device tracking probe [count interval use-svi]	<p>(任意) IP デバイス トラッキング テーブルを設定します。</p> <ul style="list-style-type: none"> count count : スイッチが ARP プロブを送信する回数を設定します。指定できる範囲は 1 ~ 5 です。デフォルトは 3 です。 interval interval : スイッチが ARP プロブを再送信するまでに応答を待機する時間 (秒単位) を設定します。指定できる範囲は 30 ~ 300 秒です。デフォルトは 30 秒です。 use-svi : Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) の IP アドレスを ARP プロブの送信元として使用します。
ステップ10	radius-server vsa send authentication	<p>ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。</p> <p>(注) ダウンロード可能な ACL が機能する必要があります。</p>

	コマンド	目的
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show ip device tracking all	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ダウンロード ポリシーのスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/1

Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mab request format attribute 32 vlan access-vlan	VLAN ID ベース MAC 認証をイネーブルにします。
ステップ 3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN ID ベース MAC 認証のステータスを確認する show コマンドはありません。 **debug radius accounting** 特権 EXEC コマンドを使用して RADIUS 属性 32 を確認できます。このコマンドの詳細については、『Cisco IOS Debug Command Reference, Release 12.2』を参照してください。
http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次の例では、スイッチで VLAN ID ベース MAC 認証をグローバルにイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

柔軟な認証順序の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>authentication order [dot1x mab] {webauth}</code>	(任意) ポート上で使用される認証方式の順序を設定します。
ステップ 4	<code>authentication priority [dot1x mab] {webauth}</code>	(任意) 認証方式をポート プライオリティ リストに追加します。
ステップ 5	<code>show authentication</code>	(任意) 設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ポートが最初に 802.1x 認証を試行してから Web 認証をフォールバック方法として設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1

Switch(config)# authentication order dot1x webauth
```

Open1x の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>authentication control-direction {both in}</code>	(任意) ポート制御を単方向モードまたは双方向モードに設定します。
ステップ 4	<code>authentication fallback name</code>	(任意) 802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 5	<code>authentication host-mode [multi-auth multi-domain multi-host single-host]</code>	(任意) ポート上で認証マネージャ モードを設定します。
ステップ 6	<code>authentication open</code>	(任意) ポート上でオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	<code>authentication order [dot1x mab] {webauth}</code>	(任意) ポート上で使用される認証方式の順序を設定します。
ステップ 8	<code>authentication periodic</code>	(任意) ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 9	<code>authentication port-control {auto force-authorized force-un authorized}</code>	(任意) ポートの許可ステータスの手動制御をイネーブルにします。

	コマンド	目的
ステップ 10	show authentication	(任意) 設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次の例では、ポートの Open1x を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1

Switch(config)# authentication control-direction both
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no dot1x pae	ポート上で 802.1x 認証をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

802.1x Port Access Entity (PAE; ポート アクセス エンティティ) オーセンティケータとしてポートを設定するには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで 802.1x がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次の例では、ポートの 802.1x 認証をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/1

Switch(config-if)# no dot1x pae authenticator
```

802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ3	dot1x default	802.1x パラメータをデフォルト値に戻します。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show authentication interface interface-id	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x の統計情報およびステータスの表示

すべてのポートに関する 802.1x 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。特定のポートに関する 802.1x 統計情報を表示するには、**show dot1x statistics interface interface-id** 特権 EXEC コマンドを使用します。

スイッチに関する 802.1x 管理および動作ステータスを表示するには、**show dot1x all [details | statistics | summary]** 特権 EXEC コマンドを使用します。特定のポートに関する 802.1x 管理および動作ステータスを表示するには、**show dot1x interface interface-id** 特権 EXEC コマンドを使用します。

Cisco IOS Release 12.2(55)SE 以降では、**no dot1x logging verbose** グローバル コンフィギュレーション コマンドを使用して、冗長な 802.1x 認証メッセージをフィルタリングできます。「[認証マネージャ CLI コマンド](#)」(P.12-9) を参照してください。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 13

Web ベース認証の設定

この章では、Web ベース認証を設定する方法について説明します。内容は次のとおりです。

- 「Web ベース認証の概要」 (P.13-1)
- 「Web ベース認証の設定」 (P.13-9)
- 「Web ベース認証ステータスの表示」 (P.13-17)



(注)

この章で使用するスイッチ コマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

Web ベース認証の概要

IEEE 802.1x サブリカントが実行されていないホスト システムのエンド ユーザを認証するには、*Web 認証プロキシ*と呼ばれる Web ベース認証機能を使用します。



(注)

Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング) サーバに送信されます。

認証に成功した場合、Web ベース認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、ウォッチ リストに載せられます。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

- 「デバイスの役割」 (P.13-2)
- 「ホストの検出」 (P.13-2)
- 「セッションの作成」 (P.13-3)
- 「認証プロセス」 (P.13-3)

- 「Web 認証カスタマイズ可能な Web ページ」 (P.13-6)
- 「その他の機能と Web ベース認証の相互作用」 (P.13-7)

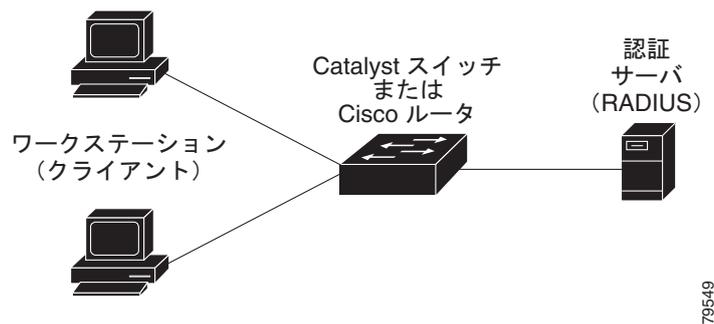
デバイスの役割

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- **クライアント**: LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス (ワークステーション)。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- **認証サーバ**: クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可するか、拒否するかをスイッチに通知します。
- **スイッチ**: クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介装置 (プロキシ) として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 13-1 は、ネットワークでのこれらのデバイスの役割を示しています。

図 13-1 Web ベース認証デバイスの役割



79549

ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス トラッキング テーブルを維持します。



(注)

デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- **ARP ベースのトリガー**: ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- **ダイナミック ARP インスペクション**。
- **DHCP スヌーピング**: スイッチにより、このホストに対する DHCP バインディング エントリが作成されると、Web ベース認証に通知が送られます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。
ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。
- 認証バイパスをレビューします。
ホスト IP が例外リストに含まれていない場合、Web ベース認証は NonResponsive-Host (NRH; 応答しないホスト) 要求をサーバに送信します。
サーバの応答が *access accepted* であった場合、認証はこのホストにバイパスされます。セッションが確立されます。
- HTTP インターセプト ACL を設定します。
NRH 要求に対するサーバの応答が *access rejected* であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログイン ページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは、認証サーバからこのユーザのアクセス ポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます。
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチは、ログイン期限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイムアウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答しない場合、AAA 失敗ポリシーが設定されていれば、スイッチは失敗アクセス ポリシーにホストを適用します。ログインの成功ページがユーザに送信されます（「ローカル Web 認証バナー」(P.13-4) を参照）。
- ホストがレイヤ 2 インターフェイス上の ARP プロローブに回答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

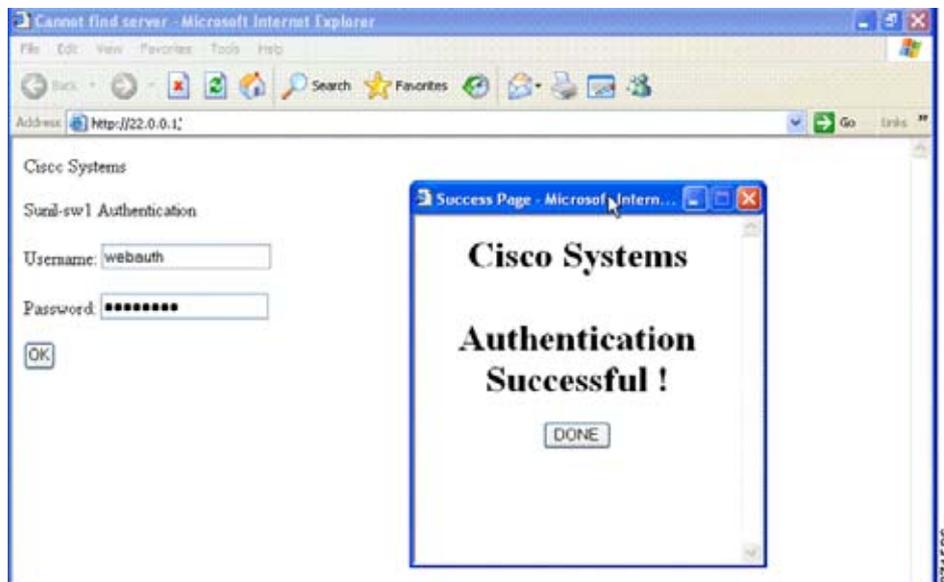
ローカル Web 認証バナー

Web 認証を使用してスイッチにログインしたときに表示されるバナーを作成できます。このバナーは、ログイン ページと認証結果ポップアップ ページの両方に表示されます。

- 認証成功
- 認証失敗
- 認証期限切れ

ip admission auth-proxy-banner http グローバル コンフィギュレーション コマンドを使用して、バナーを作成できます。ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は、[図 13-2](#) に示すように、認証結果のポップアップ ページに表示されます。

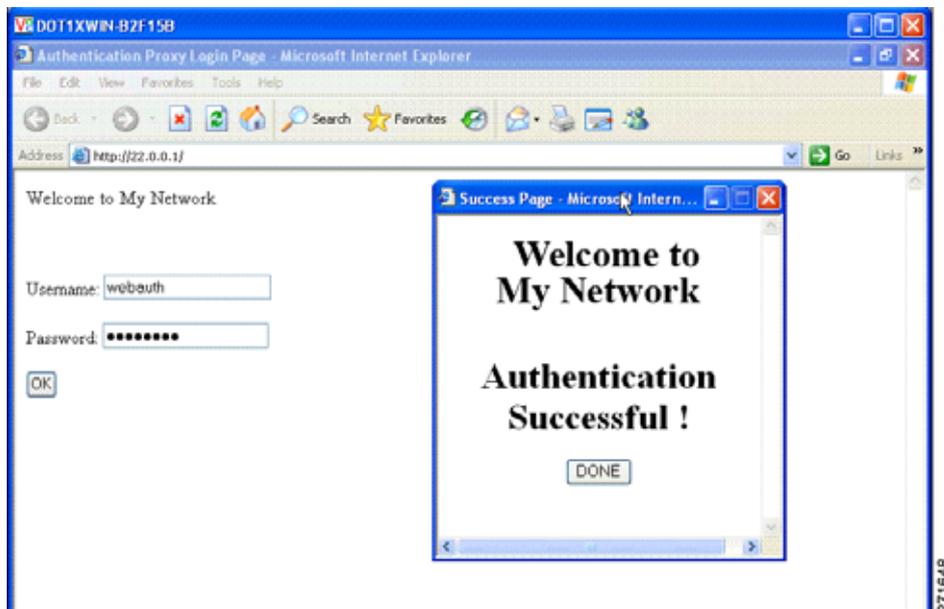
図 13-2 認証成功バナー



また、[図 13-3](#) に示すように、バナーをカスタマイズすることもできます。

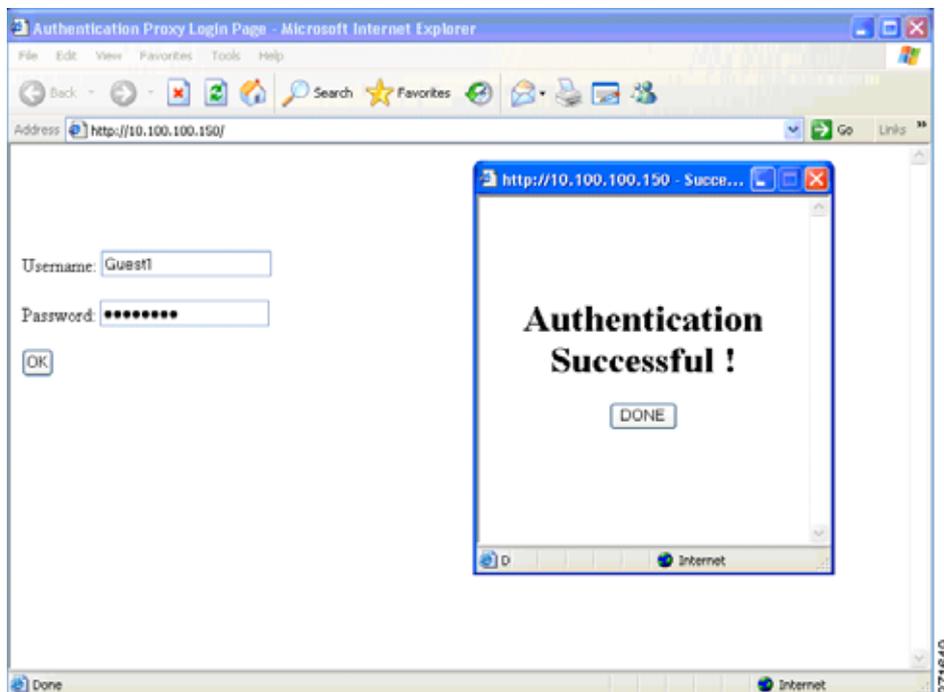
- スイッチ、ルータ、または企業名をバナーに追加するには、**ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用します。
- ログ、またはテキスト ファイルをバナーに追加するには、**ip admission auth-proxy-banner http file-path** グローバル コンフィギュレーション コマンドを使用します。

図 13-3 カスタマイズされた Web パナー



パナーがイネーブルにされていない場合、図 13-4 に示すように、Web 認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはパナーは表示されません。

図 13-4 パナーが表示されていないログイン画面



詳細については、『Cisco IOS Security Command Reference』および「Web 認証ローカル パナーの設定」(P.13-16) を参照してください。

Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステータスを通知します。

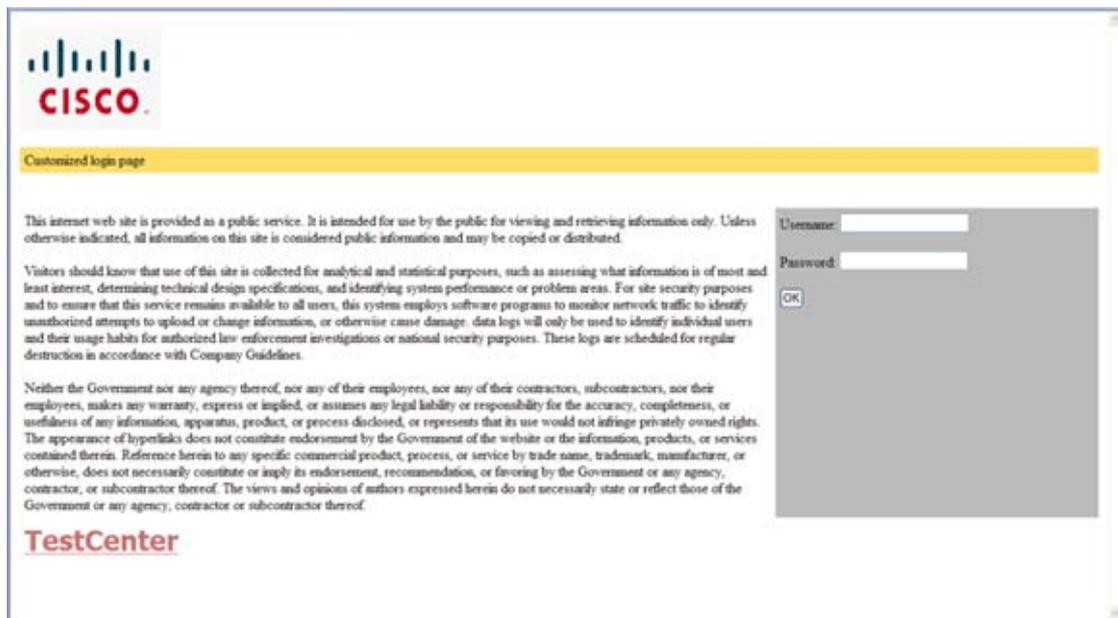
- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました。

注意事項

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：<http://www.cisco.com>）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります。
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- 設定されたページには、スタック マスターまたはメンバ上のフラッシュからアクセスできます。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システム ディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、`web_auth_<filename>` の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

図 13-5 (P.13-7) に示すように、デフォルトの内部 HTML ページを独自の HTML ページで置き換えることができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 13-5 カスタマイズ可能な認証ページ



詳細については、「[認証プロキシ Web ページのカスタマイズ](#)」(P.13-14) を参照してください。

その他の機能と Web ベース認証の相互作用

- 「ポートセキュリティ」(P.13-7)
- 「LAN ポート IP」(P.13-7)
- 「ゲートウェイ IP」(P.13-8)
- 「ACL」(P.13-8)
- 「コンテキストベース アクセス コントロール」(P.13-8)
- 「802.1x 認証」(P.13-8)
- 「EtherChannel」(P.13-8)

ポート セキュリティ

Web ベース認証とポートセキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポートセキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワークアクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

ポートセキュリティをイネーブルにする手順については、「[ポートセキュリティの設定](#)」(P.29-9) を参照してください。

LAN ポート IP

LAN Port IP (LPIP; LAN ポート IP) とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホストポリシーは、Web ベース認証のホストポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ホスチャが再度検証されます。

ゲートウェイ IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上に Gateway IP (GWIP; ゲートウェイ IP) を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、Port ACL (PACL; ポート ACL) をデフォルトのアクセス ポリシーとして設定する必要があります。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。



(注)

プロキシ ACL を Web ベース認証クライアント用に設定すると、プロキシ ACL は認可プロセスの一部としてダウンロードされ、適用されます。したがって、PACL はプロキシ ACL のアクセス コントロール エントリ (ACE) を表示します。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

802.1x 認証

フォールバック認証メソッドとして設定する場合を除き、Web ベース認証は 802.1x 認証と同じポート上には設定できません。フォールバック認証メソッドとして設定する場合を除き、Web ベース認証は 802.1x 認証と同じポート上には設定しないことを推奨します。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャンネルに適用されます。

Web ベース認証の設定

- 「デフォルトの Web ベース認証の設定」 (P.13-9)
- 「Web ベース認証の設定に関する注意事項と制約事項」 (P.13-9)
- 「Web ベース認証の設定タスク リスト」 (P.13-10)
- 「認証ルールとインターフェイスの設定」 (P.13-10)
- 「AAA 認証の設定」 (P.13-11)
- 「スイッチおよび RADIUS サーバ間の通信の設定」 (P.13-12)
- 「HTTP サーバの設定」 (P.13-13)
- 「Web ベース認証パラメータの設定」 (P.13-16)
- 「Web ベース認証キャッシュ エントリの削除」 (P.13-17)

デフォルトの Web ベース認証の設定

表 13-1 は、デフォルトの Web ベース認証の設定を示しています。

表 13-1 デフォルトの Web ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ	
<ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • Key 	<ul style="list-style-type: none"> • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。
- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスに対してポート ACL を設定するか、またはレイヤ 3 インターフェイスに対して Cisco IOS ACL を設定します。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要があります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホスト トラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レイヤ 2 (STP) トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。
- Web ベース認証は、ダウンロード可能なホスト ポリシーとして、VLAN 割り当てをサポートしていません。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。
- Web ベース認証および Network Edge Access Topology (NEAT) は、相互に排他的です。インターフェイス上で NEAT がイネーブルの場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- Web ベース認証は、RADIUS 認可サーバだけをサポートします。TACACS+ サーバまたはローカル認可は使用できません。

Web ベース認証の設定タスク リスト

- 「認証ルールとインターフェイスの設定」 (P.13-10)
- 「AAA 認証の設定」 (P.13-11)
- 「スイッチおよび RADIUS サーバ間の通信の設定」 (P.13-12)
- 「HTTP サーバの設定」 (P.13-13)
- 「Web ベース認証パラメータの設定」 (P.13-16)
- 「Web ベース認証パラメータの設定」 (P.13-16)
- 「Web ベース認証キャッシュ エントリの削除」 (P.13-17)

認証ルールとインターフェイスの設定

	コマンド	目的
ステップ 1	<code>ip admission name name proxy http</code>	Web ベース認証で使用される認証ルールを設定します。
ステップ 2	<code>interface type slot/port</code>	インターフェイス コンフィギュレーション モードを開始し、Web ベースの認証のためにイネーブルにされる入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 <i>type</i> には、 <code>fastethernet</code> 、 <code>gigabit ethernet</code> 、または <code>tengigabitethernet</code> を指定できます。
ステップ 3	<code>ip access-group name</code>	デフォルト ACL を適用します。
ステップ 4	<code>ip admission name</code>	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 5	<code>exit</code>	コンフィギュレーション モードに戻ります。
ステップ 6	<code>ip device tracking</code>	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	show ip admission configuration	コンフィギュレーションを表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Fast Ethernet ポート 5/1 で Web ベース認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name webauth1
http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

	コマンド	目的
ステップ 1	aaa new-model	AAA 機能をイネーブルにします。
ステップ 2	aaa authentication login default group {tacacs+ radius}	ログイン時の認証方法のリストを定義します。
ステップ 3	aaa authorization auth-proxy default group {tacacs+ radius}	Web ベースの認証で使用される認証方法のリストを作成します。
ステップ 4	radius-server host {hostname ip-address} test username username	AAA サーバを指定します。 リモート RADIUS サーバホストのホスト名または IP アドレスを指定します。 test username username は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された username は有効なユーザ名である必要はありません。
ステップ 5	radius-server key string	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、AAA をイネーブルにする方法を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
```

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバの識別情報は次のとおりです。

- ホスト名
- ホストの IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>ip radius source-interface interface_name</code>	RADIUS パケットが、指示されたインターフェイスの IP アドレスを持つことを指定します。
ステップ 2	<code>radius-server host {hostname ip-address} test username username</code>	リモート RADIUS サーバ ホストのホスト名または IP アドレスを指定します。 test username username は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された username は有効なユーザ名である必要はありません。 key オプションは、スイッチと RADIUS サーバの間で使用される認証と暗号キーを指定します。 複数の RADIUS サーバを使用するには、それぞれのサーバでこのコマンドを入力してください。
ステップ 3	<code>radius-server key string</code>	RADIUS サーバ上で動作するスイッチと RADIUS デモンの間で使用される認証および暗号キーを設定します。
ステップ 4	<code>radius-server vsa send authentication</code>	RADIUS サーバからの ACL のダウンロードをイネーブルにします。この機能は、Cisco IOS Release 12.2(50)SG でサポートされています。
ステップ 5	<code>radius-server dead-criteria tries num-tries</code>	RADIUS サーバに送信されたメッセージへの応答がない場合に、このサーバが非アクティブであると見なすまでの送信回数を指定します。指定できる num-tries の範囲は 1 ~ 100 です。

RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。

- 別のコマンドラインには、**key string** を指定します。

- **key string** には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号化キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。
- **key string** を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、『Cisco IOS Security Configuration Guide Release 12.2』および『Cisco IOS Security Command Reference Release 12.2』を参照してください

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html



(注)

RADIUS サーバでは、スイッチ IP アドレス、サーバとスイッチで共有される key string、および Downloadable ACL (DACL; ダウンロード可能な ACL) などの設定を行う必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

次の例では、スイッチで RADIUS サーバ パラメータを設定する方法を示します。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

	コマンド	目的
ステップ1	ip http server	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ2	ip http secure-server	HTTPS をイネーブルにします。

カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。



(注)

ip http secure-secure コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログイン ページは必ず HTTPS (セキュア HTTP) 形式になるようにします。

- [認証プロキシ Web ページのカスタマイズ](#)
- [成功ログインに対するリダイレクション URL の指定](#)

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、スイッチのデフォルト HTML ページではなく、代わりに HTML ページがユーザに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、まず、カスタム HTML ファイルをスイッチのフラッシュ メモリに保存し、次にグローバル コンフィギュレーション モードでこのタスクを実行します。

	コマンド	目的
ステップ 1	ip admission proxy http login page file <i>device:login-filename</i>	スイッチのメモリ ファイル システムで、デフォルトのログイン ページの代わりに使用されるカスタム HTML ファイルの所在地を指定します。 <i>device:</i> はフラッシュ メモリです。
ステップ 2	ip admission proxy http success page file <i>device:success-filename</i>	デフォルトのログイン成功ページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。
ステップ 3	ip admission proxy http failure page file <i>device:fail-filename</i>	デフォルトのログイン失敗ページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。
ステップ 4	ip admission proxy http login expired page file <i>device:expired-filename</i>	デフォルトのログイン期限切れページの代わりに使用されるカスタムの HTML ファイルの所在地を指定します。

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個の HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージはすべて、アクセス可能な HTTP サーバ上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定された `auth-proxy-banner` は使用されません。
- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの `no` 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログイン フォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを `uname` および `pwd` として示す必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

次の例では、カスタム認証プロキシ Web ページを設定する方法を示します。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
```

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

次の例では、カスタム認証プロキシ Web ページの設定を確認する方法を示します。

```
Switch# show ip admission configuration
Authentication proxy webpage
  Login page           : flash:login.htm
  Success page         : flash:success.htm
  Fail Page            : flash:fail.htm
  Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

成功ログインに対するリダイレクション URL の指定

認証後に、内部成功 HTML ページを効果的に置き換え、ユーザのリダイレクト先となる URL を指定することができます。

コマンド	目的
<code>ip admission proxy http success redirect <i>url-string</i></code>	デフォルトのログイン成功ページの代わりに、ユーザのリダイレクト先となる URL を指定します。

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタムログイン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルに設定されている場合、設定された `auth-proxy-banner` は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの `no` 形式を使用します。

次の例では、成功したログインに対するリダイレクション URL を設定する方法を示します。

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

次の例では、成功したログインに対するリダイレクション URL を確認する方法を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Web ベース認証パラメータの設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライアントは待機期間中、ウォッチ リストに載せられます。

	コマンド	目的
ステップ 1	<code>ip admission max-login-attempts number</code>	失敗できるログイン試行の最高回数を設定します。指定できる範囲は 1 ~ 2147483647 回です。デフォルトは 5 です。
ステップ 2	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 3	<code>show ip admission configuration</code>	認証プロキシ設定を表示します。
ステップ 4	<code>show ip admission cache</code>	認証エントリのリストを表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、失敗ログイン試行の最大回数を 10 に設定する方法を示します。

```
Switch(config)# ip admission max-login-attempts 10
```

Web 認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip admission auth-proxy-banner http [banner-text file-path]</code>	ローカル バナーをイネーブルにします。 (任意) <i>C</i> <code>banner-text</code> <i>C</i> と入力して、カスタム バナーを作成します。ここで、 <i>C</i> は区切り文字、またはバナーに表示されるファイル (例: ログ、またはテキスト ファイル) を示すファイルパスです。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、「*My Switch*」というカスタム メッセージが表示されているローカル バナーを設定する方法を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

`ip auth-proxy auth-proxy-banner` コマンドの詳細については、Cisco.com の『[Cisco IOS Security Command Reference](#)』の「Authentication Proxy Commands」を参照してください。

Web ベース認証キャッシュ エントリの削除

コマンド	目的
<code>clear ip auth-proxy cache {* host ip address}</code>	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。
<code>clear ip admission cache {* host ip address}</code>	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。

次に、IP アドレス 209.165.201.1 のクライアントに対する Web ベース認証セッションを削除する例を示します。

```
Switch# clear ip auth-proxy cache 209.165.201.1
```

Web ベース認証ステータスの表示

すべてのインターフェイス、または特定のポートに対する Web ベースの認証設定を表示する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>show authentication sessions [interface type slot/port]</code>	Web ベース認証設定を表示します。 type には、fastethernet、gigabitethernet、または tengigabitethernet を指定できます。 (任意) 特定のインターフェイスに対する Web ベース認証設定を表示するには、キーワード interface を使用します。

次に、グローバルな Web ベース認証のステータスだけを表示する例を示します。

```
Switch# show authentication sessions
```

次に、ギガビット インターフェイス 3/27 に対する Web ベースの認証設定を表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet 3/27
```




CHAPTER 14

インターフェイス特性の設定

この章では、IE 3000 スイッチ上に定義するインターフェイス タイプと、それを設定する方法について説明します。

この章の内容は、次のとおりです。

- 「インターフェイス タイプの概要」 (P.14-1)
- 「インターフェイス コンフィギュレーション モードの使用方法」 (P.14-8)
- 「イーサネット インターフェイスの設定」 (P.14-13)
- 「レイヤ 3 インターフェイスの設定」 (P.14-22)
- 「システム最大伝送単位 (MTU) の設定」 (P.14-24)
- 「インターフェイスのモニタリングおよびメンテナンス」 (P.14-26)



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスおよび『Cisco IOS Interface Command Reference』Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

インターフェイス タイプの概要

ここでは、スイッチによってサポートされる各種インターフェイス タイプについて説明するとともに、これらのインターフェイス タイプの設定に関する詳細情報が記載された章についても言及します。

- 「ポートベースの VLAN」 (P.14-2)
- 「スイッチ ポート」 (P.14-2)
- 「ルーテッド ポート」 (P.14-4)
- 「スイッチ仮想インターフェイス」 (P.14-5)
- 「EtherChannel ポート グループ」 (P.14-6)
- 「デュアルパーパス アップリンク ポート」 (P.14-7)
- 「インターフェイスの接続」 (P.14-7)

- 「[インターフェイスの接続](#)」(P.14-7)

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的に分割された、スイッチによるネットワークです。VLAN の詳細については、[第 16 章「VLAN の設定」](#)を参照してください。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が認識されるのは、ローカルポートが VLAN に対応するように設定されたとき、VLAN トランッキング プロトコル (VTP) トランク上のネイバーからその存在を学習したとき、またはユーザが VLAN を作成したときです。

VLAN を設定するには、`vlan vlan-id` グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の VLAN 設定は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 の場合に、拡張範囲 VLAN (VLAN ID が 1006 ~ 4094) を設定するには、最初に VTP モードをトランスペアレントに設定する必要があります。トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースには追加されませんが、スイッチの実行コンフィギュレーションに保存されます。VTP バージョン 3 では、クライアントまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN データベースに格納されます。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて、所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。
- トンネル ポートの場合は、カスタマー固有の VLAN タグ用に VLAN ID の設定と定義を行います。[第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」](#)を参照してください。

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。スイッチ ポートは、アクセス ポート、トランク ポート、またはトンネル ポートのいずれかに設定できます。ポートは、アクセス ポートまたはトランク ポートに設定できます。また、ポート単位で **Dynamic Trunking Protocol (DTP)** を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチ ポートモードも設定できます。IEEE 802.1Q トランク ポートに接続した非対称リンクの一部として、トンネル ポートを手動で設定する必要があります。スイッチ ポートは、物理インターフェイスおよび対応するレイヤ 2 プロトコルの管理に使用されます。

スイッチ ポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにするには、**switchport** コマンドと **no** キーワードを使用します。



(注) レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

アクセス ポートおよびトランク ポート特性の設定に関する詳細については、第 16 章「VLAN の設定」を参照してください。トンネル ポートの詳細については、17 章の「Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling」を参照してください。

アクセス ポート

アクセス ポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。

アクセス ポートが 802.1Q タグ付きパケットを受信した場合、そのパケットはドロップされ、送信元アドレスは学習されません。

2 種類のアクセス ポートがサポートされています。

- スタティック アクセス ポート。このポートは、手動で VLAN に割り当てます（IEEE 802.1x で使用する場合は RADIUS サーバを使用します）。詳細については、「VLAN 割り当てを使用した 802.1x 認証」(P.12-16) を参照してください。
- ダイナミック アクセス ポートの VLAN メンバーシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの伝送はポートの VLAN メンバーシップが検出されたときにだけイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN Membership Policy Server (VMPS; VLAN メンバーシップ ポリシー サーバ) によって VLAN に割り当てられます。VMPS を Catalyst 6500 シリーズスイッチにすることはできますが、IE 3000 スイッチは VMPS サーバとして使用できません。

また、Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータトラフィック用に使用するように設定できます。音声 VLAN ポートの詳細については、第 18 章「音声 VLAN の設定」を参照してください。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバとなります。

スイッチは IEEE 802.1Q トランク ポートだけをサポートします。IEEE 802.1Q トランク ポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートは、デフォルトの Port VLAN ID (PVID; ポート VLAN ID) に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。NULL VLAN ID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。残りのトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは、VTP に認識されているすべての VLAN のメンバですが、トランク ポートごとに VLAN の許可リストを設定して、VLAN メンバーシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN (VLAN ID 1 ~ 4094) が許可リストに含まれます。トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブル状態にある場合に限り、VLAN のメンバーになることができます。VTP が新しいイネーブル VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになり、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランク ポートの許可リストに登録されていない、新しいイネーブル VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トランク ポートの詳細については、第 16 章「VLAN の設定」を参照してください。

トンネル ポート

トンネル ポートは IEEE 802.1Q トンネリングで使用され、サービスプロバイダー ネットワークのカスタマーのトラフィックを、同じ VLAN 番号を使用するその他のカスタマーから分離します。サービスプロバイダー エッジスイッチのトンネル ポートからカスタマーのスイッチの IEEE 802.1Q トランクポートに、非対称リンクを設定します。エッジスイッチにトンネル ポートを入力するパケットは、すでにカスタマー VLAN によって IEEE 802.1Q タグが付けられており、サービスプロバイダー ネットワークで各カスタマーに固有の VLAN ID を含む、別のレイヤの IEEE 802.1Q タグ（メトロ タグと呼ばれる）によってカプセル化されます。タグが二重に付いたパケットは、その他のカスタマーのものとは異なる、元のカスタマーの VLAN が維持されてサービスプロバイダー ネットワークを通過します。発信インターフェイス、およびトンネル ポートでは、メトロ タグが削除されてカスタマーのネットワークのオリジナル VLAN 番号が取得されます。



(注)

トンネル ポートは、IP サービス イメージが稼働しているスイッチでだけサポートされます。

トンネル ポートは、トランク ポートまたはアクセス ポートにすることができず、それぞれのカスタマーに固有の VLAN に属する必要があります。

トンネル ポートの詳細については、第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

ルーテッド ポート

ルーテッド ポートは物理ポートであり、ルータ上にあるポートのように動作しますが、ルータに接続されている必要はありません。ルーテッド ポートは、アクセス ポートとは異なり、特定の VLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスのように動作します。ルーテッド ポートは、レイヤ 3 ルーティング プロトコルで設定できます。ルーテッド ポートはレイヤ 3 インターフェイス専用で、DTP や Spanning-Tree Protocol (STP; スパニングツリー プロトコル) などのレイヤ 2 プロトコルはサポートしません。ルーテッド ポートは、IP ベース イメージまたは IP サービス イメージを稼働しているスイッチだけでサポートされています。

ルーテッド ポートを設定するには、**no switchport** インターフェイス コンフィギュレーション コマンドでインターフェイスをレイヤ 3 モードにします。次に、ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、**ip routing** および **router protocol** グローバル コンフィギュレーション コマンドを使用してルーティング プロトコルの特性を指定します。



(注)

no switchport インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスがいったんシャットダウンしてから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 2 モードのインターフェイスをレイヤ 3 モードにした場合、影響のあるインターフェイスに関連する以前の設定が消失する可能性があります。

ソフトウェアに、設定できるルーテッド ポートの個数制限はありません。ただし、ハードウェアには限界があるため、この個数と設定されている他の機能の数との相互関係によって CPU パフォーマンスに影響が及ぶことがあります。ハードウェアのリソース制限に達したときに何が発生するかについては、「レイヤ 3 インターフェイスの設定」(P.14-22) を参照してください。

IP ユニキャストおよびマルチキャストのルーティングおよびルーティング プロトコルの詳細については、第 41 章「IP ユニキャスト ルーティングの設定」および第 50 章「IP マルチキャスト ルーティングの設定」を参照してください。



- (注) IP ベース イメージは、スタティック ルーティングおよび Routing Information Protocol (RIP) をサポートします。完全なレイヤ 3 ルーティングまたはフォールバック ブリッジングを実行するには、IP サービス イメージをインストールする必要があります。

スイッチ仮想インターフェイス

Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) は、スイッチ ポートの VLAN を、システムのルーティング機能またはブリッジング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に対応付けできるのは 1 つの SVI ですが、VLAN 間でルーティングする場合、VLAN 間でルーティングできないプロトコルをフォールバック ブリッジングする場合、またはスイッチと IP ホストの接続を行う場合だけ、VLAN に SVI を設定する必要があります。



- (注) SVI は、IP サービス イメージが稼働しているスイッチでだけサポートされます。

デフォルトでは、SVI はデフォルト VLAN (VLAN 1) 用に作成され、リモート スイッチの管理を可能にします。追加の SVI は明示的に設定する必要があります。



- (注) インターフェイス VLAN 1 は削除できません。

SVI はシステムにしか IP ホスト接続を行いません。レイヤ 3 モードでは、SVI 全体にルーティングを設定できます。

スイッチは合計 1005 の VLAN (および SVI) をサポートしますが、ハードウェアには限界があるため、SVI とルーテッド ポートの数および設定されている他の機能の数との相互関係によって、CPU パフォーマンスに影響が及ぶことがあります。ハードウェアのリソース制限に達したときに何が発生するかについては、「[レイヤ 3 インターフェイスの設定](#)」(P.14-22) を参照してください。

SVI は、VLAN インターフェイスに対して `vlan` インターフェイス コンフィギュレーション コマンドを実行したときに初めて作成されます。VLAN は、ISL または IEEE802.1Q カプセル化トランク上のデータ フレームに関連付けられた VLAN タグ、あるいはアクセス ポート用に設定された VLAN ID に対応します。トラフィックをルーティングするそれぞれの VLAN に対して VLAN インターフェイスを設定し、IP アドレスを割り当ててください。詳細については、「[手動でのスイッチ情報の割り当て](#)」(P.4-16) を参照してください。



- (注) 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

SVI は、ルーティング プロトコルとブリッジング設定をサポートします。IP ルーティング設定の詳細については、[第 41 章「IP ユニキャスト ルーティングの設定](#)」、[第 50 章「IP マルチキャスト ルーティングの設定](#)」および[第 52 章「フォールバック ブリッジングの設定](#)」を参照してください。



- (注) IP ベース イメージはスタティック ルーティングおよび RIP をサポートします。より高度なルーティングやフォールバック ブリッジングを行う場合は、IP サービス イメージを搭載する必要があります。

SVI 自動ステート除外

VLAN 上の複数のポートを装備した SVI のライン ステートは、次の条件を満たしたときにはアップ状態になります。

- VLAN が存在し、スイッチの VLAN データベースでアクティブです。
- VLAN インターフェイスが存在し、管理上のダウン状態ではありません。
- 少なくとも 1 つのレイヤ 2 (アクセスまたはトランク) ポートが存在し、この VLAN のリンクがアップ状態であり、ポートが VLAN でスパニングツリー フォワーディング ステートです。



(注)

対応する VLAN リンクに属する最初のスイッチポートが起動し、STP フォワーディング ステートになると、VLAN インターフェイスのプロトコル リンク ステートがアップ状態になります。

VLAN に複数のポートがある場合のデフォルトのアクションでは、VLAN 内のすべてのポートがダウンすると SVI もダウン状態になります。SVI 自動ステート除外機能を使用して、SVI ラインステート アップアンドダウン計算に含まれないようにポートを設定できます。たとえば、VLAN のアクティブポートだけがポートをモニタリングしている場合、ポートに **Autostate Exclude** を設定し、他のすべてのポートがダウンしたときに VLAN をダウンできるように設定できます。ポートがイネーブルである場合、**自動ステート除外**は、ポート上でイネーブルであるすべての VLAN に適用されます。

VLAN 内の 1 つのレイヤ 2 ポートに収束時間がある場合 (STP リスニング/ラーニング ステートから フォワーディング ステートへの移行)、VLAN インターフェイスが起動します。これにより、ルーティング プロトコルなどの機能は、完全に動作した場合と同様に VLAN インターフェイスを使用せず、ルーティング ブラック ホールなどの他の問題を最小限にします。自動ステート除外の設定については、「**SVI 自動ステート除外の設定**」(P.14-24) を参照してください。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱います。このようなポート グループは、スイッチ間、またはスイッチおよびサーバ間で高帯域接続を行う単一論理ポートとして動作します。EtherChannel は、チャンネルのリンク全体でトラフィックの負荷を分散させます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが残りのリンクに切り替えられます。複数のトランク ポートを 1 つの論理トランク ポートに、複数のアクセス ポートを 1 つの論理アクセス ポートに、複数のトンネル ポートを 1 つの論理トンネル ポートに、または複数のルーテッド ポートを 1 つの論理ルーテッド ポートにグループ化できます。

ほとんどのプロトコルは単一のまたは集約スイッチ ポートで動作し、ポート グループ内の物理ポートを認識しません。例外は、DTP、Cisco Discovery Protocol (CDP)、およびポート集約プロトコル (PAgP) で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャンネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ダイナミックにポート チャンネル論理インターフェイスを作成します。このコマンドは物理および論理ポートをバインドします。

レイヤ 3 インターフェイスの場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して手動で論理インターフェイスを作成します。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

詳細については、第 40 章「**EtherChannel およびリンクステート トラッキングの設定**」を参照してください。

デュアルパーパス アップリンク ポート

一部の 2960 スイッチでは、デュアルパーパス アップリンク ポートがサポートされています。各アップリンク ポートはデュアル フロント エンド (RJ-45 コネクタおよび Small Form-factor Pluggable モジュール コネクタ) を持つ 1 つのインターフェイスと見なされます。デュアル フロント エンドは冗長インターフェイスではありません。スイッチはペアのうちの 1 つのコネクタのみをアクティブにします。

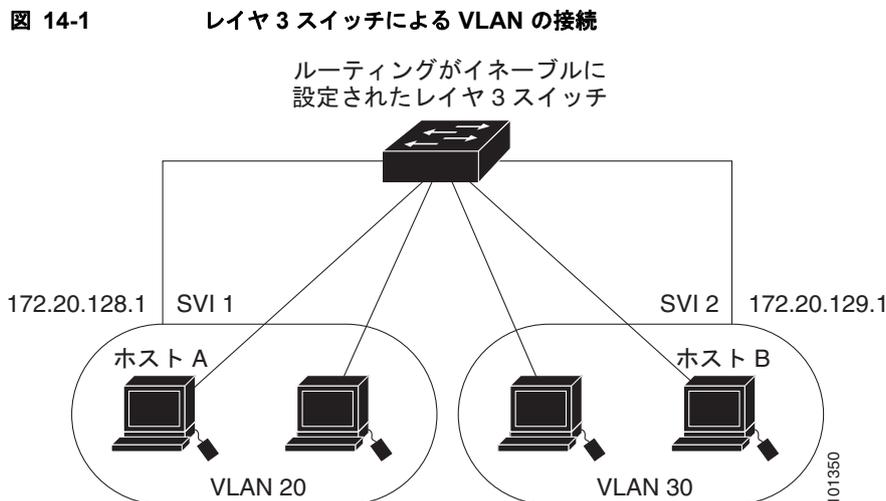
デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。デュアルパーパス アップリンクのデュプレックス設定および速度設定については、「[インターフェイス速度およびデュプレックスパラメータの設定](#)」(P.14-18) を参照してください。

各アップリンク ポートには、2 つの LED が付いています。1 つは RJ-45 ポートのステータスを示すもので、もう 1 つは SFP モジュール ポートのステータスを示すものです。ポート LED は、いずれかのコネクタがアクティブのときに点灯します。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。

標準のレイヤ 2 スイッチを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。ルーティングがイネーブルに設定されたスイッチを使用することにより、IP アドレスを割り当てた SVI で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、スイッチを介してパケットをホスト A からホスト B に直接送信できます (図 14-1 を参照)。



IP サービス イメージを使用する場合、スイッチはインターフェイス間でトラフィックを転送する方式として、ルーティングおよびフォールバックブリッジングの 2 通りをサポートします。IP ベース イメージを使用する場合は、基本ルーティング (スタティック ルーティングと RIP) だけがサポートされます。高いパフォーマンスを維持するため、可能な場合は常にスイッチ ハードウェアによって転送

を行います。ただし、ハードウェア内をルーティングできるのは、イーサネット II カプセル化機能を備えた IP バージョン 4 パケットだけです。非 IP トラフィックと、他のカプセル化方式を使用しているトラフィックは、ハードウェアによってフォールバック ブリッジングできます。

- ルーティング機能は、すべての SVI およびルーテッド ポートでイネーブルにできます。スイッチは、IP トラフィックだけをルーティングします。IP ルーティング プロトコル パラメータとアドレス設定が SVI またはルーテッド ポートに追加されると、このポートで受信した IP トラフィックはルーティングされます。第 41 章「IP ユニキャスト ルーティングの設定」、第 50 章「IP マルチキャスト ルーティングの設定」、および第 51 章「MSDP の設定」を参照してください。
- フォールバック ブリッジングを行うと、スイッチでルーティングされないトラフィックや、DECnet などのルーティングできないプロトコルに属するトラフィックが転送されます。また、フォールバック ブリッジングは、2 つ以上の SVI またはルーテッド ポート間のブリッジングによって、複数の VLAN を 1 つのブリッジ ドメインに接続します。フォールバック ブリッジングを設定する場合は、ブリッジ グループに SVI またはルーテッド ポートを割り当てます。各 SVI またはルーテッド ポートにはそれぞれ 1 つしかブリッジ グループが割り当てられません。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。詳細については、第 52 章「フォールバック ブリッジングの設定」を参照してください。

インターフェイス コンフィギュレーション モードの使用法

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポートおよびルーテッド ポート
- VLAN：スイッチ仮想インターフェイス
- ポート チャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます（「インターフェイス範囲の設定」(P.14-10) を参照）。

物理インターフェイス（ポート）を設定するには、インターフェイス タイプ、モジュール番号、およびスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

- タイプ：スイッチでのサポートに応じたポート タイプ。予想されるタイプには、10/100 Mb/s イーサネットにはファストイーサネット (fastethernet または fa)、10/100/1000 Mb/s イーサネットポートにはギガビットイーサネット (gigabitethernet または gi)、10,000 Mb/s には 10 ギガビットイーサネット (tengigabitethernet または te)、Small Form-factor Pluggable (SFP) モジュールにはギガビットイーサネット インターフェイスです。
- モジュール番号：スイッチ上のモジュール番号。モジュール番号 (1 ~ 3) は、モジュールがスイッチまたは他のモジュールと接続する方法によって異なります。
 - IE-3000-4TC および IE-3000-8TC スイッチに対応するモジュール番号は 1 です。
 - スイッチに直接接続するモジュールに対応するモジュール番号は 2 です。
 - 別のモジュールに接続するモジュールに対応するモジュール番号は 3 です。

- ポート番号：スイッチ上の物理インターフェイスの番号。ファストイーサネットポートでの IE-3000-4TC スイッチ モジュールのポート数は 1～4 であり、ギガビットイーサネットポートの場合は 1～2 です。ファストイーサネットポートでの IE-3000-8TC スイッチ モジュールのポート数は 1～8 であり、ギガビットイーサネットポートの場合は 1～2 です。表 14-1 に、スイッチとモジュールの組み合わせおよびインターフェイス番号を示します。

表 14-1 スイッチ インターフェイス番号

スイッチ モデル	モジュール番号	インターフェイスの番号付け方式
IE-3000-4TC スイッチ	1	ファストイーサネット 1/1、ファストイーサネット 1/2、ファストイーサネット 1/3、ファストイーサネット 1/4、ギガビットイーサネット 1/1、およびギガビットイーサネット 1/2
IE-3000-8TC スイッチ	1	ファストイーサネット 1/1、ファストイーサネット 1/2、ファストイーサネット 1/3、ファストイーサネット 1/4、ファストイーサネット 1/5、ファストイーサネット 1/6、ファストイーサネット 1/7、ファストイーサネット 1/8、ギガビットイーサネット 1/1、およびギガビットイーサネット 1/2
IEM-3000-8TM 拡張モジュール (スイッチに接続済み)	2	ファストイーサネット 2/1、ファストイーサネット 2/2、ファストイーサネット 2/3、ファストイーサネット 2/4、ファストイーサネット 2/5、ファストイーサネット 2/6、ファストイーサネット 2/7、およびファストイーサネット 2/8
IEM-3000-8TM 拡張モジュール (別のモジュールに接続済み)	3	ファストイーサネット 3/1、ファストイーサネット 3/2、ファストイーサネット 3/3、ファストイーサネット 3/4、ファストイーサネット 3/5、ファストイーサネット 3/6、ファストイーサネット 3/7、およびファストイーサネット 3/8

スイッチを確認することで物理インターフェイスを識別できます。**show** 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。以降、この章では、主に物理インターフェイスの設定手順について説明します。

インターフェイスの設定手順

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

- ステップ 1** 特権 EXEC プロンプトに **configure terminal** コマンドを入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- ステップ 2** **interface** グローバル コンフィギュレーション コマンドを入力します。

ギガビットイーサネットポート 1 でのインターフェイスタイプおよびインターフェイス番号の識別方法の例は、次のとおりです。

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



(注) インターフェイス タイプとインターフェイス番号の間に入れるスペースはオプションです。

ステップ 3 各 **interface** コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。入力するコマンドによって、そのインターフェイスで稼働するプロトコルとアプリケーションが定義されます。別のインターフェイス コマンドまたは **end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。

また、**interface range** または **interface range macro** グローバル コンフィギュレーション コマンドを使用すると、一定範囲のインターフェイスを設定することもできます。ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。

ステップ 4 インターフェイスを設定してから、「[インターフェイスのモニタリングおよびメンテナンス](#)」(P.14-26) に示した **show** 特権 EXEC コマンドで、そのステータスを確認してください。

show interfaces 特権 EXEC コマンドを使用して、スイッチ上のまたはスイッチ用に設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイス範囲の設定

interface range グローバル コンフィギュレーション コマンドを使用して、同じコンフィギュレーション パラメータを持つ複数のインターフェイスを設定できます。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンドパラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

同じパラメータでインターフェイス範囲を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	<p>設定するインターフェイス範囲 (VLAN または物理ポート) を指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> • interface range コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • macro 変数については、「インターフェイス レンジ マクロの設定および使用方法」(P.14-12) を参照してください。 • カンマで区切った <i>port-range</i> では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。 • ハイフンで区切った <i>port-range</i> では、インターフェイス タイプの再入力が必要ですが、ハイフンの前後にスペースを入力する必要があります。
ステップ 3		この時点で、通常のコフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。

	コマンド	目的
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show interfaces [<i>interface-id</i>]	指定した範囲内のインターフェイスの設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

interface range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- スイッチでのポート タイプに応じた *port-range* の有効なエントリは次のとおりです。
 - **vlan** *vlan-ID* - *vlan-ID*、VLAN ID は 1 ～ 4094
 - モジュールは常に 0 です。
 - **fastethernet** *module*/{*first port*} - {*last port*}、モジュールは常に 0。
 - **gigabitethernet** *module*/{*first port*} - {*last port*}、モジュールは常に 0。
 - **port-channel** *port-channel-number* - *port-channel-number*、*port-channel-number* は 1 ～ 6。



(注) ポート チャンネルを指定して **interface range** コマンドを使用する場合は、先頭および最後のチャンネル番号をアクティブなポート チャンネルにする必要があります。

- **interfacerange** コマンドを使用するときは、先頭のインターフェイス番号とハイフンの間にスペースが必要です。

たとえば、**interface range gigabitethernet1/1 - 2** は有効な範囲指定ですが、**interface range gigabitethernet 1/1-2** は無効です。

- **interface range** コマンドが機能するのは、**interface vlan** コマンドで設定された VLAN インターフェイスに限られます。**show running-config** 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。**show running-config** コマンドで表示されない VLAN インターフェイスに **interface range** コマンドを使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ（すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN）でなければなりません。ただし、1 つのコマンド内で複数のレンジを組み合わせることができます。

次の例では、**interface range** グローバル コンフィギュレーション コマンドを使用して、ポート 1 ～ 2 の速度を 100 Mb/s に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 - 2
Switch(config-if-range)# speed 100
```

この例では、カンマを使用して別のインターフェイス タイプ スtring を追加し、ファスト イーサネット ポート 1 ～ 3 と、ギガビット イーサネット ポート 1 および 2 の両方をイネーブルにし、フロー制御ポーズ フレームを受信できるようにします。

```
Switch# configure terminal
SSwitch(config)# interface range fastethernet1/1 - 3, gigabitethernet1/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイス レンジ モードを終了した後で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジ コンフィギュレー

ション モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンドプロンプトが再表示されるのを待ってから、インターフェイス範囲コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用方法

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

インターフェイス レンジ マクロを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	define interface-range macro_name interface-range	インターフェイス レンジ マクロを定義して NVRAM（不揮発性 RAM）に保存します。 <ul style="list-style-type: none"> • <i>macro_name</i> は、最大 32 文字の文字列です。 • マクロには、カンマで区切ったインターフェイスを 5 つまで指定できます。 • それぞれの <i>interface-range</i> は、同じポート タイプで構成されていなければなりません。
ステップ 3	interface range macro macro_name	<i>macro_name</i> の名前でインターフェイス レンジ マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。 ここで、通常のコフィギュレーション コマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config include define	定義済みのインターフェイス レンジ マクロの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マクロを削除するには、**no define interface-range macro_name** グローバル コンフィギュレーション コマンドを使用します。

define interface-range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- スイッチでのポート タイプに応じた *interface-range* の有効なエントリは次のとおりです。
 - **vlan** *vlan-ID* - *vlan-ID*、VLAN ID は 1 ~ 4094
 - **fastethernet** module/{*first port*} - {*last port*}、モジュールは常に 0。
 - **gigabitethernet** module/{*first port*} - {*last port*}、モジュールは常に 0。
 - **port-channel** *port-channel-number* - *port-channel-number*、*port-channel-number* は 1 ~ 6。



(注) ポート チャネルを指定して **interface range** コマンドを使用する場合は、先頭および最後のチャンネル番号をアクティブなポート チャネルにする必要があります。

- `interface-range` を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。
たとえば、`gigabitethernet1/1 - 2` は有効な範囲指定ですが、`gigabitethernet 1/1-2` は無効です。
- VLAN インターフェイスは、`interface vlan` コマンドで設定しておく必要があります。`show running-config` 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。`show running-config` コマンドで表示されない VLAN インターフェイスを `interface-range` として使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ（すべてがファストイーサネットポート、すべてがギガビットイーサネットポート、すべてが EtherChannel ポート、またはすべてが VLAN）でなければなりません。ただし、1 つのマクロ内で複数のインターフェイスタイプを組み合わせることができます。

次に、`enet_list` という名前のインターフェイス範囲マクロを定義して、ポート 1 および 2 を含め、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet1/1 - 2
```

次に、複数のタイプのインターフェイスを含むマクロ `macro1` を作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 2
Switch(config)# end
```

次に、インターフェイスレンジマクロ `enet_list` に対するインターフェイスレンジコンフィギュレーションモードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイスレンジマクロ `enet_list` を削除し、処理を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

イーサネット インターフェイスの設定

ここでは、次の設定について説明します。

- 「イーサネット インターフェイスのデフォルト設定」(P.14-14)
- 「デュアルパーパスアップリンクポートのタイプの設定」(P.14-15)
- 「インターフェイス速度およびデュプレックスモードの設定」(P.14-17)
- 「IEEE 802.3x フロー制御の設定」(P.14-19)
- 「インターフェイスでの Auto-MDIX の設定」(P.14-20)
- 「インターフェイスに関する記述の追加」(P.14-21)

イーサネット インターフェイスのデフォルト設定

表 14-2 は、イーサネット インターフェイスのデフォルト設定を示しています。表に示されている VLAN パラメータの詳細については、第 16 章「VLAN の設定」を参照してください。また、ポートへのトラフィック制御の詳細については、第 29 章「ポート単位のトラフィック制御の設定」を参照してください。



(注)

インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

表 14-2 レイヤ 2 イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード (switchport コマンド)
VLAN 許容範囲	VLAN 1 ~ 4094
デフォルト VLAN (アクセスポート用)	VLAN 1 (レイヤ 2 インターフェイスだけ)
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1 (レイヤ 2 インターフェイスだけ)
VLAN トランキング	Switchport mode dynamic auto (DTP をサポート) (レイヤ 2 インターフェイスだけ)
ポート イネーブル ステート	すべてのポートがイネーブル
ポートの説明	未定義
速度	自動ネゴシエーション
デュプレックス モード	自動ネゴシエーション
フロー制御	フロー制御は receive: off に設定されます。送信パケットでは常にオフです。
EtherChannel (PAgP)	すべてのイーサネット ポートでディセーブル。第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ポート ブロッキング (不明マルチキャストおよび不明ユニキャストトラフィック)	ディセーブル (ブロッキングされない) (レイヤ 2 インターフェイス限定)。「ポート ブロッキングの設定」(P.29-7) を参照してください。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル 「ストーム制御のデフォルト設定」(P.29-3) を参照してください。
保護ポート	ディセーブル (レイヤ 2 インターフェイス限定)。「保護ポートの設定」(P.29-6) を参照してください。
ポート セキュリティ	ディセーブル (レイヤ 2 インターフェイス限定)。「ポート セキュリティのデフォルト設定」(P.29-12) を参照してください。

表 14-2 レイヤ 2 イーサネット インターフェイスのデフォルト設定 (続き)

機能	デフォルト設定
PortFast	ディセーブル 「オプションのスパンニングツリー機能のデフォルト設定」(P.23-10) を参照してください。
Auto-MDIX	イネーブル。 (注) 受電デバイスがクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover (Auto-MIDX) がイネーブルかどうかは関係ありません。
キープアライブ メッセージ	SFP モジュールでディセーブル。他のすべてのポートでイネーブル。

デュアルパーパス アップリンク ポートのタイプの設定

一部の 2960 スイッチでは、デュアルパーパス アップリンク ポートがサポートされています。デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。詳細については、「デュアルパーパス アップリンク ポート」(P.14-7) を参照してください。

速度およびデュプレックスの設定が行えるようにアクティブにするデュアルパーパス アップリンクを選択するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するデュアルパーパス アップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

コマンド	目的
ステップ3 media-type {auto-select rj45 sfp}	<p>インターフェイスとデュアルパーパス アップリンク ポートのタイプを選択します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • auto-select : スイッチが動的にタイプを選択します。リンクがアップの状態になると、アクティブなリンクがダウンの状態になるまで、スイッチによりその他のタイプがディセーブル化されます。アクティブなリンクがダウンの状態になると、いずれかのリンクがアップの状態になるまで、スイッチにより両方のタイプがイネーブル化されます。auto-select モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます (デフォルト)。インストールされている SFP モジュールのタイプによって、スイッチで自動的に選択が行えない場合もあります。詳細については、この手順の後の説明を参照してください。 • rj45 : スイッチが SFP モジュール インターフェイスをディセーブル化します。このポートに SFP モジュールを接続する場合、RJ-45 側がダウンしている、または接続していない場合でも、リンクを確立することはできません。このモードでは、デュアルパーパス ポートは 10/100/1000BASE-TX インターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。 • sfp : スイッチが RJ-45 インターフェイスをディセーブル化します。この RJ-45 ポートにケーブルを接続している場合、SFP モジュール側がダウンしている、または SFP モジュールが接続していない場合でも、リンクを確立することはできません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能です。 <p>速度およびデュプレックスの詳細については、「速度とデュプレックス モードの設定時の注意事項」(P.14-17) を参照してください。</p>
ステップ4 end	特権 EXEC モードに戻ります。
ステップ5 show interfaces interface-id transceiver properties	設定値を確認します。
ステップ6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**media-type auto interface** または **no media-type** インターフェイス コンフィギュレーション コマンドを使用します。

スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます (デフォルト)。**auto-select** を設定した場合、**speed** および **duplex** インターフェイス コンフィギュレーション コマンドによる設定は行えません。

スイッチの電源を ON にした場合、または **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドでデュアルパーパス アップリンク ポートをイネーブル化した場合、**SFP** モジュール インターフェイスが選択されます。これ以外の場合、最初にアップの状態になったリンクのタイプに基づいて、アクティブなリンクが選択されます。

このスイッチと **100BASE-x** (-x は **-BX**、**-FX**、**-FE**、**-LX** のいずれか) **SFP** モジュールを組み合わせると、次のように動作します。

- 100BASE-x SFP モジュールがモジュール スロットに搭載されていて、RJ-45 側にリンクがない場合、スイッチにより RJ-45 インターフェイスがディセーブル化され、SFP モジュール インターフェイスが選択されます。ケーブルが接続されていない場合や、SFP モジュール側にリンクがない場合でも、このようになります。
- 100BASE-x SFP モジュールが搭載されていて、RJ-45 側にリンクがある場合、このリンクを使用して動作が続行します。リンクがダウンの状態になると、スイッチにより RJ-45 側がディセーブル化され、SFP モジュール インターフェイスが選択されます。
- 100BASE-x SFP モジュールを取り外すと、スイッチにより再び自動的にタイプが選択され (**auto-select**)、再び RJ-45 側がイネーブル化されます。

100BASE-FX-GE SFP モジュールの場合、この機能はありません。

インターフェイス速度およびデュプレックス モードの設定

サポートされるポート タイプに応じて、スイッチのイーサネット インターフェイスは、全二重または半二重モードのいずれかで、10、100、1000、または 10,000 Mb/s で動作します。全二重モードの場合、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。これは、各ステーションがトラフィックを受信するか、送信するかのどちらか一方しかできないことを意味します。

スイッチ モデルには、ファストイーサネット (10/100 Mb/s) ポート、ギガビットイーサネット (10/100/1000 Mb/s) ポート、10 ギガビット モジュール ポート、および SFP モジュールをサポートする SFP モジュール スロットの組み合わせが含まれます。

ここでは、インターフェイス速度とデュプレックス モードの設定手順について説明します。

- 「速度とデュプレックス モードの設定時の注意事項」 (P.14-17)
- 「インターフェイス速度およびデュプレックス パラメータの設定」 (P.14-18)

速度とデュプレックス モードの設定時の注意事項

インターフェイス速度およびデュプレックス モードを設定するときには、次の注意事項に留意してください。

- ファストイーサネット (10/100 Mbps) ポートは、すべての速度およびデュプレックス オプションをサポートします。
- ギガビットイーサネット (10/100/1000 Mbps) ポートは、すべての速度オプションとデュプレックス オプション (自動、半二重、全二重) をサポートします。ただし、1000 Mbps で稼働させているギガビットイーサネット ポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI (コマンドライン インターフェイス) オプションが変わります。
 - 1000 BASE-x (x には、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドで **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
 - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックス オプションをサポートします。
 - 100BASE-x (x には、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポートは、100 Mbps のみサポートします。これらのモジュールは、全二重および半二重オプションをサポートしますが、自動ネゴシエーションをサポートしません。

スイッチでサポートされる SFP モジュールについては、各製品のリリース ノートを参照してください。

- 回線の両側で自動ネゴシエーションがサポートされる場合は、できるだけデフォルトの **auto** ネゴシエーションを使用してください。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、スイッチがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。



注意

インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

インターフェイス速度およびデュプレックス パラメータの設定

物理インターフェイスの速度およびデュプレックス モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>speed {10 100 1000 auto [10 100 1000] nonegotiate}</code>	<p>インターフェイスに対する適切な速度パラメータを入力します。</p> <ul style="list-style-type: none"> • インターフェイスの速度を指定するには、10、100、または 1000 を入力します。1000 キーワードを使用できるのは、10/100/1000 Mbps ポートに対してだけです。 • インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、auto を入力します。auto キーワードと一緒に 10、100、または 1000 キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。 • nonegotiate キーワードを使用できるのは、SFP モジュールポートに対してだけです。SFP モジュールポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。 <p>速度の設定の詳細については、「速度とデュプレックス モードの設定時の注意事項」(P.14-17) を参照してください。</p>
ステップ 4	<code>duplex {auto full half}</code>	<p>インターフェイスのデュプレックス パラメータを入力します。</p> <p>半二重モードをイネーブルにします (10 または 100Mbps のみで動作するインターフェイスの場合)。1000 Mbps で動作するインターフェイスには半二重モードを設定できません。</p> <p>デュプレックスの設定の詳細については、「速度とデュプレックス モードの設定時の注意事項」(P.14-17) を参照してください。</p>
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ6	<code>show interfaces interface-id</code>	インターフェイス速度およびデュプレックス モード設定を表示します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの速度およびデュプレックス設定（自動ネゴシエーション）に戻すには、**no speed** および **no duplex** インターフェイス コンフィギュレーション コマンドを使用します。すべてのインターフェイス設定をデフォルトに戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、10/100Mbps ポートでインターフェイスの速度を 10 Mbps に、デュプレックス モードを半二重に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fasttethernet1/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitetheretnet1/2
Switch(config-if)# speed 100
```

IEEE 802.3x フロー制御の設定

フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズ フレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。



(注) スイッチのポートは、ポーズ フレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスのポーズ フレームを受信 (**receive**) する能力を **on**、**off**、または **desired** に設定します。デフォルトの状態は **off** です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイス、または必要ではないがフロー制御パケットを送信できる接続デバイスに対して動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on** (または **desired**) : ポートはポーズ フレームを送信できませんが、ポーズ フレームを送信する必要のある、または送信できる接続デバイスと組み合わせて使用できます。ポーズ フレームの受信は可能です。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じて、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。



(注) コマンドの設定と、その結果生じるローカルおよびリモート ポートでのフロー制御解決の詳細については、このリリースのコマンド リファレンスに記載された **flowcontrol** インターフェイス コンフィギュレーション コマンドを参照してください。

インターフェイス上でフロー制御を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>flowcontrol {receive} {on off desired}</code>	ポートのフロー制御モードを設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id</code>	インターフェイス フロー制御の設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フロー制御をディセーブルにするには、`flowcontrol receive off` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のフロー制御をオンにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

インターフェイスでの Auto-MDIX の設定

インターフェイス上の Auto-MDIX がイネーブルに設定されている場合、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータなどのデバイスの接続にはストレート ケーブルを使用し、他のスイッチやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、ハードウェア インストールガイドを参照してください。

Auto-MDIX はデフォルトでイネーブルです。Auto-MDIX をイネーブルに設定する場合、Auto-MDIX 機能が正しく動作するようにインターフェイスの速度およびデュプレックスを `auto` に設定する必要があります。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mb/s インターフェイスでサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

表 14-3 に、Auto-MDIX の設定およびケーブル接続ごとのリンク ステータスを示します。

表 14-3 リンク状態と Auto-MDIX の設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい場合	ケーブル接続が正しくない場合
On	On	リンク アップ	リンク アップ
On	Off	リンク アップ	リンク アップ
Off	On	リンク アップ	リンク アップ
Off	Off	リンク アップ	リンク ダウン

インターフェイス上で Auto-MDIX を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	speed auto	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 4	duplex auto	接続されたデバイスとデュプレックス モードの自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 5	mdix auto	インターフェイス上で Auto-MDIX をイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show controllers ethernet-controller interface-id phy	インターフェイスで Auto-MDIX の動作ステータスを確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Auto-MDIX をディセーブルにするには、**no mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

インターフェイスに関する記述の追加

インターフェイスの機能に関する記述を追加できます。記述は、特権 EXEC コマンド **show configuration**、**show running-config**、および **show interfaces** の出力に表示されます。

インターフェイスに関する記述を追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	記述を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに関する説明を追加します (最大 240 文字)。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id description または show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

記述を削除するには、**no description** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに記述を追加して、その説明を確認する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/2 description
Interface Status          Protocol Description
Gi1/2    admin down          down    Connects to Marketing
```

レイヤ 3 インターフェイスの設定

スイッチは、次のレイヤ 3 インターフェイスをサポートします。

- **SVI** : トラフィックをルーティングする VLAN に対応する SVI を設定する必要があります。SVI は、**interface vlan** グローバル コンフィギュレーション コマンドのあとに VLAN ID を入力して作成します。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス VLAN 1 は削除できません。



(注) 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。VLAN へのレイヤ 2 ポートの割り当てについては、[第 16 章「VLAN の設定」](#)を参照してください。

SVI を設定するとき、SVI ラインステート ステータスを判断する際に含めないようにするため、SVI 自動ステート除外を SVI のポートに設定することもできます。「[SVI 自動ステート除外の設定](#)」(P.14-24)を参照してください。

- **ルーテッド ポート** : ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。
- **レイヤ 3 EtherChannel ポート** : EtherChannel インターフェイスは、ルーテッド ポートで構成されます。

EtherChannel ポート インターフェイスについては、[第 40 章「EtherChannel およびリンクステート トラッキングの設定」](#)を参照してください。

スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。

スイッチに設定可能な SVI とルーテッド ポートの数について定義済みの制限はありません。ただし、ハードウェアには限界があるため、SVI およびルーテッド ポートの個数と、設定されている他の機能の個数の組み合わせによっては、CPU 利用率が影響を受けることがあります。スイッチが最大限のハードウェア リソースを使用している場合にルーテッド ポートまたは SVI を作成しようとする、次のような結果になります。

- 新たなルーテッド ポートを作成しようすると、スイッチはインターフェイスをルーテッド ポートに変換するための十分なリソースがないことを示すメッセージを表示し、インターフェイスはスイッチポートのままとなります。
- 拡張範囲の VLAN を作成しようすると、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。
- VTP が新たな VLAN をスイッチへ通知すると、スイッチは使用可能な十分なハードウェア リソースがないことを示すメッセージを送り、その VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

- スイッチが、ハードウェアのサポート可能な数を超える VLAN とルーテッド ポートが設定されたコンフィギュレーションを使って起動を試みると、VLAN は作成されますが、ルーテッド ポートはシャットダウンされ、スイッチはハードウェア リソースが不十分であるという理由を示すメッセージを送信します。

すべてのレイヤ 3 インターフェイスには、トラフィックをルーティングするための IP アドレスが必要です。次の手順は、レイヤ 3 インターフェイスとしてインターフェイスを設定する方法およびインターフェイスに IP アドレスを割り当てる方法を示します。



(注) 物理ポートがレイヤ 2 モードである (デフォルト) 場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを実行してインターフェイスをレイヤ 3 モードにする必要があります。**no switchport** コマンドを実行すると、インターフェイスがディセーブルになってから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが生成されることがあります。さらに、レイヤ 2 モードのインターフェイスをレイヤ 3 モードにすると、影響を受けたインターフェイスに関連する前の設定情報は失われ、インターフェイスはデフォルト設定に戻る可能性があります。

レイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>{{fastethernet gigabitethernet} interface-id}</i> <i>{vlan vlan-id}</i> <i>{port-channel port-channel-number}</i>	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 4	ip address <i>ip_address subnet_mask</i>	IP アドレスおよび IP サブネットを設定します。
ステップ 5	no shutdown	インターフェイスをイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [<i>interface-id</i>] show ip interface [<i>interface-id</i>] show running-config interface [<i>interface-id</i>]	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスの IP アドレスを削除するには、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをルーテッド ポートとして設定し、IP アドレスを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

SVI 自動ステート除外の設定

SVI のアクセスまたはトランク ポートに SVI 自動ステート除外を設定すると、同じ VLAN に属していた場合でも、SVI ステータスの計算（アップまたはダウン ライン ステート）からポートを除外できます。除外されたポートがアップ状態でも、VLAN 内の他のポートがすべてダウン状態であれば、SVI ステートはダウンに変更されます。

SVI ライン ステート アップを保持するには、VLAN で少なくとも 1 つのポートがアップで除外されていない必要があります。このコマンドを使用して、SVI のステータスを決定する際にモニタリング ポートのステータスを除外できます。

SVI ステート変更計算からポートを除外するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport autostate exclude</code>	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running config interface interface-id</code> <code>show interface interface-id switchport</code>	(任意) 実行コンフィギュレーションを示します。 設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、SVI のアクセスまたはトランク ポートを設定して、ステータス計算から除外する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

システム最大伝送単位 (MTU) の設定

すべてのインターフェイスで送受信されるフレームのデフォルト Maximum Transmission Unit (MTU; 最大伝送単位) サイズは、1500 バイトです。10 または 100 Mbps で動作するすべてのインターフェイスで MTU サイズを増やすには、`system mtu` グローバル コンフィギュレーション コマンドを使用します。また、`system mtu jumbo` グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビットイーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。

`system mtu routing` グローバル コンフィギュレーション コマンドを使用すると、ルーテッド ポートの MTU サイズを変更できます。



(注)

システム MTU サイズを超えるルーティング MTU サイズは設定できません。システム MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更すると、設定変更は受け入れられませんが、次にスイッチをリセットするまで適用されません。設定変更が有効になると、ルーティング MTU サイズは自動的にデフォルトの新しいシステム MTU サイズになります。

system mtu コマンドはギガビット イーサネット ポートには影響せず、**system mtu jumbo** コマンドは 10/100 ポートには影響しません。**system mtu jumbo** コマンドを設定していない場合、**system mtu** コマンドの設定はすべてのギガビット イーサネット インターフェイスに適用されます。

個々のインターフェイスに MTU サイズを設定することはできません。すべての 10/100 インターフェイスまたはすべてのギガビット イーサネット インターフェイスに対して設定されます。システムまたはジャンボ MTU サイズを変更する場合、新規設定を有効にするにはスイッチをリセットする必要があります。**system mtu routing** コマンドは、スイッチをリセットしなくても有効になります。

スイッチの CPU が受信できるフレーム サイズは、**system mtu** または **system mtu jumbo** コマンドで入力した値に関係なく、1998 バイトに制限されています。通常、転送またはルーティングされたフレームは CPU によって受信されませんが、場合によっては、制御トラフィック、SNMP (簡易ネットワーク管理プロトコル)、Telnet、またはルーティング プロトコルへ送信されたトラフィックなどのパケットが CPU へ送信されることがあります。

ルーテッド パケットは、出力ポートで MTU チェックの対象となります。ルーテッド ポートで使用される MTU 値は (**system mtu jumbo** 値ではなく) 適用された **system mtu** 値から抽出されます。つまり、ルーテッド MTU はどの VLAN のシステム MTU よりも大きくなりません。ルーティング プロトコルは、隣接関係とリンクの MTU をネゴシエーションする場合にシステム MTU 値を使用します。たとえば、Open Shortest Path First (OSPF) プロトコルは、ピア ルータとの隣接関係を設定する前にこの MTU 値を使用します。特定の VLAN のルーテッド パケットの MTU 値を表示するには、**show platform port-asic mvid** 特権 EXEC コマンドを使用します。



(注)

レイヤ 2 ギガビット イーサネット インターフェイスが、10/100 インターフェイスより大きいサイズのフレームを受け取るように設定されている場合、レイヤ 2 ギガビット イーサネット インターフェイスに着信するジャンボ フレームとレイヤ 2 10/100 インターフェイスで発信されるジャンボ フレームはドロップされます。

すべての 10/100 またはギガビット イーサネット インターフェイスで MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	system mtu bytes	(任意) 10 または 100 Mb/s で動作するスイッチのすべてのインターフェイスに対して MTU サイズを変更します。 指定できる範囲は、1500 ~ 1998 バイトです。デフォルトは 1500 バイトです。
ステップ 3	system mtu jumbo bytes	(任意) スwitchのすべてのギガビット イーサネット インターフェイスに対して MTU サイズを変更します。 指定できる範囲は 1500 ~ 9000 バイトです。デフォルトは 1500 バイトです。

	コマンド	目的
ステップ 4	<code>system mtu routing bytes</code>	(任意) ルーテッド ポートのシステム MTU を変更します。指定できる範囲は 1500 ~ システム MTU 値で、すべてのポートにルーティング可能な最大 MTU 値です。これより大きなパケットは受け入れられますが、ルーティングされません。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	<code>reload</code>	オペレーティング システムをリロードします。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

スイッチのリロード後、`show system mtu` 特権 EXEC コマンドを入力することによって、設定値を確認できます。

次に、ギガビットイーサネット ポートの最大パケット サイズを 1800 バイトに設定する例を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

次に、ギガビットイーサネット インターフェイスを範囲外の値に設定しようとした場合に表示される応答の例を示します。

```
Switch(config)# system mtu jumbo 25000
                          ^
% Invalid input detected at '^' marker.
```

インターフェイスのモニタリングおよびメンテナンス

ここでは、インターフェイスのモニタおよびメンテナンスについて説明します。

- 「[インターフェイス ステータスのモニタ](#)」 (P.14-26)
- 「[インターフェイスおよびカウンタのクリアとリセット](#)」 (P.14-27)
- 「[インターフェイスのシャットダウンおよび再起動](#)」 (P.14-28)

インターフェイス ステータスのモニタ

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を表示できます。表 14-4 に、このようなインターフェイス モニタ コマンドの一部を示します (特権 EXEC プロンプトに `show ?` コマンドを入力すると、すべての `show` コマンドのリストが表示されます)。これらのコマンドの詳細な説明については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Interface Command Reference, Release 12.2』を参照してください。

表 14-4 インターフェイス用の show コマンド

コマンド	目的
<code>show interfaces [interface-id]</code>	(任意) すべてのインターフェイスまたは特定のインターフェイスのステータスおよび設定を表示します。
<code>show interfaces interface-id status [err-disabled]</code>	(任意) インターフェイスのステータス、または <code>errdisable</code> ステートにあるインターフェイスの一覧を表示します。
<code>show interfaces [interface-id] switchport</code>	(任意) スイッチング ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
<code>show interfaces [interface-id] description</code>	(任意) 1 つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
<code>show ip interface [interface-id]</code>	(任意) IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
<code>show interface [interface-id] stats</code>	(任意) インターフェイスのスイッチング パスによる入出力パケットを表示します。
<code>show interfaces transceiver properties</code>	(任意) インターフェイスの速度およびデュプレックス設定を表示します。
<code>show interfaces transceiver detail</code>	(任意) インターフェイスの温度、電圧、電流量を表示します。
<code>show interfaces [interface-id] [{transceiver properties detail}] module number</code>	SFP モジュールに関する物理および動作ステータスを表示します。
<code>show running-config interface [interface-id]</code>	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
<code>show version</code>	ハードウェア構成、ソフトウェアのバージョン、コンフィギュレーション ファイルの名前とソース、ブート イメージを表示します。
<code>show controllers ethernet-controller interface-id phy</code>	インターフェイスの Auto-MDIX 動作ステータスを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 14-5 に、カウンタのクリアとインターフェイスのリセットに使用できる特権 EXEC モードの `clear` コマンドを示します。

表 14-5 インターフェイス用の clear コマンド

コマンド	目的
<code>clear counters [interface-id]</code>	インターフェイスのカウンタをクリアします。
<code>clear interface interface-id</code>	インターフェイスのハードウェア ロジックをリセットします。
<code>clear line [number console 0 vty number]</code>	非同期シリアル回線に関するハードウェア ロジックをリセットします。

`show interfaces` 特権 EXEC コマンドによって表示されたインターフェイス カウンタをリセットするには、`clear counters` 特権 EXEC コマンドを使用します。オプションの引数が特定のインターフェイス番号から特定のインターフェイス タイプのみをクリアするように指定する場合を除いて、`clear counters` コマンドは、インターフェイスから現在のインターフェイス カウンタをすべてクリアします。



(注) **clear counters** 特権 EXEC コマンドは、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を使用して取得されたカウンタをクリアしません。**show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべての **show** コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

インターフェイスをシャットダウンするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface {vlan <i>vlan-id</i> } {{ fastethernet gigabitethernet } <i>interface-id</i> } { port-channel <i>port-channel-number</i> }	設定するインターフェイスを選択します。
ステップ 3	shutdown	インターフェイスをシャットダウンします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。

インターフェイスを再起動するには、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスがディセーブルになっていることを確認するには、**show interfaces** 特権 EXEC コマンドを使用します。ディセーブルになっているインターフェイスは、出力に *administratively down* と表示されます。



CHAPTER 15

SmartPort マクロの設定

IE 3000 スイッチのコマンドリファレンスに、コマンドの構文と使用方法の情報が 있습니다。

- [「SmartPort マクロの概要」 \(P.15-1\)](#)
- [「SmartPort マクロの設定」 \(P.15-1\)](#)
- [「SmartPort マクロの表示」 \(P.15-5\)](#)

SmartPort マクロの概要

SmartPort マクロは、共通の設定を保存および共有するのに便利です。SmartPort マクロを使用すると、ネットワークでのスイッチの場所に基づいて機能および設定をイネーブルにしたり、ネットワークを通じて大規模な設定を配置したりできます。

各 SmartPort マクロは、定義する一連の CLI コマンドです。SmartPort マクロは、既存の CLI コマンドの集まりであり、新しい CLI コマンドは含まれていません。

SmartPort マクロをインターフェイスに適用すると、マクロ内の CLI コマンドがインターフェイスに設定されます。インターフェイスに SmartPort マクロを適用しても、インターフェイスの既存の設定は失われません。新しいコマンドがインターフェイスに追加され、実行コンフィギュレーションファイルに保存されます。

SmartPort マクロの設定

- [「SmartPort のデフォルト設定」 \(P.15-1\)](#)
- [「SmartPort 設定時の注意事項」 \(P.15-2\)](#)
- [「SmartPort マクロの適用」 \(P.15-3\)](#)

SmartPort のデフォルト設定

スイッチで SmartPort マクロはイネーブルになっていません。

表 15-1 デフォルト SmartPort マクロ

マクロ名 ¹	説明
cisco-ie-global	このグローバル コンフィギュレーション マクロを使用して、スイッチの設定を工業用イーサネットの環境に合わせてスイッチの設定を行います。このマクロは、Express Setup を使用してスイッチを初期設定するときに自動的に適用されます。 (注) cisco-ethernetip マクロが適切に動作するために、まず cisco-ie-global マクロを適用する必要があります。
cisco-ie-desktop	PC のようなデスクトップ デバイスをスイッチ ポートに接続する場合、ネットワーク セキュリティと信頼性を高めるために、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-phone	Cisco IP Phone を装備した PC のようなデスクトップ デバイスをスイッチ ポートに接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、 cisco-ie-desktop マクロの拡張で、同じセキュリティと復元力機能を備えていますが、遅延に影響されやすい音声 トラフィックを正しく処理できるように専用の音声 VLAN が追加されています。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-switch	このインターフェイス コンフィギュレーション マクロは、アクセス スイッチとディストリビューション スイッチを接続している場合や、Small Form-Factor Pluggable (SFP) モジュールを使用して接続されているアクセス スイッチ間で接続している場合に使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-router	スイッチと WAN ルータを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ie-wireless	スイッチとワイヤレス アクセス ポイントを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、工業オートメーション トラフィック用に最適化されています。
cisco-ethernetip	このインターフェイス コンフィギュレーション マクロは、スイッチを EtherNet IP 装置に接続しているときに使用します。 (注) cisco-ethernetip マクロが適切に動作するために、まず cisco-ie-global マクロを適用する必要があります。

1. シスコ デフォルト SmartPort マクロは、スイッチで実行されているソフトウェア バージョンによって異なります。

SmartPort 設定時の注意事項

- マクロがスイッチまたはスイッチ インターフェイスにグローバルに適用されている場合、インターフェイス上の既存のすべての設定が保持されます。これは、差分設定に適用する場合に役立ちます。
- 構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドを適用します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、**macro global trace macro-name** グローバル コンフィギュレーション コマンド、または **macro trace macro-name** インターフェイス コンフィギュレーション コマンドを使用できます。
- 特定のインターフェイス タイプ固有の CLI コマンドもあります。設定を受け入れないインターフェイスにマクロを適用すると、マクロが構文または設定のチェックに失敗し、スイッチはエラー メッセージを返します。
- インターフェイス範囲へのマクロの適用は、単一インターフェイスへのマクロの適用と同じです。インターフェイスの範囲を使用する場合、マクロはその範囲内の各インターフェイスに順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。

- スイッチまたはスイッチ インターフェイスにマクロを適用すると、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。**show running-config** ユーザ EXEC コマンドを使用して、適用されたコマンドおよびマクロ名を表示できます。

SmartPort マクロの適用

SmartPort マクロを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	show parser macro	スイッチ ソフトウェアに埋め込まれているシスコ デフォルト SmartPort マクロを表示します。
ステップ2	show parser macro name <i>macro-name</i>	適用する特定のマクロを表示します。
ステップ3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ4	macro global { apply trace } <i>macro-name</i> [parameter { <i>value</i> }] [parameter { <i>value</i> }] [parameter { <i>value</i> }]	<p>マクロに定義されている個々のコマンドをスイッチに適用するには、macro global apply macro-name を入力します。macro global trace macro-name を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。</p> <p>parameter value キーワードを使用して、必要な値をマクロに追加します。\$ で始まるキーワードには、一意のパラメータ値が必要です。</p> <p>macro global apply macro-name ? コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。</p> <p>(任意) スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。</p>
ステップ5	interface <i>interface-id</i>	(任意) インターフェイス コンフィギュレーション モードを開始し、マクロを適用するインターフェイスを指定します。
ステップ6	default interface <i>interface-id</i>	(任意) 指定のインターフェイスからすべての設定情報を消去します。
ステップ7	macro { apply trace } <i>macro-name</i> [parameter { <i>value</i> }] [parameter { <i>value</i> }] [parameter { <i>value</i> }]	<p>macro global apply macro-name を入力して、マクロで定義された個々のコマンドをポートに適用します。macro global trace macro-name を指定して、構文または設定エラーを判別するためにマクロを適用およびデバッグします。</p> <p>parameter value キーワードを使用して、必要な値をマクロに追加します。\$ で始まるキーワードには、一意のパラメータ値が必要です。</p> <p>macro global apply macro-name ? コマンドを使用すると、マクロに必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。</p> <p>(任意) スイッチに固有の一意のパラメータ値を指定します。最高 3 つのキーワードと値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。</p>
ステップ8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	show running-config interface <i>interface-id</i>	マクロがインターフェイスに適用されたことを確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マクロに含まれる各コマンドの **no** バージョンを入力したときにだけ、スイッチで適用されたグローバル マクロ設定を削除できます。**default interface interface-id** インターフェイス コンフィギュレーション コマンドを入力すれば、ポートで適用されたマクロの設定を削除できます。

次に、**cisco-ie-desktop** マクロを表示する例、およびインターフェイス上でマクロを適用し、アクセス VLAN ID を 25 に設定する例を示します。

```
Switch# show parser macro name cisco-ie-desktop
-----
Macro name : cisco-ie-desktop
Macro type : default interface
# macro keywords ACCESS_VLAN
#macro name cisco-ie-desktop
switchport mode access
switchport access vlan ACCESS_VLAN
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
no macro description
macro description cisco-ie-desktop
-----

Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/4
Switch(config-if)# macro apply cisco-ie-desktop $AVID 25
```

次に、**cisco-ethernetip** マクロを表示する例と、このマクロをインターフェイスに適用する例を示します。

```
Switch# show parser macro name cisco-ethernetip
Macro name : cisco-ie-global
Macro type : default interface
#macro name cisco-ethernetip
#macro keywords ACCESS_VLAN
#macro description cisco-ethernetip
switchport host
switchport access vlan ACCESS-VLAN
storm-control broadcast level 3.00 1.00
service-policy input CIP-Traffic
#service-policy input 1588

Switch# configure terminal
Switch(config)# interface fastethernet 1/1
Switch(config-if)# macro apply cisco-ethernetip ACCESS_VLAN 1
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

SmartPort マクロの表示

SmartPort マクロを表示するには、表 15-2 の特権 EXEC コマンドを 1 つ以上使用します。

表 15-2 SmartPort マクロを表示するコマンド

コマンド	目的
<code>show parser macro</code>	すべての SmartPort マクロを表示します。
<code>show parser macro name <i>macro-name</i></code>	特定の SmartPort マクロを表示します。
<code>show parser macro brief</code>	SmartPort マクロの名前を表示します。
<code>show parser macro description [interface <i>interface-id</i>]</code>	すべてのインターフェイスまたは特定のインターフェイスに関する SmartPort マクロの説明を表示します。



CHAPTER 16

VLAN の設定

この章では、IE 3000 スイッチに標準範囲 VLAN (VLAN ID 1 ~ 1005) および拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定する手順について説明します。VLAN メンバーシップ モード、VLAN コンフィギュレーション モード、VLAN トランク、および VLAN Membership Policy Server (VMPS; VLAN メンバーシップ ポリシー サーバ) からの動的 VLAN 割り当てについても説明します。



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

この章の内容は、次のとおりです。

- 「VLAN の概要」 (P.16-1)
- 「標準範囲 VLAN の設定」 (P.16-5)
- 「拡張範囲 VLAN の設定」 (P.16-11)
- 「VLAN の表示」 (P.16-15)
- 「VLAN トランクの設定」 (P.16-15)
- 「VMPS の設定」 (P.16-26)

VLAN の概要

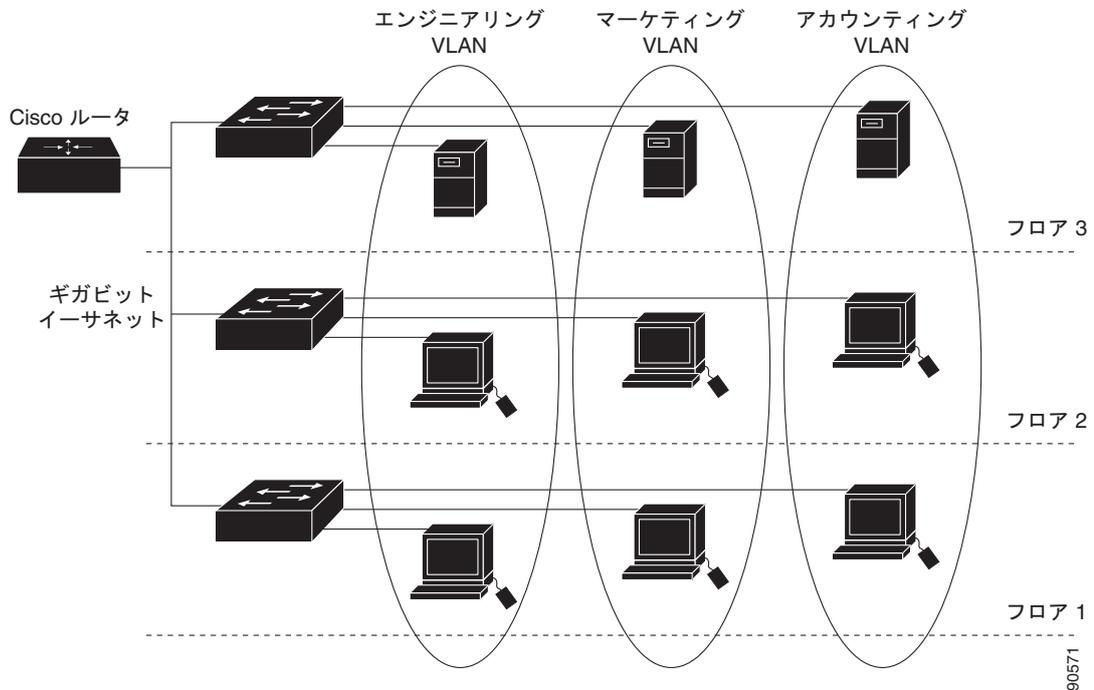
VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラグメントが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に割り当てられていないステーション宛てのパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して転送しなければなりません (図 16-1 を参照)。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ MIB (管理情報ベース) 情報があり、スパニングツリーの独自の実装をサポートできます。第 21 章「STP の設定」を参照してください。



(注) VLAN を作成する前に、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。VTP の詳細については、第 17 章「VTP の設定」を参照してください。

図 16-1 に、論理的に定義されたネットワークにセグメント化された VLAN の例を示します。

図 16-1 論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットワークに含まれるすべてのエンドステーションを同じ VLAN に属させる場合などです。スイッチ上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチインターフェイスを VLAN に割り当てた場合、これをインターフェイスベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバックブリッジする必要があります。スイッチは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。詳細については、「[スイッチ仮想インターフェイス](#)」(P.14-5) および「[レイヤ 3 インターフェイスの設定](#)」(P.14-22) を参照してください。



(注)

スイッチに多数の VLAN を設定し、ルーティングをイネーブル化しない予定の場合は、**sdm prefer vlan** グローバル コンフィギュレーション コマンドを使用して Switch Database Management (SDM; スイッチ データベース管理) 機能を VLAN テンプレートに設定できます。このテンプレートは、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースを設定します。SDM テンプレートの詳細については、[第 10 章「SDM テンプレートの設定」](#)、またはこのリリースのコマンドリファレンスの **sdm prefer** コマンドを参照してください。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ~ 4094 の番号で識別します。VLAN ID 1002 ~ 1005 は、トークンリングおよびファイバ分散データ インターフェイス (FDDI) VLAN 専用です。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN (VLAN ID 1 ~ 1005) だけをサポートします。これらのバージョンで 1006 ~ 4094 の VLAN ID を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。Cisco IOS Release 12.2(52)SE 以降では VTP バージョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体 (VLAN 1 ~ 4094) をサポートします。拡張範囲 VLAN (VLAN 1006 ~ 4094) は、VTP バージョン 3 でだけサポートされます。拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

スイッチは合計 1005 の VLAN をサポートしますが、ルーテッドポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。

スイッチは、最大 128 のスパニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus (PVST+) または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニングツリー インスタンスを使用できます。スパニングツリー インスタンス数および VLAN 数の詳細については、「標準範囲 VLAN 設定時の注意事項」(P.16-6) を参照してください。

VLAN ポート メンバーシップ モード

VLAN に所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。表 16-1 に、各種メンバーシップ モード、およびそれぞれのメンバーシップと VTP の特性を示します。

表 16-1 ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。 詳細については、「VLAN へのスタティック アクセス ポートの割り当て」(P.16-10) を参照してください。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、あるスイッチのトランク ポートに接続した別のスイッチ上に 1 つまたは複数のトランク ポートがなければなりません。
トランク (ISL または IEEE 802.1Q)	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッドイングトラフィックを阻止することもできます。 トランク ポートの設定については、「トランク ポートとしてのイーサネット インターフェイスの設定」(P.16-17) を参照してください。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。

メンバーシップモード	VLAN メンバーシップの特性	VTP の特性
ダイナミック アクセス	<p>ダイナミックアクセス ポートは 1 つの VLAN (VLAN ID が 1 ~ 4094) にのみ所属し、VMPS によって動的に割り当てられます。VMPS には、たとえば Catalyst 5000 または Catalyst 6500 シリーズのスイッチが使用できますが、IE 3000 スイッチは使用できません。IE 3000 スイッチは VMPS クライアントです。</p> <p>同一スイッチ上でダイナミックアクセス ポートとトランク ポートを使用できますが、ダイナミックアクセス ポートは別のスイッチではなく、エンドステーションまたはハブに接続する必要があります。</p> <p>設定の詳細については、「VMPS クライアント上のダイナミックアクセス ポートの設定」(P.16-29) を参照してください。</p>	<p>VTP は必須です。</p> <p>VMPS およびクライアントを同じ VTP ドメイン名で設定してください。</p> <p>VTP に加入するには、あるスイッチのトランク ポートが別のスイッチのトランク ポートに接続していなければなりません。</p>
音声 VLAN	<p>音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データトラフィックに別の VLAN を使用するように設定されたアクセス ポートです。</p> <p>音声 VLAN ポートの詳細については、第 18 章「音声 VLAN の設定」 を参照してください。</p>	VTP は不要です。VTP は音声 VLAN に対して無効です。
プライベート VLAN	<p>プライベート VLAN ポートは、プライベート VLAN のプライマリまたはセカンダリ VLAN に属するホストまたは無差別ポートです。</p> <p>プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」 を参照してください。</p>	VTP バージョン 1 および 2 では、プライベート VLAN を設定する場合は、スイッチを VTP トランスペアレント モードにする必要があります。プライベート VLAN がスイッチに設定されている場合、VTP モードをトランスペアレント モードからクライアント モードやサーバ モードに変更しないでください。VTP バージョン 3 では、すべてのモードのプライベート VLAN をサポートします。
トンネル (dot1q-tunnel)	<p>トンネル ポートは、IEEE 802.1Q トンネリング用に使用され、サービスプロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持します。トンネル ポートをサービスプロバイダー ネットワークのエッジスイッチ上に設定し、カスタマー インターフェイスの IEEE 802.1Q トランク ポートに接続して、非対称リンクを作成します。トンネル ポートは、トンネリング専用の単一の VLAN に属します。</p> <p>トンネル ポートの詳細については、第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」 を参照してください。</p>	VTP は必須ではありません。 switchport access vlan インターフェイス コンフィギュレーション コマンドを使用して、手動で VLAN にトンネル ポートを割り当てます。

アクセス モードとトランク モード、および機能の定義の詳細については、[表 16-4 \(P.16-16\)](#) を参照してください。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。詳細については、「[MAC アドレス テーブルの管理](#)」(P.7-12) を参照してください。

標準範囲 VLAN の設定

標準範囲 VLAN は、VLAN ID が 1 ～ 1005 の VLAN です。スイッチが VTP サーバモードまたは VTP トランスペアレントモードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。

VTP バージョン 1 および 2 では、拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を作成する場合は、スイッチを VTP トランスペアレントモードにする必要があります。ただし、これらの VLAN は VLAN データベースに格納されません。VTP バージョン 3 は、拡張範囲 VLAN を VTP サーバモードおよびトランスペアレントモードでサポートします。「[拡張範囲 VLAN の設定](#)」(P.16-11) を参照してください。

VLAN ID 1 ～ 1005 の設定はファイル *vlan.dat*（VLAN データベース）に書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。*vlan.dat* ファイルはフラッシュメモリに格納されます。



注意

vlan.dat ファイルを手動で削除しようとする、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応するコマンドリファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、[第 17 章「VTP の設定」](#)を参照してください。

さらに、インターフェイス コンフィギュレーションモードを使用して、ポートのメンバーシップモードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーションファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ（イーサネット、FDDI、FDDI Network Entity Title (NET)、TrBRF または TrCRF、トークンリング、トークンリング Net)
- VLAN ステート（アクティブまたは中断）
- VLAN の Maximum Transmission Unit (MTU; 最大伝送単位)
- Security Association Identifier (SAID)
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Protocol (STP; スパニングツリープロトコル) タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号



(注)

ここでは、これらのパラメータの大部分の設定手順について説明しません。VLAN 設定を制御するコマンドおよびパラメータの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

ここでは、標準範囲 VLAN の設定情報について説明します。

- 「トークンリング VLAN」 (P.16-6)
- 「標準範囲 VLAN 設定時の注意事項」 (P.16-6)
- 「標準範囲 VLAN の設定」 (P.16-7)
- 「イーサネット VLAN のデフォルト設定」 (P.16-7)
- 「イーサネット VLAN の作成または変更」 (P.16-8)
- 「VLAN の削除」 (P.16-9)
- 「VLAN へのスタティック アクセス ポートの割り当て」 (P.16-10)

トークンリング VLAN

このスイッチはトークンリング接続をサポートしていませんが、トークンリング接続を行っている Catalyst 5000 シリーズスイッチなどのリモート デバイスを、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼働しているスイッチは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

トークンリング VLAN の詳しい設定手順については、『*Catalyst 5000 Series Software Configuration Guide*』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで 1005 の VLAN をサポートしています。
- 標準範囲 VLAN は、1 ~ 1001 の番号で識別します。VLAN 番号 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ~ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もスイッチの実行コンフィギュレーション ファイルに保存されます。
- VTP バージョン 1 および 2 では、スイッチは VTP トランスペアレント モード (VTP はディセーブル) の場合だけ、VLAN ID 1006 ~ 4094 をサポートします。これらは拡張範囲 VLAN であり、設定オプションには制限があります。VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) データベース伝播をサポートします。拡張 VLAN を設定している場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。「[拡張範囲 VLAN の設定](#)」 (P.16-11) を参照してください。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにしておく必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を伝播します。

- スイッチは 128 のスパニングツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

スイッチ上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP (MSTP) を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 22 章「MSTP の設定」を参照してください。

標準範囲 VLAN の設定

VLAN を **vlan** グローバル コンフィギュレーション コマンドで設定するには、VLAN ID を入力します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。デフォルトの VLAN 設定を使用するか（表 16-2 を参照）、複数のコマンドを入力して VLAN を設定できます。このモードで使用できるコマンドの詳細については、このリリースのコマンド リファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。設定を終了したら、VLAN コンフィギュレーション モードを終了して、設定を有効にする必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN ID 1 ~ 1005 の設定は、常に VLAN データベースに保存されます（**vlan.dat** ファイル）。VTP モードがトランスペアレント モードの場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用して、スタートアップ コンフィギュレーション ファイルに設定を保存できます。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバの場合、最初の 1005 の VLAN だけのドメイン名および VLAN 設定には VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ~ 4094 もサポートします。

イーサネット VLAN のデフォルト設定

表 16-2 にイーサネット VLAN のデフォルト設定を示します。



(注) スイッチがサポートするのは、イーサネット インターフェイスだけです。FDDI およびトークンリング VLAN は、ローカルではサポートされないため、FDDI およびトークンリング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

表 16-2 イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	範囲
VLAN ID	1	1 ~ 4094 (注) 拡張範囲 VLAN (VLAN ID 1006 ~ 4094) は、VTP バージョン 3 の場合だけ VLAN データベースに保存されます。
VLAN 名	VLANxxxx。xxxx は VLAN ID 番号に等しい 4 桁の数字 (先行ゼロを含む) です。	範囲なし
IEEE 802.10 SAID	100001 (100000 と VLAN ID の和)	1 ~ 4294967294
MTU サイズ	1500	1500 ~ 18190
トランスレーショナルブリッジ 1	0	0 ~ 1005
トランスレーショナルブリッジ 2	0	0 ~ 1005
VLAN ステート	active	アクティブ、中断
リモート SPAN	ディセーブル	イネーブル、ディセーブル
プライベート VLAN	設定なし	2 ~ 1001、1006 ~ 4094

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN には、1 ~ 1001 の 4 桁の一意の ID が設定されています。VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。



(注) VTP バージョン 1 および 2 でスイッチが VTP トランスペアレント モードの場合は、1006 を超える VLAN ID を割り当てることができませんが、それらを VLAN データベースに追加できません。「[拡張範囲 VLAN の設定](#)」(P.16-11) を参照してください。

VLAN の追加時に指定されるデフォルト パラメータの一覧は、「[標準範囲 VLAN の設定](#)」(P.16-5) を参照してください。

イーサネット VLAN を作成または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vlan vlan-id</code>	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 (注) このコマンドで指定できる VLAN ID 範囲は 1 ~ 4094 です。1005 を超える VLAN ID (拡張範囲 VLAN) を追加する手順については、「 拡張範囲 VLAN の設定 」(P.16-11) を参照してください。
ステップ3	<code>name vlan-name</code>	(任意) VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた <code>vlan-id</code> が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ4	<code>mtu mtu-size</code>	(任意) MTU サイズ (または他の VLAN 特性) を変更します。
ステップ5	<code>remote-span</code>	(注) (任意) リモート Switched Port Analyzer (SPAN; スイッチドポート アナライザ) セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細は、 第 30 章「SPAN および RSPAN の設定」 を参照してください。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show vlan {name vlan-name id vlan-id}</code>	設定を確認します。
ステップ8	<code>copy running-config startup config</code>	(任意) スイッチが VTP トランスペアレント モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN 名をデフォルトの設定に戻すには、`no name`、`no mtu` または `no remote-span` コマンドを使用します。

次に、イーサネット VLAN 20 を作成し、`test20` という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのスイッチから VLAN を削除した場合、そのスイッチ上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ~ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。

**注意**

VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

スイッチ上で VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no vlan <i>vlan-id</i>	VLAN ID を入力して、VLAN を削除します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vlan brief	VLAN が削除されたことを確認します。
ステップ 5	copy running-config startup config	(任意) スイッチが VTP トランスペアレント モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって (VTP トランスペアレント モード)、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバスイッチのポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバスイッチにログインします。

**(注)**

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます（「イーサネット VLAN の作成または変更」(P.16-8) を参照）。

VLAN データベース内の VLAN にポートを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	VLAN に追加するインターフェイスを入力します。
ステップ 3	switchport mode access	ポート (レイヤ 2 アクセス ポート) の VLAN メンバーシップ モードを定義します。
ステップ 4	switchport access vlan <i>vlan-id</i>	VLAN にポートを割り当てます。指定できる VLAN ID の範囲は 1 ~ 4094 です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface <i>interface-id</i>	インターフェイスの VLAN メンバーシップ モードを確認します。
ステップ 7	show interfaces <i>interface-id</i> switchport	表示された <i>Administrative Mode</i> および <i>Access Mode VLAN</i> フィールドの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

拡張範囲 VLAN の設定

VTP バージョン 1 およびバージョン 2 でスイッチが VTP トランスペアレント モード (VTP がディセーブル) の場合、拡張範囲 VLAN (1006 ~ 4094) を作成できます。VTP バージョンは、拡張範囲 VLAN をサーバ モードおよびトランスペアレント モードでサポートします。サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている任意の **switchport** コマンドで使用できます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファイルにストアされます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。



(注)

スイッチは 4094 の VLAN ID をサポートしますが、実際にサポートされる VLAN の数については、「サポートされる VLAN」(P.16-2) を参照してください。

ここでは、拡張範囲 VLAN の設定情報について説明します。

- 「VLAN のデフォルト設定」(P.16-11)
- 「拡張範囲 VLAN 設定時の注意事項」(P.16-11)
- 「拡張範囲 VLAN の作成」(P.16-12)
- 「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.16-14)

VLAN のデフォルト設定

表 16-2 (P.16-8) にイーサネット VLAN のデフォルト設定を示します。拡張範囲 VLAN については MTU サイズ、プライベート VLAN、およびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト ステートのままでなければなりません。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。

- VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。VTP モードがサーバまたはクライアントの場合、エラーメッセージが生成され、拡張範囲 VLAN が拒否されます。VTP バージョン 3 は、拡張範囲 VLAN をサーバモードおよびトランスペアレントモードでサポートします。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。「[VTP モードの設定](#)」(P.17-10) を参照してください。VTP トランスペアレントモードでスイッチが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。
- 拡張範囲 VLAN では、STP はデフォルトでイネーブルになりますが、**no spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッチ上に最大数のスパンニングツリー インスタンスが存在している場合に、VLAN を新規作成すると、この VLAN 上でスパンニングツリーはディセーブルになります。スイッチ上の VLAN の数がスパンニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s MSTP を設定して、複数の VLAN を単一のスパンニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、[第 22 章「MSTP の設定」](#)を参照してください。
- スイッチ上の各ルーテッドポートは、内部 VLAN を使用するために作成します。この内部 VLAN は拡張範囲 VLAN 番号を使用し、その内部 VLAN ID は拡張範囲 VLAN には使用できません。内部 VLAN として割り当て済みの VLAN ID を指定して拡張範囲 VLAN を作成すると、エラーメッセージが生成され、コマンドは拒否されます。
 - 内部 VLAN ID は拡張範囲の下部の方なので、拡張範囲 VLAN を作成するには最大の番号 (4094) から始めて最小値 (1006) へと動いて、内部 VLAN ID を使用する可能性を減らすことを推奨します。
 - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、どの VLAN が内部 VLAN として割り当てられているかを確認します。
 - 必要に応じて、内部 VLAN に割り当てられたルーテッドポートをシャットダウンできます。これにより、内部 VLAN が解放され、拡張範囲 VLAN を作成してポートを再度イネーブルにし、別の VLAN を内部 VLAN として使用します。「[内部 VLAN ID を指定した拡張範囲 VLAN の作成](#)」(P.16-14) を参照してください。
- スイッチは合計 1005 (標準範囲および拡張範囲) の VLAN をサポートしますが、ルーテッドポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。拡張範囲 VLAN を作成するときに、使用できるハードウェアリソースが不足していると、エラーメッセージが生成され、拡張範囲 VLAN が拒否されます。

拡張範囲 VLAN の作成

グローバル コンフィギュレーション モードで拡張範囲 VLAN を作成するには、**vlan** グローバル コンフィギュレーション コマンドを入力し、1006 ~ 4094 の VLAN ID を指定します。拡張範囲 VLAN はイーサネット VLAN のデフォルトの特性を備えており (表 16-2 を参照)、MTU サイズ、プライベート VLAN、RSPAN 設定だけが変更できるパラメータです。すべてのパラメータのデフォルト値については、コマンドリファレンスに記載された **vlan** グローバル コンフィギュレーション コマンドの説明を参照してください。VTP バージョン 1 または 2 で、スイッチが VTP トランスペアレントモードでない場合に拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラーメッセージが生成され、拡張範囲 VLAN が作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチの実行コンフィギュレーションファイルに保存されます。拡張範囲 VLAN 設定をスイッチのスタートアップコンフィギュレーションファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 は、拡張範囲 VLAN を VLAN データベースに保存します。



(注) 拡張範囲 VLAN を作成する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、VLAN ID が内部的に使用されていないことを確認します。VLAN ID が内部的に使用されている場合に、それを解放するには、「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.16-14) を参照してから拡張範囲 VLAN を作成してください。

拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 vtp mode transparent	スイッチを VTP トランスペアレント モードに設定し、VTP をディセーブルにします。 (注) この手順は、VTP バージョン 3 では不要です。
ステップ3 vlan vlan-id	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ~ 4094 です。
ステップ4 mtu mtu-size	(任意) MTU サイズを変更して、VLAN を変更します。 (注) CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、 mtu mtu-size コマンド、 private-vlan コマンド、 remote-span コマンドだけです。
ステップ5 remote-span	(任意) RSPAN VLAN として VLAN を設定します。「RSPAN VLAN としての VLAN の設定」(P.30-17) を参照してください。
ステップ6 end	特権 EXEC モードに戻ります。
ステップ7 show vlan id vlan-id	VLAN が作成されたことを確認します。
ステップ8 copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、VTP トランスペアレント モード設定および拡張範囲 VLAN 設定をスイッチのスタートアップコンフィギュレーションファイルに保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。 (注) VTP バージョン 3 では、VLAN コンフィギュレーションは VLAN データベースにも保存されます。

拡張範囲 VLAN を削除するには、**no vlan vlan-id** グローバル コンフィギュレーション コマンドを使用します。

スタティック アクセス ポートを拡張範囲 VLAN に割り当てる手順は、標準範囲 VLAN の手順と同じです。「VLAN へのスタティック アクセス ポートの割り当て」(P.16-10) を参照してください。

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップコンフィギュレーションファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
```

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

内部 VLAN ID を指定した拡張範囲 VLAN の作成

内部 VLAN に割り当て済みの拡張範囲 VLAN ID を入力すると、エラーメッセージが生成され、拡張範囲 VLAN は拒否されます。内部 VLAN ID を手動で解放するには、内部 VLAN ID を使用しているルーテッドポートを一時的にシャットダウンする必要があります。

内部 VLAN に割り当てられた VLAN ID を解放してその ID で拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show vlan internal usage	スイッチが内部的に使用している VLAN ID を表示します。使用したい VLAN ID が内部 VLAN である場合は、その VLAN ID を使用しているルーテッドポートが表示されます。そのポート番号をステップ 3 で入力してください。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id	その VLAN ID を使用しているルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	shutdown	ポートをシャットダウンして内部 VLAN ID を解放します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	vtp mode transparent	VTP モードをトランスペアレントに設定して拡張範囲 VLAN を作成します。 (注) この手順は、VTP バージョン 3 では不要です。
ステップ 7	vlan vlan-id	新しい拡張範囲 VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。
ステップ 8	exit	VLAN コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。
ステップ 9	interface interface-id	ステップ 4 でシャットダウンしたルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	no shutdown	ルーテッドポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスペアレントモード設定と拡張範囲 VLAN 設定を保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバモードになり、拡張範囲 VLAN ID は保存されません。 (注) VTP バージョン 3 では、VLAN が VLAN データベースに保存されるため、この手順は必要ありません。

VLAN の表示

拡張範囲 VLAN を含む、スイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。VLAN ステータス、ポート、および設定情報も表示されます。

表 16-3 に、VLAN をモニタするための特権 EXEC コマンドを示します。

表 16-3 VLAN モニタ コマンド

コマンド	目的
show interfaces [vlan <i>vlan-id</i>]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [id <i>vlan-id</i>]	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。

show コマンド オプションおよび出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VLAN トランクの設定

ここでは、次の概要について説明します。

- 「[トランキングの概要](#)」 (P.16-15)
- 「[レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定](#)」 (P.16-17)
- 「[トランク ポートとしてのイーサネット インターフェイスの設定](#)」 (P.16-17)
- 「[トランク ポートの負荷分散の設定](#)」 (P.16-22)

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーク デバイス（ルータ、スイッチなど）の間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張できます。スイッチでは、IEEE 802.1Q カプセル化がサポートされています。

トランクを設定できるのは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。EtherChannel の詳細については、[第 40 章「EtherChannel およびリンクステート トランキングの設定](#)」を参照してください。

イーサネット トランク インターフェイスは、[表 16-4](#) に示すトランキング モードをサポートしています。インターフェイスをトランキングまたは非トランキングとして設定したり、ネイバー インターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、PPP（ポイントツーポイント プロトコル）である Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

この事態を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。



(注) DTP はプライベート VLAN ポートまたはトンネル ポートではサポートされていません。

表 16-4 レイヤ 2 インターフェイス モード

モード	機能
switchport mode access	インターフェイス (アクセス ポート) を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、ネイバー インターフェイスが <i>trunk</i> または <i>desirable</i> モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは dynamic auto です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、ネイバー インターフェイスが <i>trunk</i> 、 <i>desirable</i> 、または <i>auto</i> モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、ネイバー リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、ネイバー インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが access または trunk の場合だけ使用できます。トランク リンクを確立するには、手動でネイバー インターフェイスをトランク インターフェイスとして設定する必要があります。
switchport mode dot1q-tunnel	インターフェイスをトンネル (非トランキング) ポートとして設定し、IEEE 802.1Q トランク ポートと非対称リンクで接続されるようにします。IEEE 802.1Q トンネリングは、サービス プロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持するのに使用されます。トンネル ポートの詳細については、 第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」 を参照してください。



(注) このスイッチはレイヤ 3 トランクをサポートしていません。同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

IEEE 802.1Q の設定に関する考慮事項

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、トランクの VLAN のスパニングツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 16-5 に、レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 16-5 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	switchport mode dynamic auto
VLAN 許容範囲	VLAN 1 ~ 4094
プルーニングに適格な VLAN 範囲	VLAN 2 ~ 1001
デフォルト VLAN (アクセス ポート用)	VLAN 1
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

ここでは、次の設定について説明します。

- 「他の機能との相互作用」 (P.16-18)
- 「トランクでの許可 VLAN の定義」 (P.16-20)
- 「プルーニング適格リストの変更」 (P.16-21)
- 「タグなしトラフィック用ネイティブ VLAN の設定」 (P.16-22)



(注)

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルトモードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ 2 トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。

他の機能との相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートは、トンネル ポートにできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかについて、設定を変更すると、入力した設定値がスイッチによってグループ内のすべてのポートに伝播されます。
 - 許可 VLAN リスト。
 - 各 VLAN の STP ポート プライオリティ。
 - STP PortFast の設定値。
 - トランク ステータス。ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- PVST モードで設定するトランク ポートの数は 24 まで、MST モードで設定するトランク ポートの数は 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

トランク ポートの設定

ポートをトランク ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode {dynamic {auto desirable} trunk}</code>	<p>インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。</p> <ul style="list-style-type: none"> • dynamic auto: ネイバー インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これはデフォルトです。 • dynamic desirable: ネイバー インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • trunk: ネイバー インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 4	<code>switchport access vlan vlan-id</code>	(任意) インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 5	<code>switchport trunk native vlan vlan-id</code>	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show interfaces interface-id switchport</code>	インターフェイスのスイッチポート設定を表示します。 <i>Administrative Mode</i> および <i>Administrative Trunking Encapsulation</i> フィールドに表示されます。
ステップ 8	<code>show interfaces interface-id trunk</code>	インターフェイスのトランク設定を表示します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。トランキング インターフェイスのすべてのトランキング 特性をデフォルトにリセットするには、**no switchport trunk** インターフェイス コンフィギュレーション コマンドを使用します。トランキングをディセーブルにするには、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、ポートをスタティック アクセス ポートとして設定します。

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、ネイバー インターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

トランクでの許可 VLAN の定義

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID (1 ~ 4094) が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。トランクが伝送するトラフィックを制限するには、**switchport trunk allowed vlan remove vlan-list** インターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除します。



(注)

VLAN 1 は、すべての Cisco スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック (スパニングツリー アドバタイズなど) は VLAN 1 で送受信されなくなります。

スパニングツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol (CDP)、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバにはなりません。

トランクの許可リストを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	switchport trunk allowed vlan {add all except remove} vlan-list	(任意) トランク上で許可される VLAN のリストを設定します。 add 、 all 、 except 、および remove キーワードの使用方法については、このリリースに対応するコマンド リファレンスを参照してください。 vlan-list パラメータは、1 ~ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号 (小さい方が先、ハイフンで区切る) で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 5	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ6	<code>show interfaces interface-id switchport</code>	表示された <i>Trunking VLANs Enabled</i> フィールドの設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN の許可 VLAN リストをデフォルトに戻すには、**no switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに独自の適格リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。VTP プルーニングをイネーブルにする方法については、「[VTP プルーニングのイネーブル化](#)」(P.17-15) を参照してください。

トランク ポートのプルーニング適格リストから VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>switchport trunk pruning vlan {add except none remove} vlan-list [,vlan[,vlan[,...]]</code>	トランクからのプルーニングを許可する VLAN のリストを設定します (「VTP プルーニング」 (P.17-5) を参照)。 add 、 except 、 none 、および remove キーワードの使用方法については、このリリースに対応するコマンドリファレンスを参照してください。 連続していない VLAN ID は、カンマ (スペースなし) で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ~ 1001 です。拡張範囲 VLAN (VLAN ID 1006 ~ 4094) はプルーニングできません。 プルーニング不適格の VLAN は、フラグディング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ~ 1001 が含まれます。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show interfaces interface-id switchport</code>	表示された <i>Pruning VLANs Enabled</i> フィールドの設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN のプルーニング適格リストをデフォルトに戻すには、**no switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。ネイティブ VLAN は、デフォルトでは VLAN 1 です。



(注)

ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定についての詳細は、「IEEE 802.1Q の設定に関する考慮事項」(P.16-17) を参照してください。

IEEE 802.1Q トランクでネイティブ VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk native vlan vlan-id</code>	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	<i>Trunking Native Mode VLAN</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ネイティブ VLAN をデフォルト (VLAN 1) に戻すには、**no switchport trunk native vlan** インターフェイス コンフィギュレーション コマンドを使用します。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

トランク ポートの負荷分散の設定

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。STP パス コストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のスイッチにも、2 台の異なるスイッチにも接続できます。STP の詳細については、第 21 章「STP の設定」を参照してください。

STP ポート プライオリティによる負荷分散

同一スイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロック状態とするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロック状態のままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

図 16-2 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ~ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ~ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ~ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ~ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ~ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ~ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランクポート上でも、トラフィックの重複は発生しません。

図 16-2 STP ポート プライオリティによる負荷分散

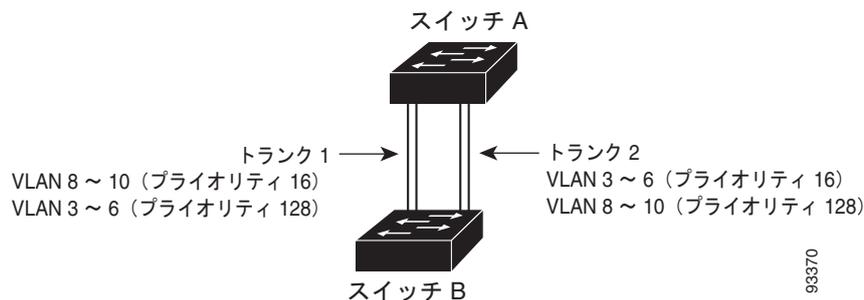


図 16-2 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp domain domain-name</code>	VTP 管理ドメインを設定します。 1 ~ 32 文字のドメイン名を使用できます。
ステップ 3	<code>vtp mode server</code>	スイッチ A を VTP サーバとして設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show vtp status</code>	スイッチ A および B の両方で、VTP 設定を確認します。 表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドをチェックします。
ステップ 6	<code>show vlan</code>	スイッチ A のデータベースに VLAN が存在していることを確認します。

VLAN トランクの設定

	コマンド	目的
ステップ 7	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 8	<code>interface interface-id_1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show interfaces interface-id_1 switchport</code>	VLAN 設定を確認します。
ステップ 12		スイッチの 2 番目のポートについて、スイッチ A 上でステップ 7 ~ 10 を繰り返します。
ステップ 13		スイッチ B でステップ 7 ~ 10 を繰り返し、スイッチ A で設定されたトランク ポートに接続するトランク ポートを設定します。
ステップ 14	<code>show vlan</code>	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 15	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 16	<code>interface interface-id_1</code>	STP のポートプライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	<code>spanning-tree vlan 8-10 port-priority 16</code>	VLAN 8 ~ 10 にポート プライオリティ 16 を割り当てます。
ステップ 18	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 19	<code>interface interface-id_2</code>	STP のポートプライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 20	<code>spanning-tree vlan 3-6 port-priority 16</code>	VLAN 3 ~ 6 にポート プライオリティ 16 を割り当てます。
ステップ 21	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 22	<code>show running-config</code>	設定を確認します。
ステップ 23	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

STP パス コストによる負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

図 16-3 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2 ~ 4 は、トランク ポート 1 で 30 というパス コストが割り当てられています。
- VLAN 8 ~ 10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8 ~ 10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2 ~ 4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コストである 19 のままです。

図 16-3 パス コストによってトラフィックが分散される負荷分散トランク

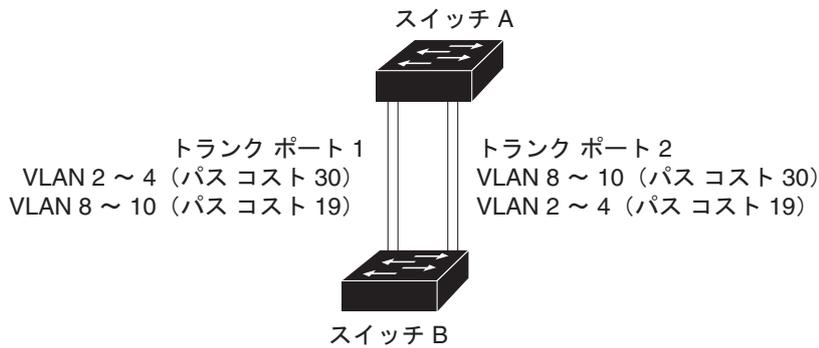


図 16-3 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id_1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。
ステップ 4	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 5		スイッチ A の 2 番目のインターフェイスでステップ 2 ~ 4 を繰り返します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 8	<code>show vlan</code>	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。スイッチ A が VLAN 設定を学習したことを確認します。
ステップ 9	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 10	<code>interface interface-id_1</code>	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	<code>spanning-tree vlan 2-4 cost 30</code>	VLAN 2 ~ 4 のスパニングツリー パス コストを 30 に設定します。
ステップ 12	<code>end</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 13		スイッチ A に設定したもう一方のトランク インターフェイスで、ステップ 9 ~ 12 を繰り返し、VLAN 8、9、および 10 のスパニングツリー パス コストを 30 に設定します。
ステップ 14	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 15	<code>show running-config</code>	設定を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 16	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VMPS の設定

VLAN Query Protocol (VQP) は、ダイナミックアクセス ポートをサポートする場合に使用します。ダイナミックアクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC (メディア アクセス コントロール) 送信元アドレスに基づいて VLAN を割り当てます。未知の MAC アドレスが検出されるたびに、スイッチはリモート VMPS に VQP クエリーを送信します。クエリーには新たに検出された MAC アドレスとそのアドレスを検出したポートが含まれます。VMPS はそのポートの VLAN 割り当てで応答します。このスイッチを VMPS サーバにすることはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信できます。

ここでは、次の情報について説明します。

- 「VMPS の概要」 (P.16-26)
- 「VMPS クライアントのデフォルト設定」 (P.16-27)
- 「VMPS 設定時の注意事項」 (P.16-27)
- 「VMPS クライアントの設定」 (P.16-28)
- 「VMPS のモニタリング」 (P.16-31)
- 「ダイナミックアクセス ポート VLAN メンバーシップのトラブルシューティング」 (P.16-31)
- 「VMPS の設定例」 (P.16-32)

VMPS の概要

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを送信します。このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピングを検索します。サーバの応答は、このマッピングと、サーバがオープン モードかセキュア モードかに基づいて行われます。セキュア モードの場合、サーバは不正なホストが検出されると、ポートをシャットダウンします。オープン モードでは、サーバはホストに対してポート アクセスを拒否するだけです。

ポートが未割り当ての場合 (つまり、VLAN 割り当てがまだ設定されていない場合)、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホストへのアクセスを許可する VLAN 割り当て応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS はアクセス拒否応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS はポートシャットダウン応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は成功応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、アクセス拒否またはポートシャットダウン応答を送信します。

VMPS からアクセス拒否応答を受信した場合、スイッチはそのホスト MAC アドレスのトラフィックを双方向で引き続きブロックします。スイッチはポート宛ての packets を引き続きモニタし、新しいホスト アドレスを検出すると VMPS にクエリーを送信します。VMPS からポートシャットダウン応答を受信した場合、スイッチはそのポートをディセーブルにします。Network Assistant、CLI、または SNMP を使用して、ポートを手動で再びネーブルにする必要があります。

ダイナミックアクセス ポート VLAN メンバーシップ

ダイナミックアクセス ポートが所属できるのは、VLAN ID が 1 ~ 4094 の 1 つの VLAN だけです。リンクがアップになっても、VMPS によって VLAN が割り当てられるまで、このポートとの間でトラフィック転送は行われません。VMPS は、ダイナミックアクセス ポートに接続した新しいホストの最初の packets から送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレスを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。クライアント スイッチがまだ設定されていない場合は、スイッチは VMPS からトランク ポートで受信した最初の VTP パケットからのドメイン名を使用します。クライアント スイッチがすでに設定されている場合は、クエリー パケットにスイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。VMPS はパケット内のドメイン名が自身のドメイン名と一致することを確認した後、要求を受け入れ、クライアントに割り当てられた VLAN 番号を応答します。一致しない場合、(VMPS セキュア モードの設定に応じて) VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミックアクセス ポート上で複数のホスト (MAC アドレス) をアクティブにできますが、それらのホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数が 20 を超えると、VMPS はダイナミックアクセス ポートをシャットダウンします。

ダイナミックアクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、VLAN の所属から外れます。ポート経由でオンラインになるホストは VMPS によって VQP 経由で再チェックされてから、ポートが VLAN に割り当てられます。

ダイナミックアクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。スイッチ上のポートごとに、最大 20 の MAC アドレスを使用できます。ダイナミックアクセス ポートが一度に所属できる VLAN は 1 つだけですが、VLAN は検出された MAC アドレスに基づいて後で変更されることがあります。

VMPS クライアントのデフォルト設定

表 16-6 に、クライアント スイッチ上の VMPS およびダイナミック アクセス ポートのデフォルト設定を示します。

表 16-6 VMPS クライアントおよびダイナミックアクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミックアクセス ポート VLAN メンバーシップには、次の注意事項および制限事項があります。

- VMPS を設定してから、ポートをダイナミックアクセス ポートとして設定する必要があります。
- ポートをダイナミックアクセス ポートとして設定すると、そのポートに対してスパニングツリーの PortFast 機能が自動的にイネーブルになります。PortFast モードにより、ポートをフォワーディング ステートに移行させるプロセスが短縮されます。

- IEEE 802.1x ポートをダイナミックアクセス ポートとして設定することはできません。ダイナミックアクセス (VQP) ポートで IEEE 802.1x をイネーブルにしようとすると、エラーメッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミックアクセス ポートにすることはできませんが、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力することは可能です。その場合、スイッチの設定は維持され、後にアクセス ポートとして設定された場合には、その設定が適用されます。

ダイナミックアクセス設定を有効にするには、ポート上でトランキングをオフにしておく必要があります。

- ダイナミックアクセス ポートをモニタ ポートにすることはできません。
- セキュア ポートをダイナミックアクセス ポートにすることはできません。ポートをダイナミックにするには、ポート上でポート セキュリティをディセーブルにしておく必要があります。
- プライベート VLAN ポートは、ダイナミックアクセス ポートにできません。
- ダイナミックアクセス ポートを EtherChannel グループのメンバにすることはできません。
- ポート チャネルをダイナミックアクセス ポートとして設定することはできません。
- ダイナミックアクセス ポートは、フォールバック ブリッジングに加入できます。
- VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。
- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。

VMPS クライアントの設定

ダイナミック VLAN を設定するには、VMPS (サーバ) を使用します。スイッチを VMPS クライアントにすることはできますが、VMPS サーバにすることはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。



(注)

スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

VMPS の IP アドレスを入力するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vmps server ipaddress primary	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	vmps server ipaddress	(任意) セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 4	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show vmps</code>	表示された <i>VMPS Domain Server</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) ダイナミックアクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。IP 接続が可能かどうかをテストするには、VMPS の IP アドレスに ping を実行し、応答が得られるかどうかを確認します。

VMPS クライアント上のダイナミックアクセス ポートの設定

クラスタ メンバスイッチのポートをダイナミックアクセス ポートとして設定するには、最初に `rcommand` 特権 EXEC コマンドを使用して、そのクラスタ メンバスイッチにログインします。



注意

ダイナミックアクセス ポート VLAN メンバーシップはエンドステーション用、またはエンドステーションに接続されたハブ用です。他のスイッチにダイナミックアクセス ポートを接続すると、接続が切断されることがあります。

VMPS クライアントスイッチにダイナミックアクセス ポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	エンドステーションに接続するスイッチポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode access</code>	ポートをアクセス モードにします。
ステップ 4	<code>switchport access vlan dynamic</code>	ポートをダイナミック VLAN メンバーシップ適格として設定します。 ダイナミックアクセス ポートは、エンドステーションに接続されている必要があります。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id switchport</code>	表示された <i>Operational Mode</i> フィールドの設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、`default interface interface-id` インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスをデフォルトのスイッチポート モード (dynamic auto) に戻すには、`no switchport mode` インターフェイス コンフィギュレーション コマンドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、`no switchport access vlan` インターフェイス コンフィギュレーション コマンドを使用します。

VLAN メンバーシップの再確認

スイッチが VMPS から受信したダイナミックアクセス ポート VLAN メンバーシップの割り当てを確認するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	vmmps reconfirm	ダイナミックアクセス ポート VLAN メンバーシップを再確認します。
ステップ 2	show vmmps	ダイナミック VLAN の再確認ステータスを確認します。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信する VLAN メンバーシップの情報を定期的に再確認します。再確認を実行する間隔は数字を使用して分単位で設定できます。

クラスタのメンバスイッチを設定する場合、このパラメータはコマンドスイッチの再確認インターバルの設定値以上でなければなりません。メンバスイッチにログインするには、最初に **rcommand** 特権 EXEC コマンドを使用する必要があります。

再確認インターバルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vmmps reconfirm minutes	ダイナミック VLAN メンバーシップの再確認を行う間隔 (分) を入力します。指定できる範囲は 1 ~ 120 です。デフォルトは 60 分です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vmmps	表示された <i>Reconfirm Interval</i> フィールドのダイナミック VLAN の再確認ステータスを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

再試行回数の変更

スイッチが次のサーバにクエリーを送信する前に、VMPS との接続を試行する回数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vmmps retry count	再試行の回数を変更します。指定できる再試行回数の範囲は 1 ~ 10 です。デフォルトは 3 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vmmps	表示された <i>Server Retry Count</i> フィールドの設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

VMPS のモニタリング

show vmmps 特権 EXEC コマンドを使用して、VMPS に関する情報を表示できます。スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP バージョン：VMPS との通信に使用する VQP のバージョン。スイッチは VQP バージョン 1 を使用する VMPS にクエリーを送信します。
- 再確認インターバル：スイッチが VLAN と MAC アドレスの割り当てを再確認する間隔（分）。
- サーバ再試行回数：VQP が VMPS にクエリーを再送信する回数。この回数すべてを試行しても応答が得られない場合、スイッチはセカンダリ VMPS へのクエリーを開始します。
- VMPS ドメイン サーバ：設定されている VLAN メンバーシップ ポリシー サーバの IP アドレス。スイッチは *current* と表示されているサーバにクエリーを送信します。*primary* と表示されているサーバは、プライマリ サーバです。
- VMPS 動作：最新の再確認の結果。再確認は、再確認インターバルが経過したときに自動的に行われますが、**vmmps reconfirm** 特権 EXEC コマンドを入力するか、Network Assistant または SNMP で同等の操作を行うことによって、強制的に再確認することもできます。

次に、**show vmmps** 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                   172.20.128.87

Reconfirmation status
-----
VMPS Action:          other
```

ダイナミックアクセス ポート VLAN メンバーシップのトラブルシューティング

VMPS は次の状況でダイナミックアクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、なおかつホストのポートへの接続を許可しない場合。VMPS はポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- ダイナミックアクセス ポート上のアクティブ ホストが 20 を超えた場合。

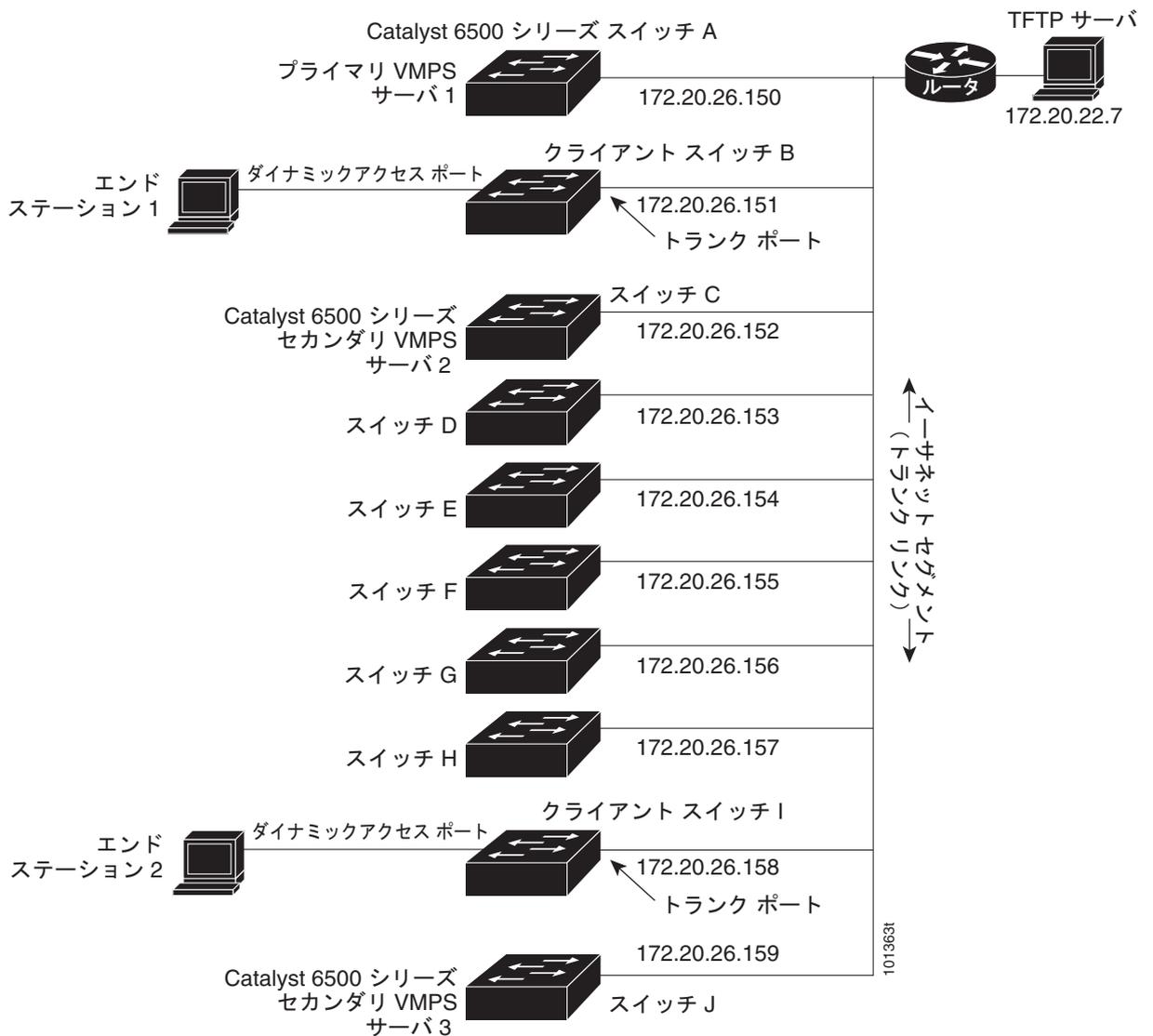
ディisableにされているダイナミックアクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の設定例

図 16-4 に、VMPS サーバスイッチと、ダイナミック アクセス ポートを備えた VMPS クライアント スイッチが含まれるネットワークの例を示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンドステーションはクライアント (スイッチ B、スイッチ I) に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。

図 16-4 ダイナミック ポート VLAN メンバーシップの構成例





CHAPTER 17

VTP の設定

この章では、VLAN トランッキング プロトコル (VTP) と VLAN データベースを使用して、IE 3000 スイッチで VLAN を管理する方法について説明します。

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

この章の内容は、次のとおりです。

- 「VTP の概要」 (P.17-1)
- 「VTP の設定」 (P.17-7)
- 「VTP のモニタ」 (P.17-18)

VTP の概要

VTP は、レイヤ 2 のメッセージプロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN 情報を他のスイッチに送信することはできません。

VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

スイッチは 1005 の VLAN をサポートしますが、設定済み機能の個数によって、スイッチ ハードウェアの使用が左右されます。VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限のハードウェア リソースをすでに使用している場合、スイッチはハードウェア リソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。show vlan ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN (VLAN ID 1 ~ 1005) だけをサポートします。Cisco IOS Release 12.2(52)SE 以降では VTP バージョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体 (VLAN 1 ~ 4094) をサポートします。拡張範囲 VLAN (VLAN 1006 ~ 4094) は、VTP バージョン 3 でだけサポートされます。拡張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

ここでは、次の概要について説明します。

- 「VTP ドメイン」 (P.17-2)
- 「VTP モード」 (P.17-3)
- 「VTP アドバタイズ」 (P.17-3)
- 「VTP バージョン 2」 (P.17-4)
- 「VTP バージョン 3」 (P.17-5)
- 「VTP プルーニング」 (P.17-5)

VTP ドメイン

VTP ドメイン (別名 VLAN 管理ドメイン) は、1つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチで構成されます。スイッチは、1つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランク リンク (複数 VLAN のトラフィックを伝送するリンク) を介してドメインについてのアドバタイズを受信しない限り、またはユーザがドメイン名を設定しない限り、スイッチは VTP 非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、スイッチは管理ドメイン名および VTP コンフィギュレーション リビジョン番号を継承します。その後スイッチは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。



注意

VTP クライアント スイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP コンフィギュレーション リビジョン番号の確認手順およびリセット手順については、「[VTP ドメインへの VTP クライアント スイッチの追加](#)」 (P.17-16) を参照してください。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP トランスペアレント モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

ドメイン名およびパスワードの設定時の注意事項については、「[VTP 設定時の注意事項](#)」 (P.17-8) を参照してください。

VTP モード

サポートされているスイッチは、表 17-1 に示すいずれかの VTP モードに設定できます。

表 17-1 VTP モード

VTP モード	説明
VTP サーバ	<p>VTP サーバモードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ (VTP バージョンなど) を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。</p> <p>VTP サーバがデフォルトのモードです。</p> <p>(注) VTP サーバモードでは、VLAN 設定は NVRAM に保存されます。スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバモードからクライアントモードに自動的に移行します。この場合、スイッチは NVRAM が動作するまで VTP サーバモードに戻ることができません。</p>
VTP クライアント	<p>VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバモードのスイッチで設定します。</p> <p>VTP バージョン 1 および 2 の VTP クライアントモードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 では、VLAN 設定はクライアントモードで NVRAM に保存されます。</p>
VTP トランスペアレント	<p>VTP トランスペアレントスイッチは、VTP に参加しません。VTP トランスペアレントスイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレントスイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP トランスペアレントモードでは、スイッチ上の VLAN を作成、変更、削除できます。</p> <p>VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成するときはスイッチを VTP トランスペアレントモードにする必要があります。VTP バージョン 3 でも、クライアントモードまたはサーバモードでの拡張範囲 VLAN の作成をサポートしています。「拡張範囲 VLAN の設定」(P.16-11) を参照してください。</p> <p>スイッチが VTP トランスペアレントモードの場合、VTP および VLAN の設定は NVRAM に保存されますが、他のスイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップコンフィギュレーションファイルに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。</p>
VTP オフ	<p>VTP オフモードでのスイッチの機能は、トランクを介して VTP アドバタイズを転送しないことを除くと VTP トランスペアレントスイッチとしての機能と同じです。</p>

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャストアドレスに対して、それぞれのトランクポートからグローバルコンフィギュレーションアドバタイズを定期的送信します。このようなアドバタイズを受信したネイバースイッチは、必要に応じて各自の VTP および VLAN 設定をアップデートします。



(注)

トランク ポートは VTP アドバタイズメントを送受信するので、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。トランク ポートの詳細については「[VLAN トランクの設定](#)」(P.16-15) を参照してください。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP 設定のリビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の Maximum Transmission Unit (MTU; 最大伝送単位) サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム形式

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID (ISL および IEEE 802.1Q)
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

VTP バージョン 2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン 1 でサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリング サポート : VTP バージョン 2 は、Token Ring Bridge Relay Function (TrBRF; トークンリングブリッジリレー機能) および Token Ring Concentrator Relay Function (TrCRF; トークンリングコンセンレータリレー機能) VLAN をサポートします。トークンリング VLAN の詳細については、「[標準範囲 VLAN の設定](#)」(P.16-5) を参照してください。
- 認識不能な Type-Length-Value (TLV) のサポート : VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバモードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレントモード : VTP バージョン 1 の場合、VTP トランスペアレントスイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけですが、VTP バージョン 2 トランスペアレントスイッチは、ドメイン名が一致した場合のみメッセージを転送します。
- 整合性検査 : VTP バージョン 2 の場合、CLI (コマンドラインインターフェイス)、または SNMP (簡易ネットワーク管理プロトコル) を介して新しい情報が入力された場合に限り、VLAN 整合性検査 (VLAN 名、値など) を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

VTP バージョン 1 または 2 でサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 拡張認証：認証を **hidden** または **secret** として設定できます。設定を **hidden** にしている場合、パスワード文字列からの秘密キーは VLAN のデータベース ファイルに保存されますが、設定においてプレーン テキストで表示されることはありません。代わりに、パスワードに関連付けられているキーが 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。キーワード **secret** を入力する場合、パスワードに秘密キーを直接設定できます。
- 拡張範囲 VLAN (VLAN 1006 ~ 4094) のデータベース伝播のサポート。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ~ 1005 だけです。拡張 VLAN を設定している場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。



(注) VTP プルーニングは引き続き VLAN 1 ~ 1005 にだけ適用され、VLAN 1002 ~ 1005 は予約されたままで変更できません。

- プライベート VLAN のサポート。
- ドメインの任意のデータベースをサポートします。VTP 情報の伝播に加えて、バージョン 3 は Multiple Spanning Tree Protocol (MSTP) データベース情報を伝播できます。VTP プロトコルの個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ。VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート済み VTP コンフィギュレーションのバックアップだけです。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。vtp primary 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。プライマリ サーバのステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースのアップデート用に必要となるだけです。プライマリ サーバなしで実用 VTP ドメインを持つことができます。プライマリ サーバのステータスは、スイッチにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。

- トランク (ポート) 単位で VTP をオンまたはオフにするオプション。[no] vtp インターフェイス コンフィギュレーション コマンドを使用すると、ポート単位で VTP をイネーブルまたはディセーブルにできます。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには off にする一方で、同じポートの VLAN データベースには on にすることはできません。

グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定することはできません。たとえば、VLAN データベースには、スイッチを VTP サーバとして設定する一方で、MST データベースには VTP を off に設定することができます。

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッドイングが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可

能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、スイッチのトランク ポート上で VLAN 2 ~ 1001 がプルーニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッディングが行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

図 17-1 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A は、このブロードキャストをフラッディングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

図 17-1 VTP プルーニングを使用しない場合のフラッディング トラフィック

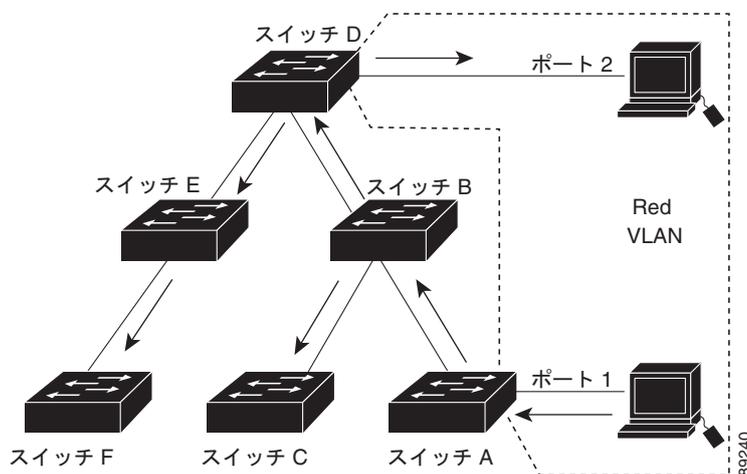
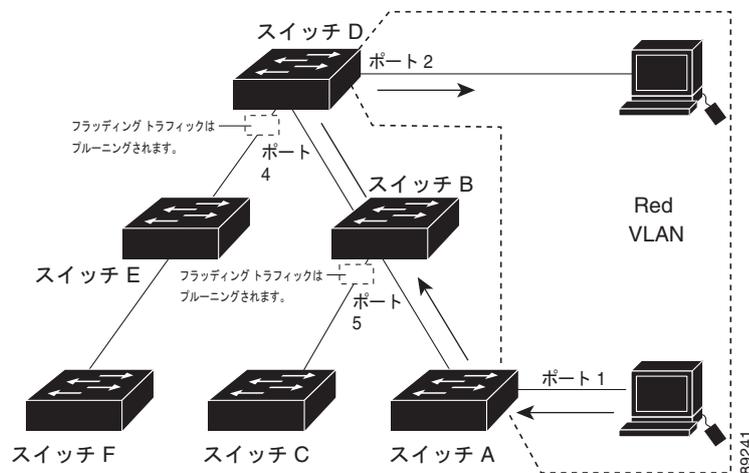


図 17-2 に、VTP プルーニングをイネーブルに設定したスイッチド ネットワークを示します。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されているリンク ポート (スイッチ B のポート 5、およびスイッチ D のポート 4) で、Red VLAN のトラフィックがプルーニングされるからです。

図 17-2 VTP プルーニングによるフラッディング トラフィックの最適化



VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングがイネーブルになります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトランク上の VLAN のプルーニングだけです (VTP ドメイン内のすべてのスイッチに影響するわけではありません)。

「VTP プルーニングのイネーブル化」(P.17-15) を参照してください。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ~ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN (1005 を超える VLAN ID) もプルーニング不適格です。

VTP プルーニングは VTP トランスペアレント モードでは機能しないように設計されています。ネットワーク内に VTP トランスペアレント モードのスイッチが 1 台または複数存在する場合は、次のいずれかを実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します (「プルーニング適格リストの変更」(P.16-21) を参照)。VTP プルーニングは、インターフェイスがトランッキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランッキングを実行しているかどうかにかかわらず、設定できます。

VTP の設定

ここでは、次の設定について説明します。

- 「VTP のデフォルト設定」(P.17-8)
- 「VTP 設定時の注意事項」(P.17-8)
- 「VTP モードの設定」(P.17-10)
- 「VTP バージョンのイネーブル化」(P.17-14)

- 「VTP プルーニングのイネーブル化」 (P.17-15)
- 「ポート単位の VTP の設定」 (P.17-16)
- 「VTP ドメインへの VTP クライアントスイッチの追加」 (P.17-16)

VTP のデフォルト設定

表 17-2 に、VTP のデフォルト設定を示します。

表 17-2 VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード (VTP バージョン 1 およびバージョン 2)	サーバ
VTP モード (VTP バージョン 3)	このモードは、VTP バージョン 3 に変換する前のバージョン 1 または 2 のモードと同じです。
VTP バージョン	バージョン 1
MST データベース モード	トランスペアレント
VTP バージョン 3 のサーバタイプ	セカンダリ
VTP パスワード	なし。
VTP プルーニング	ディセーブル

VTP 設定時の注意事項

VTP パスワード、バージョン、VTP ファイル名、最新の VTP 情報を提供するインターフェイス、ドメイン名、およびモードを設定する場合、さらにプルーニングをディセーブルまたはイネーブルに設定する場合には、**vtp** グローバル コンフィギュレーション コマンドを使用します。使用できるキーワードの詳細については、このリリースに対応するコマンドリファレンスに記載されているコマンドの説明を参照してください。VTP 情報は VTP VLAN データベースに保存されます。VTP モードがトランスペアレントである場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーションファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーションファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。スイッチをリセットした場合、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する必要があります。

スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ) ます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

ドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのスイッチを、同じドメイン名で設定しなければなりません。VTP トランスペアレントモードのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのスイッチについては VTP ドメイン名を設定する必要はありません。

**(注)**

NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバモードにする必要があります。

**注意**

すべてのスイッチが VTP クライアントモードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のスイッチを VTP サーバモードに設定してください。

パスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメインパスワードを設定する場合は、すべてのドメインスイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。パスワードのないスイッチ、またはパスワードが不正なスイッチは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワードを使用して設定しない限り、VTP アドバタイズを受信しません。設定後、スイッチは同じパスワードおよびドメイン名を使用した VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、スイッチはドメイン名を学習します。

**注意**

VTP ドメインパスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメインパスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルに設定されている場合、VTP バージョン 2 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ VTP ドメインで動作できます (デフォルトでは VTP バージョン 2 はディセーブルになっています)。
- VTP バージョン 1 を実行しているものの、VTP バージョン 2 に対応可能なスイッチが VTP バージョン 3 アドバタイズを受信すると、このスイッチは VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 を実行しているスイッチが VTP バージョン 1 を実行しているスイッチに接続すると、VTP バージョン 1 のスイッチは VTP バージョン 2 に移行し、VTP バージョン 3 のスイッチは、スケールダウンしたバージョンの VTP パケットを送信するため、VTP バージョン 2 スwitchは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するスイッチは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行できません。

- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応可能な場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。あるスイッチでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがドメインに含まれている場合、そのスイッチはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 のスイッチは VTP バージョン 3 のアドバタイズを転送しないため、これらをネットワーク エッジに配置することを推奨します。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークンリング VLAN スwitチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン 3 は拡張範囲 VLAN をサポートします。拡張 VLAN を設定している場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- VTP バージョン 3 装置のトランク ポートが VTP バージョン 2 装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上で VTP バージョン 2 フォーマットを使用して送信します。VTP バージョン 3 装置は、最初にそのトランク ポートで VTP バージョン 2 パケットを受信しない限り、VTP バージョン 2 フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方のネイバーが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バージョン 3 パケットの送信も続きます。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 リージョンまたはバージョン 2 リージョンでは、トランスペアレント モードでだけ通信できます。
- VTP バージョン 1 にだけ対応する装置は、VTP バージョン 3 装置との相互運用はできません。

設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズメントを送受信できるように、トランク ポートを設定する必要があります。

詳細については、「[VLAN トランクの設定](#)」(P.16-15) を参照してください。

クラスタ メンバスイッチの VTP を VLAN に設定する場合、**rcommand** 特権 EXEC コマンドを使用して、そのメンバスイッチにログインします。コマンドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VTP バージョン 1 および 2 では、そのスイッチで拡張範囲 VLAN を設定するとき、スイッチは VTP トランスペアレント モードでなければなりません。VTP バージョン 3 でも、クライアント モードまたはサーバ モードでの拡張範囲 VLAN の作成をサポートしています。

VTP モードの設定

次のいずれかに VTP モードを設定できます。

- スイッチが VTP サーバ モードの場合には、VLAN 設定を変更し、その変更をネットワーク全体に伝播できます。

- スイッチが VTP クライアント モードの場合には、そのスイッチの VLAN 設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- スイッチを VTP トランスペアレント モードに設定すると、スイッチの VTP はディセーブルになります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 を実行する VTP トランスペアレント モードのスイッチは、対応するトランク リンクで、受信した VTP アドバタイズを転送します。
- VTP オフ モードは、VTP アドバタイズが転送されない以外は、VTP トランスペアレント モードと同じです。

次の注意事項に従ってください。

- VTP バージョン 1 およびバージョン 2 では、拡張範囲 VLAN がスイッチ上に設定されている場合、VTP モードをクライアントまたはサーバに変更できません。エラー メッセージが表示され、設定が許可されません。VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。



(注) VTP バージョン 1 およびバージョン 2 の場合、拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を作成するには、事前に **vtp mode transparent** グローバル コンフィギュレーション コマンドを使用して、VTP モードをトランスペアレントに設定する必要があります。VTP トランスペアレント モードでスイッチが開始するように、この設定をスタートアップ コンフィギュレーションに保存してください。このようにしないと、スイッチのリセット時に拡張範囲 VLAN 設定が失われ、VTP サーバ モード (デフォルト) で起動します。

- VTP バージョン 3 は拡張範囲 VLAN をサポートします。拡張 VLAN が設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- スイッチを VTP クライアント モードに設定した場合、VLAN データベース ファイル (vlan.dat) は作成されません。そのままスイッチの電源をオフにすると、VTP 設定はデフォルトにリセットされます。スイッチが再起動された後も VTP 設定を VTP クライアント モードに維持するには、VTP モードを設定する前に、VTP ドメイン名を設定する必要があります。

**注意**

すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメイン名を設定しないでください。ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。したがって、少なくとも 1 台のスイッチを VTP サーバとして設定してください。

VTP モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vtp domain domain-name</code>	VTP 管理ドメイン名を設定します。1 ~ 32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのスイッチは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードではドメイン名が必要です。スイッチで VTP ドメインにトランクを接続している場合、スイッチはドメインの VTP サーバからドメイン名を学習します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。
ステップ3	<code>vtp mode {client server transparent off} {vlan mst unknown}</code>	VTP モード (クライアント、サーバ、トランスペアレントまたはオフ) のスイッチの設定。 (任意) データベースを次のように設定します。 <ul style="list-style-type: none"> • vlan : 何も設定されていない場合は VLAN データベースがデフォルトです。 • mst : 多重スパンニングツリー (MST) データベース。 • unknown : データベース タイプは不明。
ステップ4	<code>vtp password password</code>	(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ~ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各スイッチに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。 VTP バージョン 3 で使用可能なオプションについては、「 VTP バージョン 3 のパスワードの設定 」(P.17-13) を参照してください。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show vtp status</code>	表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドの設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。 (注) スイッチの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

設定したドメイン名は、削除できません。別のドメインにスイッチを再び割り当てるしかありません。

別のモードのスイッチを VTP サーバ モードに戻すには、**no vtp mode** グローバル コンフィギュレーション コマンドを使用します。スイッチをパスワードがない状態に戻すには、**no vtp password** グローバル コンフィギュレーション コマンドを使用します。

次に、ドメイン名が *eng_group*、パスワードが *mypassword* という VTP サーバとしてスイッチを設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANs.
Switch(config)# vtp password mypassword
```

```
Setting device VLAN database password to mypassword.
Switch(config)# end
```

VTP バージョン 3 のパスワードの設定

VTP バージョン 3 を使用する場合にパスワードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vtp password password [hidden secret]</code>	<p>(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ~ 64 文字です。</p> <ul style="list-style-type: none"> (任意) hidden : パスワード文字列から生成された秘密キーが <code>nvam:vlan.dat</code> ファイルに保存されるようにするには、hidden を入力します。VTP プライマリ サーバを設定してテイクオーバーを設定しようとする、パスワードの再入力を要求されます。 (任意) secret : パスワードを直接設定するには、secret を入力します。シークレットパスワードには 16 進数文字を 32 個含める必要があります。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show vtp password</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

パスワードをクリアするには、`no vtp password` グローバル コンフィギュレーション コマンドを入力します。

次に、非表示のパスワードの設定方法とその表示方法の例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP バージョン 3 のプライマリ サーバの設定

VTP サーバを VTP プライマリ サーバ (バージョン 3 限定) として設定し、テイクオーバー操作を開始するには、特権 EXEC モードの VTP サーバで次の手順を実行します。

コマンド	目的
ステップ1 <code>vtp primary-server [vlan mst] [force]</code>	<p>スイッチの動作ステートをセカンダリ サーバ (デフォルト) からプライマリ サーバに変更し、その設定をドメインにアドバタイズします。スイッチのパスワードが hidden に設定されている場合は、パスワードの再入力を要求されます。</p> <ul style="list-style-type: none"> (任意) vlan : テイクオーバー機能として VLAN データベースを選択します。これはデフォルトです。 (任意) mst : テイクオーバー機能として Multiple Spanning Tree (MST; 多重スパニングツリー) データベースを選択します。 (任意) force : force と入力すると、競合するサーバの設定が上書きされます。force を入力しない場合、テイクオーバーの実行前に確認を求められます。

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプライマリ サーバ (デフォルト) としてスイッチを設定する方法の例を示します。

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP domain

VTP Database Conf Switch ID      Primary Server Revision System Name
-----
VLANDB          Yes  00d0.00b8.1400=00d0.00b8.1400 1      stp7

Do you want to continue (y/n) [n]? y
```

VTP バージョンのイネーブル化

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。

- あるスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各スイッチ上で手動によって設定する必要があります。
- VTP バージョン 1 および 2 では、VTP サーバモードまたはトランスペアレントモードのスイッチでだけバージョンを設定できます。VTP バージョン 3 を実行するスイッチがクライアントモードの場合、既存の拡張 VLAN や既存のプライベート VLAN がなく、パスワードが非表示に設定されていないときであれば、バージョン 2 に変更できます。



注意

同一 VTP ドメイン内のスイッチ上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにする必要があります。
- VTP バージョン 3 は、Cisco IOS Release 12.2(52) SE 以降でサポートされます。



注意

VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

VTP バージョンを設定する場合の注意事項については、「[VTP バージョン](#)」(P.17-9) を参照してください。

VTP バージョンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vtp version {1 2 3}</code>	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show vtp status</code>	設定された VTP バージョンがイネーブルであることを確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルトの VTP バージョン 1 に戻るには、`no vtp version` グローバル コンフィギュレーション コマンドを使用します。

VTP プルーニングのイネーブル化

プルーニングは、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクだけにフラッドイング トラフィックを制限することによって、使用可能な帯域幅を増やします。VTP プルーニングをイネーブルにできるのは、スイッチが VTP サーバ モードの場合だけです。

VTP ドメイン内で VTP プルーニングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vtp pruning</code>	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバ モードの 1 台のスイッチ上に限ってプルーニングをイネーブルにする必要があります。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show vtp status</code>	表示された <i>VTP Pruning Mode</i> フィールドの設定を確認します。

VTP プルーニングをディセーブルにするには、`no vtp pruning` グローバル コンフィギュレーション コマンドを使用します。

VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメイン全体でプルーニングがイネーブルになります。VTP バージョン 3 では、ドメイン内の各スイッチ上で手動によってプルーニングをイネーブルにする必要があります。

プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、トランク ポート上で VLAN 2 ~ 1001 がプルーニング適格です。専用の VLAN および拡張範囲 VLAN をプルーニングすることはできません。プルーニング適格の VLAN を変更する手順については、「[プルーニング適格リストの変更](#)」(P.16-21) を参照してください。

ポート単位の VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP は、トランク モードのポート上でだけイネーブルにできます。VTP トラフィックの着信または発信はブロックされ、転送されません。

ポート上で VTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>vtp</code>	指定されたポート上で VTP をイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config interface interface-id</code>	ポートの変更を確認します。
ステップ 6	<code>show vtp status</code>	設定を確認します。

インターフェイス上で VTP をディセーブルにするには、`no vtp` インターフェイス コンフィギュレーション コマンドを使用します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# vtp
Switch(config-if)# end
```

VTP ドメインへの VTP クライアント スイッチの追加

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報が消去されることはありません。

VTP ドメインに追加する前に、スイッチ上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>show vtp status</code>	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、スイッチを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 a. ドメイン名を書き留めます。 b. コンフィギュレーション リビジョン番号を書き留めます。 c. 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>vtp domain domain-name</code>	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ4	<code>end</code>	スイッチの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。特権 EXEC モードに戻ります。
ステップ5	<code>show vtp status</code>	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ6	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ7	<code>vtp domain domain-name</code>	スイッチの元のドメイン名を入力します。
ステップ8	<code>end</code>	スイッチの VLAN 情報が更新されて、特権 EXEC モードに戻ります。
ステップ9	<code>show vtp status</code>	(任意) ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

コンフィギュレーション リビジョン番号をリセットした後に、スイッチを VTP ドメインに追加します。



(注) スイッチ上で VTP をディセーブルにし、VTP ドメイン内の他のスイッチに影響を与えることなく VLAN 情報を変更するには、`vtp mode transparent` グローバル コンフィギュレーション コマンドを使用します。

VTP のモニタ

VTP の設定情報（ドメイン名、現在の VTP バージョン、VLAN 数）を表示することによって、VTP をモニタします。スイッチで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 17-3 に、VTP アクティビティをモニタするための特権 EXEC コマンドを示します。

表 17-3 VTP モニタ コマンド

コマンド	目的
<code>show vtp counters</code>	送受信された VTP メッセージに関するカウンタを表示します。
<code>show vtp devices [conflict]</code>	ドメイン内のすべての VTP バージョン 3 デバイズに関する情報を表示します。プライマリ サーバと競合する VTP バージョン 3 の装置が表示されます。 <code>show vtp devices</code> コマンドは、スイッチがトランスペアレントモードまたはオフモードのときは情報を表示しません。
<code>show vtp interface [interface-id]</code>	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
<code>show vtp password</code>	VTP パスワードを表示します。表示されるパスワードの形式は、 hidden キーワードが入力されているか、または、暗号化がスイッチでイネーブル化されているかどうかによって異なります。
<code>show vtp status</code>	VTP スイッチの設定情報を表示します。



CHAPTER 18

音声 VLAN の設定

この章では、IE 3000 スイッチで音声 VLAN 機能を設定する方法について説明します。Catalyst 6500 ファミリー スイッチの一部のマニュアルでは、音声 VLAN を *補助 VLAN* と表しています。



(注)

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

この章で説明する内容は、次のとおりです。

- 「音声 VLAN の概要」 (P.18-1)
- 「音声 VLAN の設定」 (P.18-3)
- 「音声 VLAN の表示」 (P.18-7)

音声 VLAN の概要

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP precedence およびレイヤ 2 サービスクラス (CoS) 値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service (QoS) をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワークトラフィックを予測可能な方法で送信します。QoS の詳細については、[第 39 章「QoS の設定」](#)を参照してください。

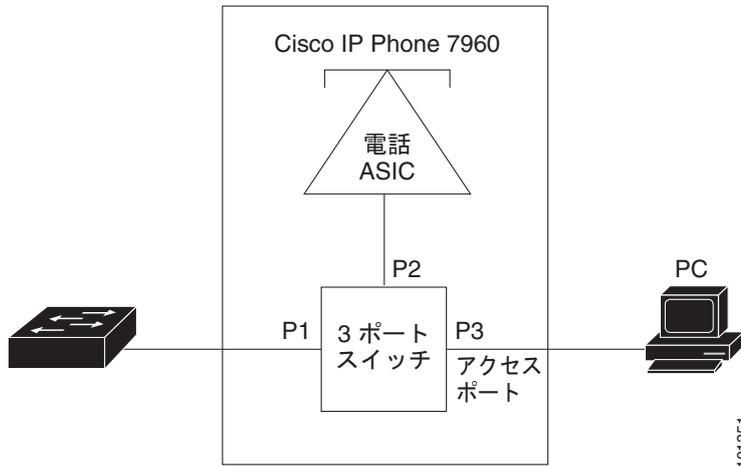
Cisco 7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

Cisco IP Phone には、3 ポートの 10/100 スイッチが統合されています。[図 18-1](#)を参照してください。これらのポートは、次のデバイスへの接続専用です。

- ポート 1 は、スイッチまたは他の Voice over IP (VoIP) デバイスに接続します。
- ポート 2 は、IP Phone のトラフィックを伝送する内部 10/100 インターフェイスです。
- ポート 3 (アクセス ポート) は、PC または他のデバイスに接続します。

図 18-1 に、Cisco7960 IP Phone の接続方法の例を示します。

図 18-1 スイッチに接続された Cisco7960 IP Phone



Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセスポートを、1つの VLAN は音声トラフィック用に、もう1つの VLAN は Cisco IP Phone に接続しているデバイスからのデータトラフィック用に使用するように設定できます。スイッチ上のアクセスポートを設定して、Cisco Discovery Protocol (CDP) パケットを送信させることができます。CDP には、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指定します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし (レイヤ 2 CoS プライオリティ値なし) のアクセス VLAN による送信



(注)

いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値 (音声トラフィックはデフォルトで 5、音声制御トラフィックは 3) を伝送します。

Cisco IP Phone のデータトラフィック

スイッチは、Cisco IP Phone のアクセスポートに接続されたデバイス (図 18-1 を参照) から送られた、タグ付きデータトラフィック (IEEE 802.1Q または IEEE 802.1p フレームタイプのトラフィック) を処理することもできます。スイッチ上のレイヤ 2 アクセスポートが、CDP パケットを送信するように設定できます。CDP は、接続する IP Phone に、次のいずれかのモードで IP Phone 上のアクセスポートを設定するように指定します。

- **trusted** (信頼性がある) モードでは、Cisco IP Phone のアクセスポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- **untrusted** (信頼性がない) モードでは、Cisco IP Phone のアクセスポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。untrusted モードがデフォルトの設定です。



(注) Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

音声 VLAN の設定

ここでは、次の設定について説明します。

- 「音声 VLAN のデフォルト設定」 (P.18-3)
- 「音声 VLAN 設定時の注意事項」 (P.18-3)
- 「Cisco7960 IP Phone に接続するポートの設定」 (P.18-4)

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN 設定時の注意事項

音声 VLAN の設定時の注意事項を次に示します。

- 音声 VLAN 設定はスイッチのアクセス ポートだけでサポートされており、トランク ポートではサポートされていません。



(注) トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。音声 VLAN の設定は、トランク ポートでは不要です。

- IP Phone での通信が適切に行えるように、音声 VLAN はスイッチ上でアクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します (リストで表示されます)。VLAN がリストになかった場合、音声 VLAN の作成方法について、第 16 章「VLAN の設定」を参照してください。
- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を **trust** に設定しておくことを推奨します。自動 QoS 機能を使用すると、これらは自動的に設定されます。詳細については、第 39 章「QoS の設定」を参照してください。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります (デフォルト設定では、CDP がすべてのスイッチ インターフェイスでグローバルにイネーブルです)。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
 - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
 - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
 - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
 - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです（ルーティングによってフレーム タイプの相違が排除されます）。
- 音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。
- 音声 VLAN ポートには次のポート タイプがあります。
 - ダイナミック アクセス ポート。詳細については、「[VMPS クライアント上のダイナミックアクセス ポートの設定](#)」(P.16-29) を参照してください。
 - IEEE 802.1x 認証ポート。詳細については、「[802.1x 準備状態チェックの設定](#)」(P.12-36) を参照してください。



(注) 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにした場合、その IP Phone のスイッチへの接続が最大 30 秒間失われます。

- 保護ポート。詳細については、「[保護ポートの設定](#)」(P.29-6) を参照してください。
- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) または Remote SPAN (RSPAN) セッションの送信元ポートまたは宛先ポート。
- セキュア ポート。詳細については、「[ポートセキュリティの設定](#)」(P.29-9) を参照してください。



(注) 音声 VLAN も設定しているインターフェイス上でポートセキュリティをイネーブルにする場合、ポートで許容されるセキュアアドレスの最大数を、アクセス VLAN におけるセキュアアドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

Cisco7960 IP Phone に接続するポートの設定

Cisco7960 IP Phone は、PC または他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータトラフィックの伝送方法を決定できます。

ここでは、次の設定について説明します。

- 「Cisco IP Phone の音声トラフィックの設定」 (P.18-5)
- 「着信データ フレームのプライオリティ設定」 (P.18-6)

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティタグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ (アクセス) VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値 (デフォルトは 5) を伝送します。

ポート上で音声トラフィックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>mls qos trust cos</code>	パケットの CoS 値を使用して着信するトラフィック パケットを分類するように、インターフェイスを設定します。タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。 (注) ポートの信頼状態を設定する前に、 <code>mls qos</code> グローバル コンフィギュレーション コマンドを使用することによって、QoS をグローバルでイネーブルに設定しておく必要があります。
ステップ4	<code>switchport voice vlan {vlan-id dot1p none untagged}</code>	Cisco IP Phone による音声トラフィックの伝送方法を設定します。 <ul style="list-style-type: none"> • vlan-id : すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。指定できる VLAN ID の範囲は 1 ~ 4094 です。 • dot1p : 音声トラフィック用に IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN (VLAN 0) を使用してすべてのトラフィックを搬送するように、Cisco IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 • none : IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 • untagged : タグなしの音声トラフィックを送信するように IP Phone を設定します。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show interfaces interface-id switchport</code> または <code>show running-config interface interface-id</code>	音声 VLAN の設定を確認します。 QoS および音声 VLAN の設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Cisco IP Phone に接続されたポートが、CoS 値を使用して着信トラフィックを分類し、音声トラフィックに IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN (VLAN0) を使用してすべてのトラフィックを搬送するように設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport voice vlan** インターフェイス コンフィギュレーション コマンドを使用します。

着信データ フレームのプライオリティ設定

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック (IEEE 802.1Q または IEEE 802.1p フレーム) を処理するために、スイッチが CDP パケットを送信するように設定できます。CDP は、Cisco IP Phone に、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケットをどのように送信するかを指定します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない (信頼する) または変更する (信頼しない) ように、IP Phone を設定できます。

Cisco IP Phone の非音声ポートから受信したデータ トラフィックのプライオリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport priority extend {cos value trust}	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを設定します。 <ul style="list-style-type: none"> • cos value : PC または接続しているデバイスから受信したプライオリティを指定の CoS 値に変更するように、IP Phone を設定します。値は 0 ~ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは cos 0 です。 • trust : PC または接続しているデバイスから受信したプライオリティを信頼するように IP Phone のアクセス ポートを設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id switchport	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Cisco IP Phone に接続しているポートを設定して、PC または接続しているデバイスから受信するフレームのプライオリティを変更しないようにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。

音声 VLAN の表示

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを使用します。



CHAPTER 19

プライベート VLAN の設定

この章では、IE 3000 スイッチにプライベート VLAN を設定する手順について説明します。プライベート VLAN は、IP サービス イメージが稼働しているスイッチでだけサポートされます。



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

この章の内容は、次のとおりです。

- 「プライベート VLAN の概要」(P.19-1)
- 「プライベート VLAN の設定」(P.19-6)
- 「プライベート VLAN のモニタリング」(P.19-15)



(注) プライベート VLAN を設定した場合、スイッチは VLAN Trunking Protocol (VTP; VLAN トランキングプロトコル) トランスペアレント モードでなければなりません。第 17 章「VTP の設定」を参照してください。

プライベート VLAN の概要

プライベート VLAN 機能は、サービス プロバイダーが VLAN を使用している場合に直面する 2 つの問題に対処します。

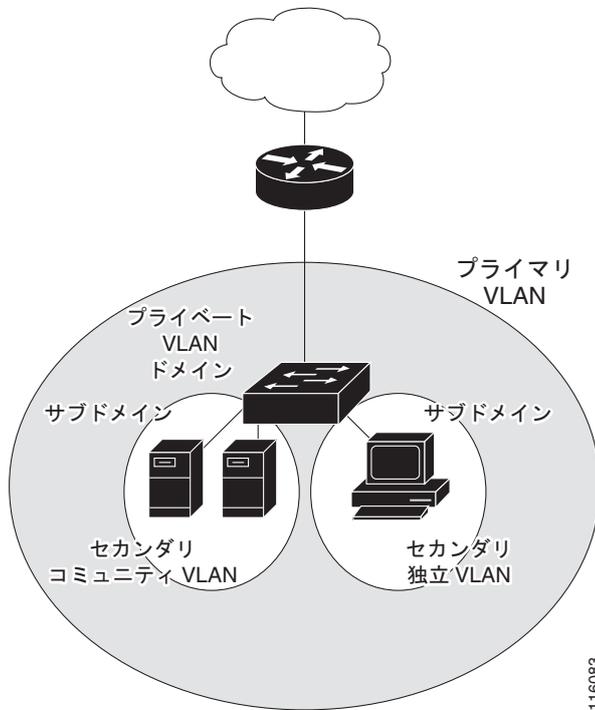
- スケーラビリティ：スイッチは最大 1005 のアクティブ VLAN をサポートします。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネットアドレス空間またはアドレスブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処でき、サービス プロバイダーにとっては IP アドレス管理上の利得がもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。

プライベート VLAN は、通常の VLAN ドメインをサブドメインに分割するもので、複数の VLAN ペア（各サブドメインに 1 つの VLAN）を持つことができます。サブドメインは、プライマリ VLAN およびセカンダリ VLAN という VLAN のペアで表現されます。

プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。図 19-1 を参照してください。

図 19-1 プライベート VLAN ドメイン



セカンダリ VLAN には、次の 2 種類があります。

- 独立 VLAN : 独立 VLAN 内のポートは、レイヤ 2 レベルでは互いに通信できません。
- コミュニティ VLAN : コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次の 3 つのタイプがあります。

- 無差別 : 無差別ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立 : 独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。これは、無差別ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートだけに転送されます。
- コミュニティ : コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同一コミュニティ VLAN のその他のポート、および無差別ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。



(注)

トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- **プライマリ VLAN** : プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、無差別ポートからの単一方向トラフィックのダウンストリームを、(独立およびコミュニティ) ホストポートおよび他の無差別ポートへ伝送します。
- **独立 VLAN** : プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN は、ホストからの単一方向トラフィック アップストリームを無差別ポートおよびゲートウェイへ伝送するセカンダリ VLAN です。
- **コミュニティ VLAN** : コミュニティ VLAN は、コミュニティポートからのアップストリームトラフィックを無差別ポートゲートウェイおよび同じコミュニティ内の他のホストポートへ伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

無差別ポートが扱えるのは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN だけです。レイヤ 3 ゲートウェイは通常無差別ポートを介してスイッチに接続されています。無差別ポートでは、広範囲なデバイスをプライベート VLAN のアクセスポイントとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションから監視したりバックアップしたりするのに、無差別ポートを使用できます。

スイッチ環境では、個々のプライベート VLAN とアソシエートされている IP サブネットを、各エンドステーションやエンドステーションの共通グループに割り当てることができます。プライベート VLAN の外部と通信するには、エンドステーションでは、デフォルトゲートウェイのみと通信する必要があります。

プライベート VLAN を使用してエンドステーションへのアクセスを次のように制御できます。

- エンドステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンドステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- すべてのエンドステーションがデフォルトゲートウェイにアクセスできるようにするには、デフォルトゲートウェイおよびエンドステーションに接続されているインターフェイスを、無差別ポートとして設定します。

プライマリ、独立、およびコミュニティ VLAN をプライベート VLAN をサポートする他のデバイスにトランッキングすることで、プライベート VLAN を複数のデバイスに拡張できます。プライベート VLAN コンフィギュレーションのセキュリティを保って VLAN の他のユーザがプライベート VLAN に設定されないようにするには、プライベート VLAN ポートのないデバイスを含む、すべての中間デバイス内にプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

- カスタマーの VLAN にアドレスブロックを割り当てると、未使用の IP アドレスが出てきます。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

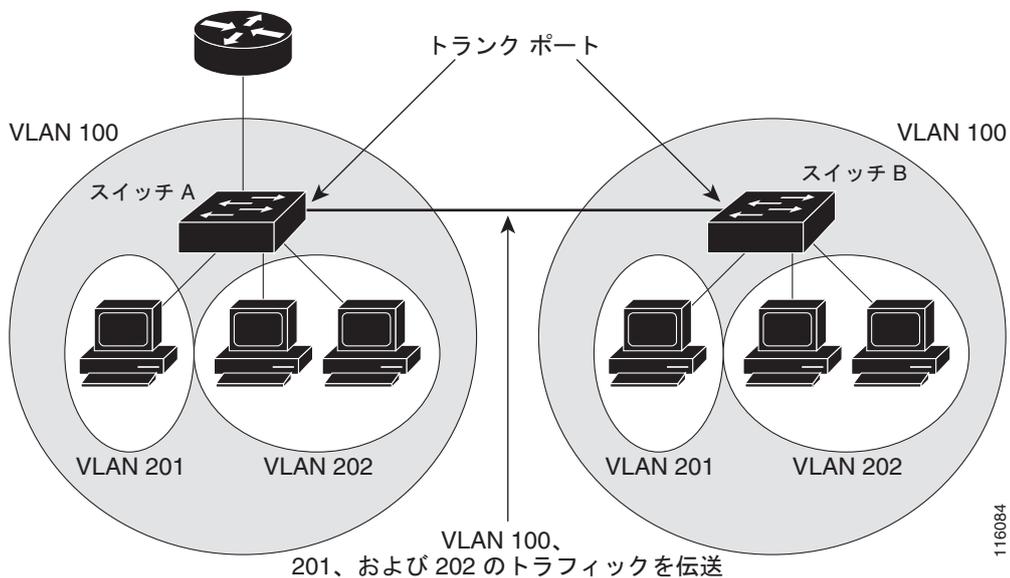
これらの問題は、プライベート VLAN を使用することで軽減できます。この場合、プライベート VLAN 内のすべてのメンバーがプライマリ VLAN に割り当てられた共通アドレス空間を共有します。ホストはセカンダリ VLAN に接続され、DHCP サーバがプライマリ VLAN に割り当てられたアドレスブロックから IP アドレスを割り当てます。後続の IP アドレスは、同じプライマリ VLAN にある別の

セカンダリ VLAN にあるカスタマー デバイスに割り当てることができます。新しいデバイスが追加されると、DHCP サーバはサブネット アドレスの大きなプールから次に使用可能なアドレスをデバイスに割り当てます。

複数のスイッチの PVLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランク ポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランク ポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。図 19-2 を参照してください。

図 19-2 複数のスイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
 VLAN 201 = セカンダリ独立 VLAN
 VLAN 202 = セカンダリ コミュニティ VLAN

VTP はプライベート VLAN をサポートしないので、レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、これらのスイッチのレイヤ 2 データベースは統合されません。これにより、これらのスイッチにプライベート VLAN トラフィックの不要なフラッドが発生する可能性があります。



(注)

プライベート VLAN をスイッチに設定するときに、ユニキャスト ルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management (SDM) テンプレートを请使用してください。別の SDM テンプレートが設定されている場合、デフォルト テンプレートを設定するのに `sdm prefer default` グローバル コンフィギュレーション コマンドを使用します。第 10 章「SDM テンプレートの設定」を参照してください。

プライベート VLAN の他機能との相互作用

プライベート VLAN には、次のように他の機能と相互作用があります。

- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」 (P.19-5)
- 「プライベート VLAN と SVI」 (P.19-5)

「セカンダリ VLAN およびプライマリ VLAN の設定」 (P.19-7) の下にある「プライベート VLAN 設定時の注意事項」も参照してください。

プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN では、無差別ポートはプライマリ VLAN のメンバーで、ホストポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN ブロードキャスト転送は、次のようにブロードキャストを送信するポートに左右されます。

- 独立ポートはブロードキャストを無差別ポートまたはトランク ポートにだけ送信します。
- コミュニティ ポートは、すべての無差別ポート、トランク ポート、および同じコミュニティ VLAN 内のポートにブロードキャストを送信します。
- 無差別ポートは、プライベート VLAN のすべてのポート（他の無差別ポート、トランク ポート、独立ポート、コミュニティ ポート）にブロードキャストを送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて単一のコミュニティ VLAN 内にルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN 内のポート間で転送されず、また別のセカンダリ VLAN 内のポート間でも転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチでは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなくプライマリ VLAN を介してだけプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイスをプライマリ VLAN に対してだけ設定します。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。VLAN がセカンダリ VLAN として設定されている間、セカンダリ VLAN の SVI は非アクティブになります。

- アクティブ SVI を設定した VLAN をセカンダリ VLAN として設定しようとする、SVI をディセーブルにするまで設定が許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされません。

プライマリ VLAN がセカンダリ VLAN に対応付けられていてマッピングされていると、プライマリ VLAN 上の設定はセカンダリ VLAN SVI に伝播されます。たとえば、IP サブネットをプライマリ VLAN SVI に割り当てる場合、このサブネットはプライベート VLAN 全体の IP サブネットアドレスです。

プライベート VLAN の設定

ここでは、次の設定について説明します。

- 「プライベート VLAN の設定手順」 (P.19-6)
- 「デフォルトのプライベート VLAN 設定」 (P.19-6)
- 「プライベート VLAN 設定時の注意事項」 (P.19-6)
- 「プライベート VLAN 内の VLAN の設定および対応付け」 (P.19-10)
- 「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」 (P.19-11)
- 「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」 (P.19-12)
- 「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」 (P.19-13)

プライベート VLAN の設定手順

プライベート VLAN を設定するには、次の手順を実行します。

-
- ステップ 1** VTP モードをトランスペアレントに設定します。
- ステップ 2** プライマリおよびセカンダリ VLAN を作成してこれらに対応付けします。「プライベート VLAN 内の VLAN の設定および対応付け」 (P.19-10) を参照してください。
-  **(注)** VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。
-
- ステップ 3** インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバーシップを割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」 (P.19-11) を参照してください。
- ステップ 4** インターフェイスを無差別ポートとして設定し、無差別ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。「プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定」 (P.19-12) を参照してください。
- ステップ 5** VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」 (P.19-13) を参照してください。
- ステップ 6** プライマリ VLAN 設定を確認します。
-

デフォルトのプライベート VLAN 設定

プライベート VLAN は設定されていません。

プライベート VLAN 設定時の注意事項

プライベート VLAN 設定時の注意事項は、次のカテゴリに分けられます。

- 「セカンダリ VLAN およびプライマリ VLAN の設定」 (P.19-7)

- 「プライベート VLAN ポート設定」(P.19-8)
- 「他の機能に関連する制約事項」(P.19-9)

セカンダリ VLAN およびプライマリ VLAN の設定

プライベート VLAN の設定を行うときは、次の注意事項に従ってください。

- スイッチで VTP バージョン 1 または 2 が稼働している場合は、VTP をトランスペアレント モードに設定する必要があります。プライベート VLAN を設定した後で、VTP モードをクライアントまたはサーバに変更できません。VTP の詳細については、第 17 章「VTP の設定」を参照してください。VTP バージョン 3 では、プライベート VLAN はすべてのモードでサポートされます。
- VTP バージョン 1 または 2 でプライベート VLAN を設定後、**copy running-config startup config** 特権 EXEC コマンドを使用して VTP トランスペアレント モード設定およびプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 ではプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 では、プライベート VLAN 設定の伝播は行われません。プライベート VLAN ポートが必要なデバイスで VTP バージョン 3 が実行されていない場合は、そのデバイス上でプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ~ 1005 をプライマリ VLAN またはセカンダリ VLAN として設定できません。拡張 VLAN (VLAN ID 1006 ~ 4094) はプライベート VLAN に属することができます。
- プライマリ VLAN には、1 つの独立 VLAN および複数のコミュニティ VLAN を関連付けることができます。独立またはコミュニティ VLAN には、これに対応付けられたプライマリ VLAN を 1 つだけ設定できます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能なスパンニングツリー プロトコル (STP) インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、プライマリ VLAN の STP パラメータがセカンダリ VLAN に伝播されます。
- プライベート VLAN で DHCP スヌーピングをイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにする場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN で DHCP を設定しても、プライマリ VLAN をすでに設定している場合、その設定は有効になりません。
- プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
- プライベート VLAN 内でトラフィックを伝送していないデバイスのトランクからプライベート VLAN をブルーニングすることを推奨します。
- プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN には、別々の Quality of Service (QoS) を適用できます。
- Sticky ARP
 - sticky ARP エントリとは、SVI およびレイヤ 3 インターフェイス上で学習されるエントリです。Sticky ARP エントリには期限切れがありません。
 - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI だけでサポートされます。
 - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、次の上でだけサポートされます。
レイヤ 3 インターフェイス

標準 VLAN に属する SVI

プライベート VLAN に属する SVI

ip sticky-arp グローバルコンフィギュレーション コマンドおよび **ip sticky-arp** インターフェイス コンフィギュレーション コマンドの使用の詳細については、このリリースを参照してください。

- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます（「[VLAN マップの設定](#)」(P.38-31) を参照）。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
 - ホスト ポートから無差別ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
 - 無差別ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。

- プライマリ VLAN SVI にだけルータ Access Control List (ACL; アクセス コントロール リスト) を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
- プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
- プライベート VLAN では、次のスイッチド ポート アナライザ (SPAN) 機能がサポートされます。
 - プライベート VLAN を SPAN 送信元ポートとして設定できます。
 - VLAN ベースの SPAN (VSPAN) はプライマリ VLAN、独立 VLAN、およびコミュニティ VLAN で使用できます。また、出力または入力トラフィックを別々にモニタするために、1 つの VLAN だけで SPAN を使用できます。

プライベート VLAN ポート設定

プライベート VLAN ポートの設定を行うときは、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN コンフィギュレーション コマンドだけを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定した VLAN に割り当てられたレイヤ 2 アクセスポートは、VLAN がプライベート VLAN 設定の一部の間は非アクティブになります。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- ポート集約プロトコルまたは Link Aggregation Control Protocol (LACP) EtherChannel に属するポートをプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN 設定に含まれていると、ポートの EtherChannel 設定が非アクティブになります。
- 誤った設定による STP ループを発生させず、STP コンバージェンスを高速にするために、独立およびコミュニティ ホスト ポートで PortFast および Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) ガードをイネーブルにします（第 23 章「[オプションのスパニングツリー機能の設定](#)」を参照）。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを無差別ポートでイネーブルにしないでください。
- プライベート VLAN 設定で VLAN を削除した場合、VLAN に対応付けられたプライベート VLAN ポートが非アクティブになります。

- デバイスがトランクに接続されていてプライマリおよびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートを別のネットワーク デバイス上に設定できます。

他の機能に関連する制約事項

プライベート VLAN を設定する際に、他の機能との間で次のような制限があることに留意してください。



(注)

エラー メッセージなしで設定が受け入れられていても、コマンドが機能しない場合があります。

- プライベート VLAN が設定されたスイッチにフォールバック ブリッジングを設定しないでください。
- Internet Group Management Protocol (IGMP) スヌーピングがスイッチ上でイネーブル (デフォルト) の場合、スイッチがサポートするプライベート VLAN ドメイン数は、20 までです。
- Remote SPAN (RSPAN; リモート SPAN) をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。

SPAN の詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。

- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
 - ダイナミックアクセス ポート VLAN メンバーシップ
 - ダイナミック トランッキング プロトコル (DTP)
 - Port Aggregation Protocol (PAgP; ポート集約プロトコル)
 - リンク アグリゲーション制御プロトコル (LACP)
 - Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション)
 - 音声 VLAN
 - Web Cache Communication Protocol (WCCP)
- プライベート VLAN ポートはセキュア ポートにはできないので、保護ポートとして設定できません。
- IEEE 802.1X ポートベース認証をプライベート VLAN ポートに設定できますが、IEEE 802.1X とポート セキュリティ、音声 VLAN、またはポート単位のユーザ ACL を、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは無差別ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN 内の無差別ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連セカンダリ VLAN に追加する必要があります。セカンダリ VLAN 内ホスト ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連プライマリ VLAN に追加する必要があります。スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。



(注)

プライベート VLAN の 1 つの VLAN で学習したダイナミック MAC アドレスは、関連 VLAN で複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。元のダイナミック MAC アドレスが削除されたり期限が切れた場合、複製アドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイスをプライマリ VLAN に対してだけ設定します。

プライベート VLAN 内の VLAN の設定および対応付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を行います。



(注) **private-vlan** コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vtp mode transparent	VTP モードをトランスペアレントに設定します (VTP をディセーブルにします)。
ステップ 3	vlan vlan-id	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 4	private-vlan primary	VLAN をプライマリ VLAN として指定します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	vlan vlan-id	(任意) VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 7	private-vlan isolated	VLAN を独立 VLAN として指定します。
ステップ 8	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	vlan vlan-id	(任意) VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 10	private-vlan community	VLAN をコミュニティ VLAN として指定します。
ステップ 11	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	vlan vlan-id	ステップ 2 で指定したプライマリ VLAN 用の VLAN コンフィギュレーション モードを開始します。
ステップ 13	private-vlan association [add remove] secondary_vlan_list	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 14	end	特権 EXEC モードに戻ります。
ステップ 15	show vlan private-vlan [type] または show interfaces status	設定を確認します。
ステップ 16	copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。プライベート VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスペアレント モード設定とプライベート VLAN 設定を保存する必要があります。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。

セカンダリ VLAN をプライマリ VLAN に関連付ける際に、構文に関して次のことに留意してください。

- `secondary_vlan_list` パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- `secondary_vlan_list` パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。
- `secondary_vlan_list` を入力するか、または `add` キーワードを指定した `secondary_vlan_list` を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。
- `remove` キーワードとともに `secondary_vlan_list` を使用して、セカンダリ VLAN とプライマリ VLAN の関連付けを解除します。
- このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
-----
Primary Secondary Type          Ports
-----
20      501      isolated
20      502      community
20      503      community
20      504      non-operational
```

プライベート VLAN ホストポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN ホストポートとして設定し、これをプライマリおよびセカンダリ VLAN と関連付けるには、特権 EXEC モードで次の手順を実行します。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ 3	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	switchport private-vlan host-association <i>primary_vlan_id secondary_vlan_id</i>	レイヤ 2 ポートをプライベート VLAN に関連付けます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces [<i>interface-id</i>] switchport	設定を確認します。
ステップ 7	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをプライベート VLAN ホスト ポートとして設定し、これにプライベート VLAN ペアを関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces gigabitEthernet1/2 switchport
Name: Gi1/2
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
```

<output truncated>

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ3	switchport mode private-vlan promiscuous	レイヤ 2 ポートをプライベート VLAN 無差別ポートとして設定します。
ステップ4	switchport private-vlan mapping primary_vlan_id {add remove} secondary_vlan_list	プライベート VLAN 無差別ポートを、プライマリ VLAN と選択したセカンダリ VLAN にマッピングします。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show interfaces [interface-id] switchport	設定を確認します。
ステップ7	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 インターフェイスをプライベート VLAN 無差別ポートとして設定した場合、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN をプライベート VLAN 無差別ポートにマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライベート VLAN 無差別ポートのマッピングを解除します。

次に、インターフェイスをプライベート VLAN 無差別ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。インターフェイスは、プライマリ VLAN 20 のメンバで、セカンダリ VLAN 501 ~ 503 がマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

show vlan private-vlan または **show interface status** 特権 EXEC コマンドを使用してプライマリおよびセカンダリ VLAN とスイッチ上のプライベート VLAN ポートを表示します。

セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface vlan primary_vlan_id	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して VLAN を SVI として設定します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 3 private-vlan mapping [add remove] secondary_vlan_list	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングしてプライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show interface private-vlan mapping	設定を確認します。
ステップ 6 copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。



(注) **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにだけ影響します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際、構文について次の点に留意してください。

- **secondary_vlan_list** パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。
- **secondary_vlan_list** を入力するか、または **add** キーワードを指定した **secondary_vlan_list** を使用してセカンダリ VLAN をプライマリ VLAN にマッピングします。
- **remove** キーワードを指定した **secondary_vlan_list** を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

次に、VLAN 501 および 502 のインターフェイスをプライマリ VLAN 10 にマッピングする例を示します。VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ VLAN 入力トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan10      501          isolated
vlan10      502          community
```

プライベート VLAN のモニタリング

表 19-1 プライベート VLAN モニタリング コマンド

コマンド	目的
<code>show interfaces status</code>	所属する VLAN を含む、インターフェイスのステータスを表示します。
<code>show vlan private-vlan [type]</code>	スイッチのプライベート VLAN 情報を表示します。
<code>show interface switchport</code>	インターフェイス上のプライベート VLAN 設定を表示します。
<code>show interface private-vlan mapping</code>	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、`show vlan private-vlan` コマンドの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type          Ports
-----
10      501      isolated      Gi1/1, Gi1/3
10      502      community     Gi1/5, Gi1/4
10      503      non-operational
```




CHAPTER 20

IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定

Virtual Private Network (VPN; バーチャル プライベート ネットワーク) では、多くの場合にイーサネットベースの共有インフラストラクチャである企業規模の接続に、プライベート ネットワークと同じセキュリティ、プライオリティ、信頼性、管理の容易さが提供されます。トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダー用に設計された機能です。IE 3000 スイッチは、IP サービスイメージを稼働している場合に、IEEE 802.1Q トンネリングとレイヤ 2 プロトコル トンネリングをサポートします。



(注)

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

この章で説明する内容は、次のとおりです。

- 「[IEEE 802.1Q トンネリングの概要](#)」 (P.20-1)
- 「[IEEE 802.1Q トンネリングの設定](#)」 (P.20-4)
- 「[レイヤ 2 プロトコル トンネリングの概要](#)」 (P.20-8)
- 「[レイヤ 2 プロトコル トンネリングの設定](#)」 (P.20-11)
- 「[トンネリング ステータスのモニタリングおよびメンテナンス](#)」 (P.20-18)

IEEE 802.1Q トンネリングの概要

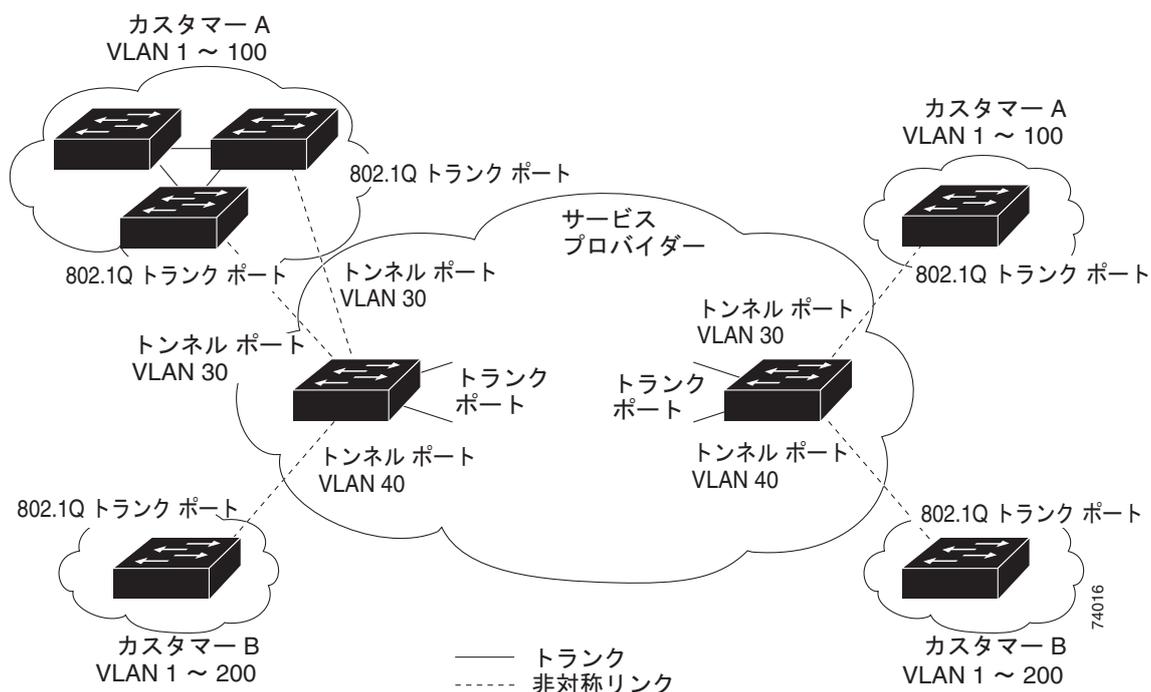
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限 (4096) を簡単に超えてしまうことがあります。

サービス プロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID は、同一 VLAN に見えるように見えても保護され、さまざまなカスタマーのトラフィックは、サービスプロバイダー ネットワーク内で区別されます。IEEE 802.1Q トンネリングを使用する場合、VLAN-in-VLAN 階層構造およびタグ付きパケットへの再タグ付けによって、VLAN スペースを拡張できます。IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネル ポートと呼ばれます。トンネリングを設定

する場合は、トンネリング専用の VLAN ID にトンネル ポートを割り当てます。それぞれのカスタマーには別個のサービスプロバイダー VLAN ID が必要ですが、その VLAN ID ではすべてのカスタマーの VLAN がサポートされます。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの IEEE 802.1Q トランク ポートからサービスプロバイダーのエッジスイッチのトンネル ポートに発信されます。カスタマー デバイスとエッジスイッチ間のリンクは、片方が IEEE 802.1Q トランク ポートとして設定され、もう一方がトンネル ポートとして設定されているので非対称です。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。図 20-1 を参照してください。

図 20-1 サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネル ポート



カスタマーのトランク ポートからサービスプロバイダーのエッジスイッチのトンネル ポートに発信されるパケットには、通常、適切な VLAN ID とともに IEEE 802.1Q タグが付いています。タグはスイッチ内でそのまま残り、タグ付きパケットがトランク ポートからサービスプロバイダー ネットワークに発信されると、カスタマーに固有の VLAN ID を含む IEEE 802.1Q タグの別のレイヤ（メトロタグと呼ばれる）でカプセル化されます。カスタマーの元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービスプロバイダー ネットワークに入るパケットには、カスタマーのアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付いています。

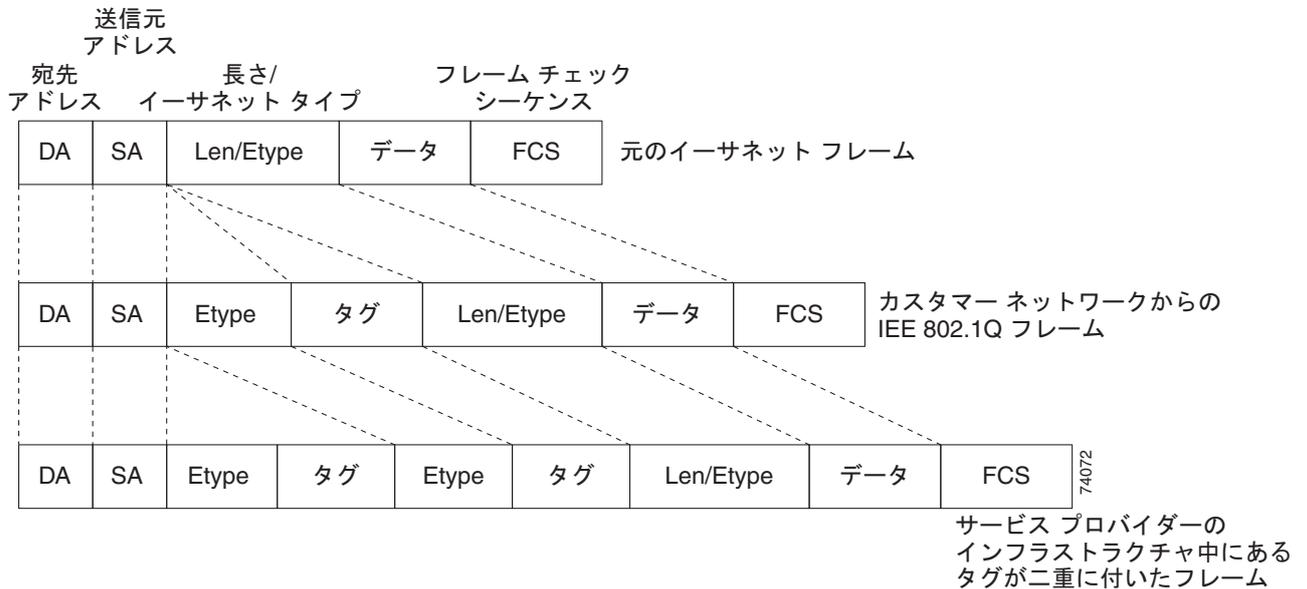
二重タグパケットがサービスプロバイダー コア スwitchの別のトランク ポートに入ると、スイッチがパケットを処理する間に外部タグが外されます。パケットが、そのコア スwitchの別のトランク ポートを出るとき、同じメトロタグがパケットに再び追加されます。図 20-2 は、二重タグパケットのタグ構造です。



(注)

カプセル化された着信パケットによってそのトランク ポートが `errdisable` に変更されたため、トランク ポートからレイヤ 2 プロトコル設定を削除します。カプセル化された発信 VTP (CDP および STP) パケットが、そのトランクからドロップされます。

図 20-2 元の（通常）イーサネット パケット、IEEE 802.1Q イーサネット パケット、二重タグ イーサネット パケットの形式



パケットがサービス プロバイダー 出カス イッチの トランク ポートに入ると、スイッチがパケットを内部処理する間に外部タグは再び外されます。ただし、パケットがエッジ スイッチのトンネル ポートからカスタマー ネットワークに送信される時、メトロ タグは追加されません。パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

図 20-1 では、カスタマー A に VLAN 30 が、カスタマー B に VLAN 40 が割り当てられています。エッジ スイッチのトンネル ポートに入る、IEEE 802.1Q タグが付いたパケットには、サービス プロバイダー ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、サービス プロバイダー ネットワーク内で区別されます。それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービス プロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

発信トンネル ポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。トンネリングおよびタグ付けを複数のレベルにすることもできますが、このリリースのスイッチでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。エッジ スイッチのトンネル ポートを通してサービス プロバイダー ネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、IEEE 802.1Q トランク ポートでサービス プロバイダー ネットワークを通じて送信される場合、メトロ タグ VLAN ID（トンネル ポートのアクセス VLAN に設定）でカプセル化されます。メトロ タグのプライオリティ フィールドは、トンネル ポートで設定されているインターフェイス サービス クラス（CoS）プライオリティに設定されます（設定されていない場合、デフォルトはゼロです）。

IEEE 802.1Q トンネリングの設定

ここでは、次の設定について説明します。

- 「IEEE 802.1Q トンネリングのデフォルト設定」(P.20-4)
- 「IEEE 802.1Q トンネリング設定時の注意事項」(P.20-4)
- 「IEEE 802.1Q トンネリングおよびその他の機能」(P.20-6)
- 「IEEE 802.1Q トンネリング ポートの設定」(P.20-6)

IEEE 802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが dynamic auto であるため、IEEE 802.1Q トンネルはディセーブルです。すべての IEEE 802.1Q トランク ポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

IEEE 802.1Q トンネリング設定時の注意事項

IEEE 802.1Q トンネリングを設定する場合は、カスタマー デバイスおよびエッジ スイッチの間で非対称リンクを常に使用する必要があります。カスタマー デバイスのポートを IEEE 802.1Q トランク ポートに、エッジ スイッチのポートをトンネル ポートとして設定してください。

トンネリングに使用する VLAN だけにトンネル ポートを割り当ててください。

ネイティブ VLAN および Maximum Transmission Unit (MTU; 最大伝送単位) の設定要件については、次の項で説明します。

ネイティブ VLAN

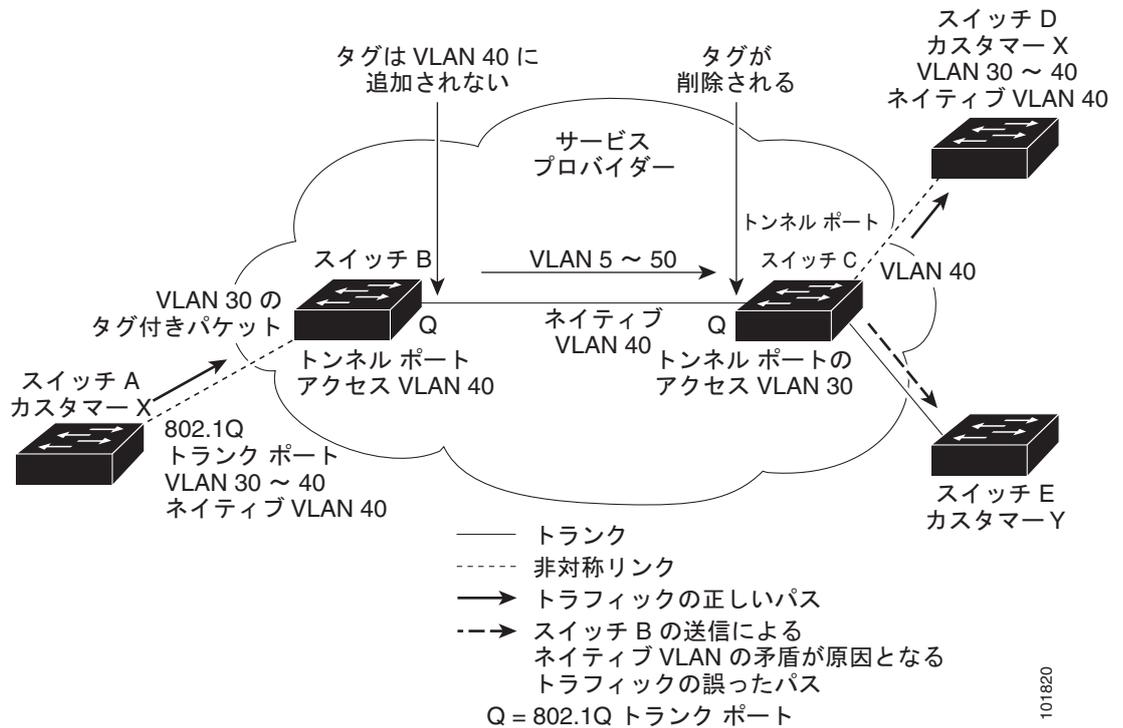
エッジ スイッチで IEEE 802.1Q トンネリングを設定する場合は、サービスプロバイダー ネットワークにパケットを送信するために、IEEE 802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、Inter Switch Link (ISL; スイッチ間リンク) トランク、非トランキング リンクのいずれかで送信できます。コア スイッチで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN を、同一スイッチの非トランキング (トンネリング) ポートのネイティブ VLAN と一致させることはできません。ネイティブ VLAN のトラフィックに、IEEE 802.1Q 送信トランク ポートでタグが付かないためです。

図 20-3 を参照してください。VLAN 40 は、サービスプロバイダー ネットワークの入力エッジ スイッチ (スイッチ B) において、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN (VLAN 40) は、エッジ スイッチのトランク ポートのネイティブ VLAN (VLAN 40) と同じなので、トンネル ポートから受信したタグ付きパケットにメトロタグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ スイッチ (スイッチ C) のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

この問題の解決方法は次のとおりです。

- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用し、ネイティブ VLAN を含む、IEEE 802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジスイッチを設定します。すべての IEEE 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。
- エッジスイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲内でないことを確認します。たとえばトランク ポートが VLAN100 ~ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

図 20-3 IEEE 802.1Q トンネリングおよびネイティブ VLAN に潜在する問題



システム MTU

スイッチのトラフィックのデフォルト システム最大伝送単位は 1500 バイトです。system mtu グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにファストイーサネットポートを設定できます。system mtu jumbo グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにギガビットイーサネットポートを設定できます。IEEE 802.1Q トンネリング機能では、メトロ タグが追加されると、フレーム サイズが 4 バイト増加するので、スイッチ システム MTU サイズを最低 1504 バイトに増加して最大フレームを処理できるように、サービスプロバイダ ネットワークのすべてのスイッチを設定する必要があります。ギガビットイーサネット インターフェイスの最大許容システム MTU は 9000 バイトです。ファストイーサネット インターフェイスの最大システム MTU は 1998 バイトです。

IEEE 802.1Q トンネリングおよびその他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。
- IEEE 802.1Q ポートを含む VLAN では IP ルーティングがサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネル ポートを含む Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) でルーティングがイネーブルである場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN でインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。
- フォールバック ブリッジングは、トンネル ポートでサポートされません。トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネル ポートが設定されている VLAN でフォールバック ブリッジングがイネーブルである場合、IP パケットは VLAN を越えて不適切にブリッジングされます。このため、トンネル ポートを含む VLAN ではフォールバック ブリッジングをイネーブルにしないでください。
- トンネル ポートでは IP Access Control List (ACL; アクセス コントロール リスト) がサポートされません。
- レイヤ 3 の Quality of Service (QoS) ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。MAC ベース QoS はトンネル ポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- ポート集約プロトコル、Link Aggregation Control Protocol (LACP)、UniDirectional Link Detection (UDLD; 単一方向リンク検出) は、IEEE 802.1Q トンネル ポートでサポートされます。
- トンネル ポートとトランク ポートで非対称リンクを手動で設定する必要があるため、Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) には IEEE 802.1Q トンネリングとの互換性がありません。
- VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネル ポートとしてポートを設定すると、スパニングツリー Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フィルタリングがインターフェイスで自動的にイネーブルになります。Cisco Discovery Protocol (CDP) および Layer Link Discovery Protocol (LLDP) は、インターフェイスで自動的にディセーブルになります。

IEEE 802.1Q トンネリング ポートの設定

IEEE 802.1Q トンネル ポートとしてポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続するサービスプロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1 ~ 48）が含まれます。
ステップ3	switchport access vlan vlan-id	デフォルト VLAN を指定します。これは、インターフェイスがトランキングを停止した場合に使用されます。この VLAN ID は特定カスタマーに固有です。
ステップ4	switchport mode dot1q-tunnel	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ6	vlan dot1q tag native	(任意) すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタグ付けをイネーブルにするようにスイッチを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。
ステップ7	end	特権 EXEC モードに戻ります。
ステップ8	show running-config show dot1q-tunnel	IEEE 802.1Q トンネリング用に設定したポートを表示します。 トンネリング モードになっているポートを表示します。
ステップ9	show vlan dot1q tag native	IEEE 802.1Q ネイティブ VLAN タグ付けステータスを表示します。
ステップ10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

dynamic desirable のデフォルト状態にポートを戻すには、**no switchport mode dot1q-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。ネイティブ VLAN パケットのタグ付けをディセーブルにするには、**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用します。

以下は、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法の例です。この設定では、ギガビット イーサネット インターフェイス 7 に接続するカスタマーの VLAN ID は、VLAN 22 になります。

```
Switch(config)# interface gigabitethernet1/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet1/7
Port
-----
Gi1/1Port

-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

レイヤ 2 プロトコル トンネリングの概要

サービスプロバイダー ネットワークを越えて接続されている、さまざまなサイトに散在するカスタマーは、さまざまなレイヤ 2 プロトコルを使用してトポロジをスケールし、すべてのリモート サイトおよびローカル サイトを含める必要があります。STP を適切に動作させる必要があります。サービスプロバイダー ネットワークを越えたローカル サイトおよびすべてのリモート サイトを含む、適切なスパンニングツリーをすべての VLAN で構築する必要があります。CDP では、隣接するシスコ デバイスをローカル サイトおよびリモート サイトから検出する必要があります。VTP では、カスタマー ネットワークのすべてのサイトで矛盾しない VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルである場合、サービスプロバイダー ネットワークの着信側のエッジスイッチでは、特殊 MAC アドレスでレイヤ 2 プロトコルパケットがカプセル化され、サービスプロバイダー ネットワークを越えて送信されます。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、VTP のレイヤ 2 Protocol Data Unit (PDU; プロトコル データ ユニット) は、サービスプロバイダー ネットワークをまたがり、サービスプロバイダー ネットワークの発信側のカスタマー スイッチに配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信され、次のような結果になります。

- それぞれのカスタマー サイトのユーザは STP を適切に実行でき、すべての VLAN では、ローカル サイトだけではなく、すべてのサイトからのパラメータに基づいて、正しいスパンニングツリーが構築されます。
- CDP では、サービスプロバイダー ネットワークによって接続されているその他のシスコ デバイスに関する情報が検出されて表示されます。
- VTP ではカスタマー ネットワーク全体で矛盾しない VLAN 設定が提供され、サービス プロバイダーを通してすべてのスイッチに伝播されます。



(注)

サードパーティベンダーとの相互運用性を提供するには、レイヤ 2 プロトコルトンネルバイパス機能を使用します。バイパスモードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。バイパスモードを実装するには、出力トランク ポートでレイヤ 2 プロトコル トンネリングをイネーブルにします。レイヤ 2 プロトコル トンネリングがトランク ポートでイネーブルの場合、カプセル化された MAC アドレスが削除されて、プロトコルパケットに通常の MAC アドレスを持つようになります。

レイヤ 2 プロトコル トンネリングは個別に使用できます。レイヤ 2 プロトコル トンネリングでは、IEEE 802.1Q トンネリングを向上させることができます。IEEE 802.1Q トンネリング ポートでプロトコル トンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは PDU が受信されず、STP、CDP、VTP を適切に実行できません。プロトコル トンネリングがイネーブルである場合、それぞれのカスタマー ネットワークのレイヤ 2 プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。IEEE 802.1Q トンネリングでサービスプロバイダー ネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。IEEE 802.1Q トンネリングを使用しない場合は、アクセス ポートでカスタマー スイッチに接続し、サービスプロバイダーのアクセス ポートでトンネリングをイネーブルにすることで、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば図 20-4 の場合、カスタマー X には同一 VLAN に 4 つのスイッチがあり、サービスプロバイダー ネットワークで接続されています。ネットワークで PDU がトンネルされない場合、ネットワークの向こう側のスイッチでは、STP、CDP、VTP を適切に実行できません。たとえば、カスタマー X のサイト 1 内のスイッチ上の VLAN に対する STP は、サイト 2 のカスタマー X のスイッチに基づくコンバージェンス パラメータを考慮せずに、サイト 1 のスイッチ上にスパンニングツリーを構築します。そのトポロジを図 20-5 に示します。

図 20-4 レイヤ 2 プロトコル トンネリング

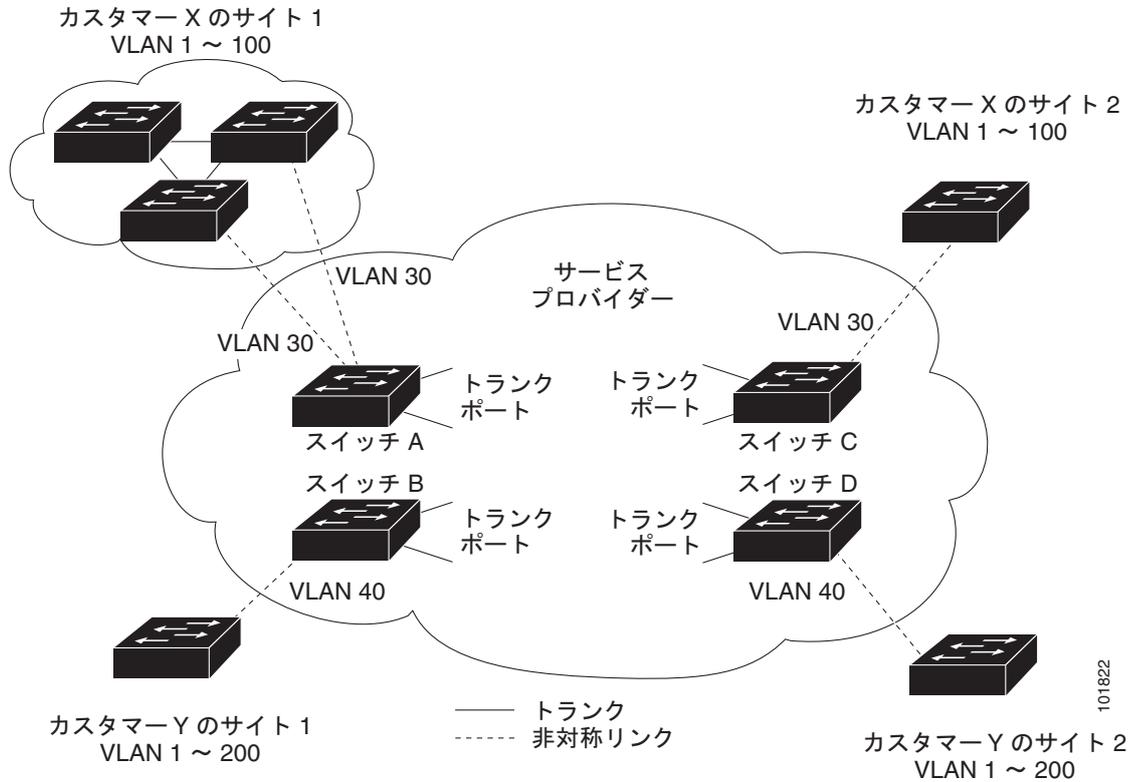
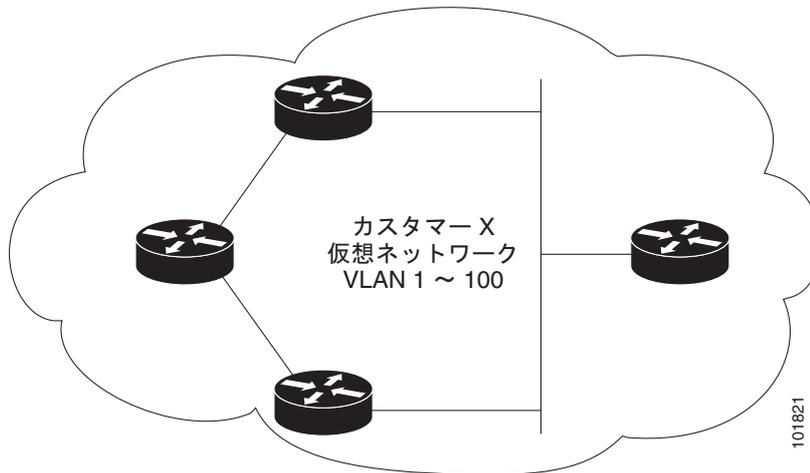


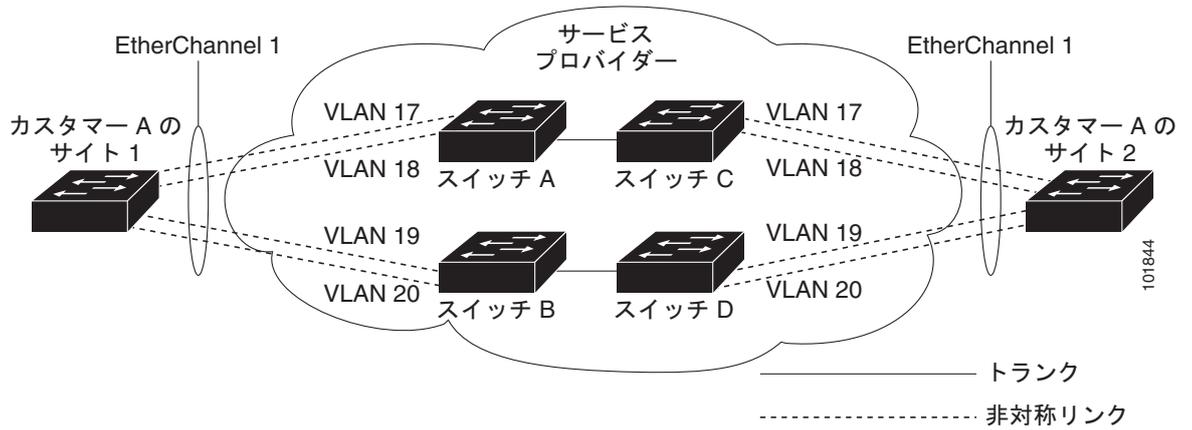
図 20-5 適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ



サービスプロバイダー ネットワークでは、レイヤ 2 プロトコル トンネリングを使用し、ポイントツーポイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を向上させることができます。サービスプロバイダー スイッチでプロトコル トンネリング (PAgP または LACP) をイネーブルにすると、リモート カスタマー スイッチでは PDU が受信され、EtherChannel の自動作成をネゴシエーションできるようになります。

たとえば図 20-6 の場合、カスタマー A には同一 VLAN に 2 つのスイッチがあり、サービス プロバイダーネットワークで接続されています。ネットワークで PDU がトンネリングされると、ネットワークの向こう側のスイッチでは、専用回線を必要とせずに、EtherChannel の自動作成をネゴシエーションできます。手順については、「EtherChannel のレイヤ 2 トンネリングの設定」(P.20-15) を参照してください。

図 20-6 EtherChannel のレイヤ 2 プロトコル トンネリング



レイヤ 2 プロトコル トンネリングの設定

サービスプロバイダー ネットワークのエッジスイッチで、カスタマーに接続されているポートにおいて、レイヤ 2 プロトコル トンネリングをプロトコルごとにイネーブルにできます。カスタマー スイッチに接続されているサービスプロバイダー エッジスイッチでは、トンネリング処理が実行されます。エッジスイッチ トンネル ポートは、カスタマーの IEEE 802.1Q トランク ポートに接続します。エッジスイッチ アクセス ポートは、カスタマー アクセス ポートに接続します。カスタマー スイッチに接続されているエッジスイッチでは、トンネリング処理が実行されます。

アクセス ポートまたはトンネル ポートのいずれかとして設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできます。switchport モードが **dynamic auto** (デフォルト モード) または **dynamic desirable** に設定されているポートでは、レイヤ 2 プロトコル トンネリングはイネーブルにできません。

スイッチでは、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングがサポートされます。ポイントツーポイント ネットワーク トポロジのエミュレートの場合は、PAgP、LACP、UDLD のプロトコルもサポートされます。スイッチは、LLDP のレイヤ 2 プロトコル トンネリングをサポートしません。



注意

PAgP、LACP、UDLD プロトコル トンネリングでは、ポイントツーポイント トポロジのエミュレートだけが目的です。設定を間違えたことによりトンネリング パケットが多く送られると、ネットワーク障害が発生する可能性があります。

レイヤ 2 プロトコルがイネーブルになっているポートでサービスプロバイダーの着信エッジスイッチに入ったレイヤ 2 PDU が、トランク ポートからサービスプロバイダー ネットワークに出る場合、スイッチでは、カスタマー PDU 宛先 MAC アドレスが、周知のシスコ固有のマルチキャストアドレス (01-00-0c-cd-cd-d0) で上書きされます。IEEE 802.1Q トンネリングがイネーブルである場合、パケットにはタグが二重に付きます。外部タグはカスタマーのメトロ タグであり、内部タグはカスタマーの VLAN タグです。コアスイッチでは内部タグが無視され、同じメトロ VLAN のすべてのトランクポートにパケットが転送されます。発信側のエッジスイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートかアクセス ポートにパケットが転送されます。このため、レイヤ 2 PDU はそのまま残り、サービスプロバイダー インフラストラクチャを越えてカスタマー ネットワークの反対側に配信されます。

[図 20-4](#) を参照してください。カスタマー X およびカスタマー Y が、それぞれアクセス VLAN 30 および 40 になっています。非対称リンクにより、サイト 1 のカスタマーは、サービスプロバイダー ネットワークのエッジスイッチに接続されています。サイト 1 のカスタマー Y からスイッチ 2 に発信されたレイヤ 2 PDU (たとえば BPDU) は、既知の MAC アドレスが宛先 MAC アドレスになっている二重タグパケットとしてインフラストラクチャに転送されます。この二重タグパケットには、40 というメトロ VLAN タグ、および VLAN 100 などの内部 VLAN タグが付いています。二重タグパケットがスイッチ D に入ると、外部 VLAN タグ 40 が外されて周知の MAC アドレスがそれぞれのレイヤ 2 プロトコル MAC アドレスで置き換わり、パケットは、VLAN 100 の 1 重タグフレームとしてサイト 2 のカスタマー Y に送信されます。

カスタマー スイッチのアクセス ポートまたはトランク ポートに接続されているエッジスイッチのアクセス ポートでも、レイヤ 2 プロトコル トンネリングをイネーブルにできます。この場合は、カプセル化プロセスとカプセル開放プロセスが、前の段落で説明したものと同じですが、パケットはサービスプロバイダー ネットワークで二重タグになりません。カスタマー固有のアクセス VLAN タグの 1 重タグになります。

ここでは、次の設定について説明します。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」(P.20-12)
- 「レイヤ 2 プロトコル トンネリング設定時の注意事項」(P.20-12)
- 「レイヤ 2 プロトコル トンネリングの設定」(P.20-13)

- 「EtherChannel のレイヤ 2 トンネリングの設定」(P.20-15)

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 20-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 20-1 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル
シャットダウンしきい値	未設定。
ドロップしきい値	未設定。
CoS 値	インターフェイスで CoS 値が設定されている場合は、その値がレイヤ 2 プロトコル トンネリングの BPDU CoS 値を設定するために使用されます。インターフェイス レベルで CoS 値が設定されていない場合は、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 になります。これはデータ トラフィックに適用されません。

レイヤ 2 プロトコル トンネリング設定時の注意事項

以下は、レイヤ 2 プロトコル トンネリングの設定時の注意事項および動作特性です。

- スイッチでは、CDP、STP (Multiple STP (MSTP) を含む)、VTP のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- スイッチでは、**switchport** モードが **dynamic auto** または **dynamic desirable** に設定されているポートにおいて、レイヤ 2 プロトコル トンネリングがサポートされません。
- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。
- サービスプロバイダー ネットワークの発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル 情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートおよびアクセス ポートにパケットが転送されます。
- サードパーティ ベンダー スイッチとの相互運用性のため、スイッチではレイヤ 2 プロトコル トンネル バイパス機能がサポートされます。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。スイッチの入力ポートでレイヤ 2 プロトコル トンネルがイネーブルである場合は、出力トランク ポートにより、トンネリングされたパケットが特殊なカプセル化で転送されます。出力トランク ポートでもレイヤ 2 プロトコル トンネリングをイネーブルにすると、この動作がバイパスされて、スイッチによって、処理や修正が行われずに制御 PDU が転送されます。
- スイッチでは、ポイントツーポイント ネットワーク トポロジのエミュレートの場合、PAgP、LACP、UDLD のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- PAgP トンネリングまたは LACP トンネリングの場合は、リンク障害検出を高速にするため、インターフェイスで UDLD もイネーブルにすることを推奨します。

- PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのレイヤ 2 プロトコル トンネリングでは、ループバック検出がサポートされません。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ 2 トンネリングがイネーブルになっているトンネル ポートまたはアクセス ポートから受信される場合、トンネル ポートは、ループを防止するためにシャットダウンされます。このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。**shutdown** コマンドに続けて **no shutdown** コマンドを入力すると、ポートを再び手動でイネーブルにできます。**errdisable recovery** がイネーブルである場合は、指定された間隔で動作が再試行されます。
- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。サービスプロバイダー ネットワーク上で動作しているスパンニングツリー インスタンスでは、BPDU がトンネル ポートに転送されません。CDP パケットはトンネル ポートから転送されません。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのシャットダウンしきい値やポートごとのシャットダウンしきい値を設定できます。制限を超えると、ポートはシャットダウンされます。QoS ACL およびポリシー マップをトンネル ポートで使用すると、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのドロップしきい値やポートごとのドロップしきい値を設定できます。制限を超えると、ポートが PDU を受信するレートがドロップしきい値未満になるまで、ポートで PDU がドロップされます。
- トンネリングされた PDU (特に STP BPDU) は、カスタマーの仮想ネットワークが正しく動作するためにすべてのリモート サイトに配信される必要があるため、同じトンネル ポートから受信されるデータ パケットよりも PDU のプライオリティをサービスプロバイダー ネットワーク内で高くできます。デフォルトの場合、PDU ではデータ パケットと同じ CoS 値が使用されます。

レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング用にポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービスプロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスは、物理インターフェイスおよびポートチャネル論理インターフェイス (ポート チャネル 1 ~ 48) です。
ステップ 3	switchport mode access または switchport mode dot1q-tunnel	アクセス ポートまたは IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 4	l2protocol-tunnel [cdp stp vtp]	目的のプロトコルのプロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのレイヤ 2 プロトコルでイネーブルになります。

	コマンド	目的
ステップ 5	l2protocol-tunnel shutdown-threshold [cdp stp vtp] value	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値の値は、ドロップしきい値の値以上とする必要があります。
ステップ 6	l2protocol-tunnel drop-threshold [cdp stp vtp] value	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットがドロップされます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値の値は、シャットダウンしきい値の値以下である必要があります。
ステップ 7	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	errdisable recovery cause l2ptguard	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。 errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 9	l2protocol-tunnel cos value	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show l2protocol	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel [cdp | stp | vtp]** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp]** コマンドおよび **no l2protocol-tunnel drop-threshold [cdp | stp | vtp]** コマンドを使用します。

以下は、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する方法の例です。

```
Switch(config)# interface fastethernet1/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa1/11	cdp	1500	1000	2288	2282	0
	stp	1500	1000	116	13	0
	vtp	1500	1000	3	67	0
	pagp	----	----	0	0	0
	lacp	----	----	0	0	0
	udld	----	----	0	0	0

EtherChannel のレイヤ 2 トンネリングの設定

レイヤ 2 ポイントツーポイント トンネリングを設定して EtherChannel の自動作成を容易にするには、サービスプロバイダー エッジ スイッチおよびカスタマー スイッチの両方を設定する必要があります。

サービスプロバイダー エッジ スイッチの設定

EtherChannel のレイヤ 2 プロトコル トンネリング用にサービスプロバイダー エッジ スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、トンネルポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービスプロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスは物理インターフェイスです。
ステップ 3	<code>switchport mode dot1q-tunnel</code>	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 4	<code>l2protocol-tunnel point-to-point [pagp lacp udld]</code>	(任意) 目的のプロトコルのポイントツーポイント プロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのプロトコルでイネーブルになります。  注意 ネットワーク障害を避けるため、ネットワークがポイントツーポイント トポロジになっていることを確認してから、PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのトンネリングをイネーブルにしてください。
ステップ 5	<code>l2protocol-tunnel shutdown-threshold [point-to-point [pagp lacp udld]] value</code>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値の値は、ドロップしきい値の値以上とする必要があります。

■ レイヤ 2 プロトコル トンネリングの設定

コマンド	目的
ステップ 6 l2protocol-tunnel drop-threshold [point-to-point [pagp lacp udld]] value	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットがドロップされます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値の値は、シャットダウンしきい値の値以下である必要があります。
ステップ 7 no cdp enable	インターフェイス上で CDP をディセーブルにします。
ステップ 8 spanning-tree bpdupfilter enable	インターフェイス上で BPDU フィルタリングをイネーブルにします。
ステップ 9 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 10 errdisable recovery cause l2ptguard	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 11 l2protocol-tunnel cos value	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 12 end	特権 EXEC モードに戻ります。
ステップ 13 show l2protocol	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 14 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel [point-to-point [pagp | lacp | udld]]** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold [point-to-point [pagp | lacp | udld]]** コマンドおよび **no l2protocol-tunnel drop-threshold [[point-to-point [pagp | lacp | udld]]** コマンドを使用します。

カスタマー スイッチの設定

サービスプロバイダー エッジ スイッチを設定したら、特権 EXEC モードで次の手順を実行し、EtherChannel のレイヤ 2 プロトコル トンネリング用にカスタマー スイッチを設定します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	インターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチ ポートにする必要があります。
ステップ 3 switchport trunk encapsulation dot1q	トランキング カプセル化形式を IEEE 802.1Q に設定します。
ステップ 4 switchport mode trunk	インターフェイス上でトランキングをイネーブルにします。
ステップ 5 udld enable	インターフェイスの通常モードで UDLD をイネーブルにします。

コマンド	目的
ステップ 6 channel-group channel-group-number mode desirable	チャンネル グループにインターフェイスを割り当て、PAgP モードに desirable を指定します。EtherChannel の設定の詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
ステップ 7 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8 interface port-channel port-channel number	ポートチャンネル インターフェイス モードを開始します。
ステップ 9 shutdown	インターフェイスをシャットダウンします。
ステップ 10 no shutdown	インターフェイスをイネーブルにします。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show l2protocol	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**no switchport mode trunk**、**no udld enable**、**no channel group channel-group-number mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel の場合は、サービスプロバイダー エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります (図 20-6 (P.20-10) を参照)。

以下は、サービス プロバイダーのエッジ スイッチ 1 およびエッジ スイッチ 2 を設定する方法の例です。VLAN 17、18、19、20 はアクセス VLAN、ファスト イーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、ドロップ しきい値は 1000、ファスト イーサネット インターフェイス 3 はトランク ポートです。

サービスプロバイダー エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

サービスプロバイダー エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
```

```
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

次は、サイト 1 のカスタマー スイッチを設定する方法の例です。ファストイーサネット インターフェイス 1、2、3、4 は IEEE 802.1Q トンネリング用に設定されており、UDLD はイネーブル、EtherChannel グループ 1 はイネーブル、ポート チャネルはシャットダウンされた後にイネーブルになり EtherChannel 設定がアクティブになります。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

トンネリング ステータスのモニタリングおよびメンテナンス

表 20-2 は、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングのモニタリングとメンテナンスを行う特権 EXEC コマンドの説明です。

表 20-2 トンネリングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>clear l2protocol-tunnel counters</code>	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
<code>show dot1q-tunnel</code>	スイッチの IEEE 802.1Q トンネル ポートを表示します。
<code>show dot1q-tunnel interface interface-id</code>	特定インターフェイスがトンネル ポートであるかどうかを確認します。
<code>show l2protocol-tunnel</code>	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。

表 20-2 トンネリングのモニタおよびメンテナンスのためのコマンド (続き)

コマンド	目的
<code>show errdisable recovery</code>	レイヤ 2 プロトコル トンネル エラー ディセーブル状態からの回復タイマーがイネーブルかどうかを確認します。
<code>show l2protocol-tunnel interface <i>interface-id</i></code>	特定レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
<code>show l2protocol-tunnel summary</code>	レイヤ 2 プロトコルのサマリー情報だけを表示します。
<code>show vlan dot1q tag native</code>	スイッチのネイティブ VLAN タグのステータスを表示します。

この表示の詳細については、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 21

STP の設定

この章では、IE3000 スイッチのポートベース VLAN でスパンニングツリー プロトコル (STP) を設定する方法について説明します。このスイッチは、IEEE 802.1D 標準に準拠した Per-VLAN Spanning-Tree plus (PVST+) とシスコ独自の拡張機能の組み合わせか、もしくは IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) プロトコルのいずれかを使用できます。

Multiple Spanning-Tree Protocol (MSTP) および複数の VLAN を同一のスパンニングツリー インスタンスにマッピングする方法については、第 22 章「MSTP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどのその他のスパンニングツリーの機能については、第 23 章「オプションのスパンニングツリー機能の設定」を参照してください。



(注)

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

この章で説明する内容は、次のとおりです。

- 「スパンニングツリー機能の概要」 (P.21-1)
- 「スパンニングツリー機能の設定」 (P.21-11)
- 「スパンニングツリー ステータスの表示」 (P.21-23)

スパンニングツリー機能の概要

ここでは、次の概要について説明します。

- 「STP の概要」 (P.21-2)
- 「スパンニングツリー トポロジと BPDU」 (P.21-3)
- 「ブリッジ ID、スイッチ プライオリティ、および拡張システム ID」 (P.21-4)
- 「スパンニングツリー インターフェイス ステート」 (P.21-4)
- 「スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み」 (P.21-7)
- 「スパンニングツリーおよび冗長接続」 (P.21-8)
- 「スパンニングツリー アドレスの管理」 (P.21-8)
- 「接続を維持するためのエイジング タイムの短縮」 (P.21-9)
- 「スパンニングツリー モードおよびプロトコル」 (P.21-9)
- 「サポートされるスパンニングツリー インスタンス」 (P.21-10)
- 「スパンニングツリーの相互運用性と下位互換性」 (P.21-10)

- 「STP および IEEE 802.1Q トランク」 (P.21-10)
- 「VLAN ブリッジ スパニングツリー」 (P.21-11)

設定の詳細については、「スパニングツリー機能の設定」 (P.21-11) を参照してください。

オプションのスパニングツリー機能については、第 23 章「オプションのスパニングツリー機能の設定」を参照してください。

STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。エンドステーション間に複数のアクティブパスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ 2 インターフェイスのエンドステーション MAC アドレスを学習する可能性があります。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリー アルゴリズムは、アクティブ トポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

冗長データ パスはスパニングツリーによって、強制的にスタンバイ（ブロックされた）状態にされます。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的に Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータ ユニット) と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。



(注)

デフォルトでは、Small Form-factor Pluggable (SFP) を搭載していないインターフェイスにだけ、スイッチがキープアライブ メッセージを（接続が有効か確認するために）送信します。[no] keepalive インターフェイス コンフィギュレーション コマンドを使用してインターフェイスのデフォルトを変更することができます。

スパンニングツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパンニングツリー トポロジは、次の要素によって制御されます。

- 各スイッチのそれぞれの VLAN に対応付けられた一意のブリッジ ID (スイッチ プライオリティおよび MAC アドレス)
- ルート スイッチに対するスパンニングツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID (ポート プライオリティおよび MAC アドレス)。

ネットワーク内のスイッチに電源が投入されると、それぞれがルート スイッチとして機能します。各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパンニングツリー トポロジが計算されます。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側スイッチがルート スイッチと見なしたスイッチの固有ブリッジ ID
- ルートに対するスパンニングツリー パス コスト
- 送信側スイッチのブリッジ ID
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および最大エージングプロトコル タイマーの値

スイッチは、*優位*の情報（より小さいブリッジ ID、より低いパス コストなど）を格納したコンフィギュレーション BPDU を受信すると、そのポートのためにこの情報を保存します。スイッチは、この BPDU をルート ポートで受信した場合は、更新されたメッセージ付きで、自身が指定スイッチであるすべての接続 LAN に対して BPDU を転送します。

そのポートに対して現在保存されているものより *下位*の情報を格納したコンフィギュレーション BPDU を受信した場合は、BPDU は廃棄されます。スイッチが、下位 BPDU の送信元の LAN の指定スイッチである場合は、そのポート用に保存された最新情報を格納した BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 台のスイッチがルート スイッチ（スイッチド ネットワークのスパンニングツリー トポロジの論理的な中心）として選択されます。
各 VLAN で、スイッチのプライオリティが最も高い（プライオリティ値が数値的に最も小さい）スイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリティ（32768）で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート スイッチになります。スイッチのプライオリティ値は、ブリッジ ID の最上位ビットを占めます（表 21-1 (P.21-4) を参照）。
- 各スイッチ（ルート スイッチを除く）に対して 1 つのルート ポートが選択されます。このポートは、スイッチによってパケットがルート スイッチに転送されるときに、最適なパス（最小コスト）を提供します。

- スイッチごとに、パス コストに基づいてルート スイッチまでの最短距離が計算されます。
- 各 LAN セグメントの指定スイッチが選定されます。指定スイッチでは、LAN からルート スイッチへのパケット転送の場合、パス コストが最小となります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

スイッチド ネットワーク上のすべての地点からルート スイッチに到達する場合に必要なパスはすべて、スパニングツリー ブロッキング モードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチに一意のブリッジ識別子（ブリッジ ID）を設定する必要があります。この ID によってルート スイッチの選択が制御されます。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のスイッチは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。スイッチ上の各 VLAN には一意の 8 バイトブリッジ ID が設定されます。上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチでは IEEE 802.1t スパニングツリー拡張機能がサポートされ、従来はスイッチ プライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。その結果、スイッチに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。表 21-1 に示すように、従来はスイッチ プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 21-1 スイッチ プライオリティ値および拡張システム ID

スイッチ プライオリティ値				拡張システム ID (VLAN ID と同設定)											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティの手動での設定方法に影響が生じます。たとえば、スイッチのプライオリティ値を変更すると、ルート スイッチとして選定される可能性も変更されることとなります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。詳細については、「ルート スイッチの設定」(P.21-15)、「セカンダリ ルート スイッチの設定」(P.21-17)、および「VLAN のスイッチ プライオリティの設定」(P.21-20) を参照してください。

スパニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジの変化が発生します。インターフェイスがスパニングツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパンニングツリーを使用しているスイッチの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

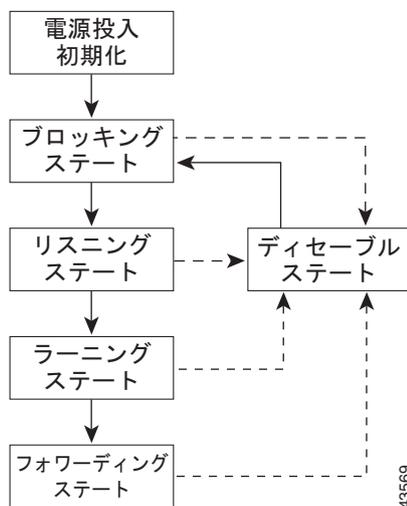
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパンニングツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパンニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパンニングツリー インスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 21-1 に、インターフェイスがステートをどのように移行するかを示します。

図 21-1 スパンニングツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパンニングツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパンニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパンニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパンニングツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。

2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートで、スイッチがデータベース転送のためにエンドステーションの位置情報を学習している間、インターフェイスはフレーム転送を引き続きブロックします。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまで、ルートとして動作します。この BPDU 交換によって、ネットワーク上のどのスイッチがルート、つまりルートスイッチであるかが確立されます。ネットワークにスイッチが 1 台しかない場合、交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはスイッチの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレームの転送やスパンニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

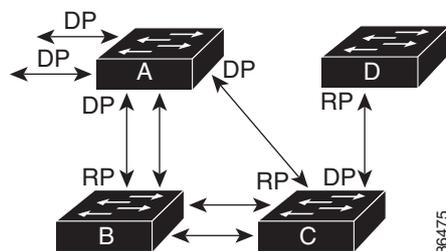
ディセーブル インターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチまたはポートがルート スイッチまたはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパンニングツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。図 21-2 では、スイッチ A がルート スイッチとして選定されます（すべてのスイッチのスイッチ プライオリティがデフォルト (32768) に設定されており、スイッチ A の MAC アドレスが最小であるため）。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパンニングツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 21-2 スパンニングツリー トポロジ



RP = ルート ポート
DP = 指定ポート

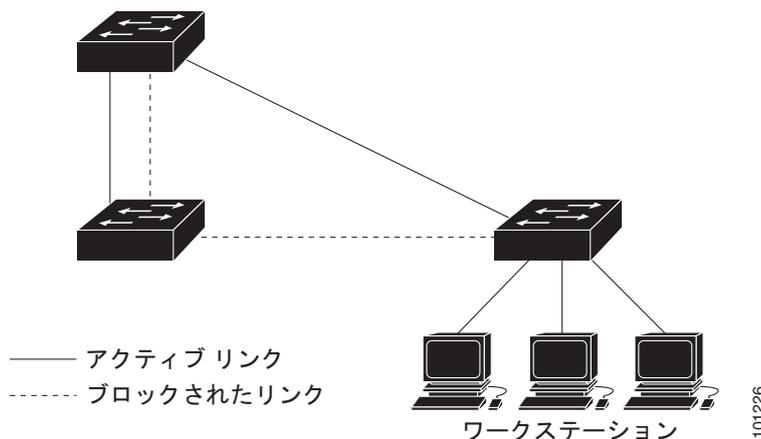
スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが重要です。

たとえば、スイッチ B のあるポートがギガビット イーサネット リンクで、別のポート (10/100 リンク) がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパニングツリー ポート プライオリティをルート ポートより高くする (数値を小さくする) と、ギガビット イーサネット ポートが新しいルート ポートになります。

スパニングツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます (図 21-3 を参照)。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート プライオリティとポート ID が加算され、値の小さいリンクがスパニングツリーによってディセーブルにされます。

図 21-3 スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ~ 0x00180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、各スイッチは 0x00180C2000000 ~ 0x00180C200000F のアドレス宛の packets を受信しますが、転送は行いません。

スパンニングツリーがイネーブルな場合、スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛のパケットを受信します。スパンニングツリーがディセーブルな場合は、スイッチは、それらのパケットを不明のマルチキャストアドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルト値です。ただし、スパンニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、アドレス テーブルからステーションアドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。スパンニングツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値 (**spanning-tree vlan vlan-id forward-time seconds** グローバル コンフィギュレーション コマンド) と同じです。

各 VLAN はそれぞれ独立したスパンニングツリー インスタンスなので、スイッチは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパンニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージング タイムがそのまま適用されます。

スパンニングツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

- **PVST+** : このスパンニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。すべてのイーサネット ポートベースの VLAN で使用されるスパンニングツリーのデフォルト モードです。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルートスイッチがあります。このルートスイッチは、その VLAN に対応するスパンニングツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の情報を持つようになるので、ネットワーク トポロジが確実に維持されます。

- **Rapid PVST+** : このスパンニングツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

Rapid PVST+ は PVST+ と同じ設定を使用している (特に明記する場合を除く)、必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行するのに、複雑な MSTP 設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパンニングツリー インスタンスを最大数実行します。

- **MSTP** : このスパンニングツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパンニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要なスパンニングツリー インスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree

Protocol (RSTP) (IEEE 802.1w 準拠) 上で実行され、転送遅延を解消し、ルートポートおよび指定ポートをフォワーディングステートにすばやく移行することにより、スパニングツリーの高速コンバージェンスを可能にします。RSTP を使用しない場合、MSTP は稼働できません。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの配備です。詳細については、第 22 章「MSTP の設定」を参照してください。

サポートされるスパニングツリー インスタンス数については、次の項を参照してください。

サポートされるスパニングツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、スイッチは最大 65 MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

スパニングツリーと VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) の相互作用については、「スパニングツリー設定時の注意事項」(P.21-12) を参照してください。

スパニングツリーの相互運用性と下位互換性

表 21-2 に、ネットワークでサポートされるスパニングツリー モード間の相互運用性と下位互換性を示します。

表 21-2 PVST+、MSTP、および Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり (制限あり)	あり (PVST+ に戻る)
MSTP	あり (制限あり)	あり	あり (PVST+ に戻る)
Rapid PVST+	あり (PVST+ に戻る)	あり (PVST+ に戻る)	あり

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree (CST) のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ が稼働しているスイッチと PVST+ が稼働しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニングツリー インスタンスにすることを推奨します。Rapid PVST+ スパニングツリー インスタンスでは、ルートスイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルートスイッチは PVST+ スイッチでなければなりません。PVST+ スイッチはネットワークのエッジに配置する必要があります。

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクによって接続された Cisco スイッチのネットワークでは、スイッチはトランク上で使用できる各 VLAN に 1 つずつ、スパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは PVST+ を使用してスパンニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパンニングツリー インスタンスと他社の IEEE 802.1Q スイッチのスパンニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありません。アクセス ポートおよびスイッチ間リンク (ISL) トランク ポートでの外部スパンニングツリーの動作は、PVST+ の影響を受けません。

IEEE 802.1Q トランクの詳細については、第 16 章「VLAN の設定」を参照してください。

VLAN ブリッジ スパンニングツリー

シスコ VLAN ブリッジ スパンニングツリーは、フォールバック ブリッジング機能 (ブリッジ グループ) で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。VLAN ブリッジ スパンニングツリーにより、ブリッジ グループは個々の VLAN スパンニングツリーの上部にスパンニングツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパンニングツリーが単一のスパンニングツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパンニングツリーをサポートするには、一部のスパンニングツリー タイマーを増やします。フォールバック ブリッジング機能を使用するには、スイッチに IP サービス イメージをインストールする必要があります。詳細については、第 52 章「フォールバック ブリッジングの設定」を参照してください。

スパンニングツリー機能の設定

ここでは、次の設定について説明します。

- 「スパンニングツリー機能のデフォルト設定」 (P.21-12)
- 「スパンニングツリー設定時の注意事項」 (P.21-12)
- 「スパンニングツリー モードの変更」 (P.21-14) (必須)
- 「スパンニングツリーのディセーブル化」 (P.21-15) (任意)
- 「ルート スイッチの設定」 (P.21-15) (任意)
- 「セカンダリ ルート スイッチの設定」 (P.21-17) (任意)
- 「ポート プライオリティの設定」 (P.21-17) (任意)
- 「パス コストの設定」 (P.21-19) (任意)
- 「VLAN のスイッチ プライオリティの設定」 (P.21-20) (任意)
- 「スパンニングツリー タイマーの設定」 (P.21-21) (任意)

スパニングツリー機能のデフォルト設定

表 21-3 に、スパニングツリー機能のデフォルト設定を示します。

表 21-3 スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル 詳細については、「サポートされるスパニングツリー インスタンス」(P.21-10) を参照してください。
スパニングツリー モード	PVST+ (Rapid PVST+ と MSTP はディセーブル)
スイッチ プライオリティ	32768
スパニングツリー ポート プライオリティ (インターフェイス単位で設定可能)	128
スパニングツリー ポート コスト (インターフェイス単位で設定可能)	1000 Mb/s : 4 100 Mb/s : 19 10 Mb/s : 100
スパニングツリー VLAN ポート プライオリティ (VLAN 単位で設定可能)	128
スパニングツリー VLAN ポート コスト (VLAN 単位で設定可能)	1000 Mb/s : 4 100 Mb/s : 19 10 Mb/s : 100
スパニングツリー タイマー	hello タイム : 2 秒 転送遅延時間 : 15 秒 最大エージング タイム : 20 秒 転送保留カウント : 6 BPDU

スパニングツリー設定時の注意事項

VTP にスパニングツリー インスタンスよりも多くの VLAN が定義されている場合、PVST+ または Rapid PVST+ をイネーブルにできるのは、スイッチ上の 128 の VLAN に限られます。残りの VLAN は、スパニングツリーがディセーブルの状態で作動します。ただし、MSTP を使用して複数の VLAN を同一のスパニングツリー インスタンスにマッピングすることが可能です。詳細については、第 22 章「MSTP の設定」を参照してください。

128 のスパニングツリー インスタンスがすでに使用されている場合、VLAN の 1 つでスパニングツリーをディセーブルにして、STP を稼働させたい別の VLAN でイネーブルにできます。no **spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して、特定の VLAN でスパニングツリーをディセーブルにし、**spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して、所定の VLAN でスパニングツリーをイネーブルにします。



注意

スパニングツリーが稼働していないスイッチは、スパニングツリー インスタンスが稼働している VLAN 上の他のスイッチがループを切断できるように、受信した BPDU を引き続き転送します。したがって、スパニングツリーは、ネットワーク上のすべてのループを切断できるように十分な数のスイッチ上で稼働している必要があります。たとえば、VLAN の各ループで少なくとも 1 台のス

スイッチがスパンニングツリーを稼働している必要があります。VLAN 内のすべてのスイッチでスパンニングツリーを稼働させる必要はありません。ただし、最小限の数のスイッチだけでスパンニングツリーが稼働している状況では、不注意なネットワーク変更によって VLAN に別のループが発生し、ブロードキャスト ストームを引き起こす可能性があります。



(注)

スイッチ上の使用可能なスパンニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメイン内にさらに別の VLAN を追加すると、そのスイッチ上にスパンニングツリーが稼働しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リストが設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパンニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパンニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。ただし、ネットワークに VLAN を追加するときより多くの作業を伴うことになるので、通常、許可リストの設定は必要ありません。

VLAN スパンニングツリー インスタンスの設定はスパンニングツリー コマンドによって制御されます。スパンニングツリー インスタンスは、VLAN にインターフェイスを割り当てるときに作成します。スパンニングツリー インスタンスは最終インターフェイスが別の VLAN に移されたときに削除されます。スパンニングツリー インスタンスの作成前に、スイッチとポートのパラメータを設定できます。設定されたパラメータは、スパンニングツリー インスタンスを作成するときに適用されます。

スイッチは、PVST+、Rapid PVST+、および MSTP をサポートしますが、アクティブにできるバージョンは常に 1 つだけです (たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります)。さまざまなスパンニングツリー モードおよび相互運用性については、「スパンニングツリーの相互運用性と下位互換性」(P.21-10) を参照してください。

UplinkFast および BackboneFast の設定時の注意事項については、「オプションのスパンニングツリー設定時の注意事項」(P.23-10) を参照してください。



注意

ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

スパニングツリー モードの変更

スイッチは、PVST+、Rapid PVST+、および MSTP の 3 つのスパニングツリー モードをサポートします。デフォルトで、スイッチは PVST+ プロトコルを使用します。

スパニングツリー モードを変更するには、特権 EXEC モードで次の手順を実行します。デフォルトモード以外のモードをイネーブルにする場合、この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mode {pvst mst rapid-pvst}</code>	スパニングツリー モードを設定します。 <ul style="list-style-type: none"> • pvst を指定して、PVST+ をイネーブルにします (デフォルト設定)。 • mst を指定して、MSTP (および RSTP) をイネーブルにします。設定手順の詳細については、第 22 章「MSTP の設定」を参照してください。 • rapid-pvst を指定して、Rapid PVST+ をイネーブルにします。
ステップ 3	<code>interface interface-id</code>	(Rapid PVST+ モードの場合のみ推奨) 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。VLAN ID の範囲は 1 ~ 4094 です。ポートチャネルの範囲は 1 ~ 6 です。
ステップ 4	<code>spanning-tree link-type point-to-point</code>	(Rapid PVST+ モードの場合のみ推奨) このポートのリンク タイプをポイントツーポイントに指定します。 このポート (ローカル ポート) をポイントツーポイントリンクでリモートポートと接続し、ローカルポートが指定ポートになると、スイッチはリモートポートとネゴシエーションし、ローカルポートをフォワーディングステートに高速変更します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>clear spanning-tree detected-protocols</code>	(Rapid PVST+ モードの場合のみ推奨) スイッチ上の任意のポートが IEEE 802.1D 準拠のレガシースイッチのポートと接続されている場合に、スイッチ全体でプロトコル移行プロセスを再開します。 このステップは、このスイッチで Rapid PVST+ が稼働していることを指定スイッチが検出する場合のオプションです。
ステップ 7	<code>show spanning-tree summary</code> および <code>show spanning-tree interface interface-id</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree mode** グローバル コンフィギュレーション コマンドを使用します。ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

スパンニングツリーのディセーブル化

スパンニングツリーはデフォルトで、VLAN 1 および「サポートされるスパンニングツリー インスタンス」(P.21-10) のスパンニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパンニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。



注意

スパンニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

VLAN 単位でスパンニングツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>no spanning-tree vlan <i>vlan-id</i></code>	<i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree vlan <i>vlan-id</i></code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スパンニングツリーを再びイネーブルにするには、`spanning-tree vlan vlan-id` グローバル コンフィギュレーション コマンドを使用します。

ルート スイッチの設定

スイッチは、スイッチ上で設定されているアクティブ VLAN ごとに 1 つずつ、個別のスパンニングツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるブリッジ ID が対応付けられます。VLAN ごとに、ブリッジ ID が最小のスイッチがその VLAN のルート スイッチになります。

特定の VLAN でスイッチがルートになるように設定するには、`spanning-tree vlan vlan-id root` グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値 (32768) からかなり小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 21-1 (P.21-4) を参照)。



(注)

ルート スイッチとして設定する必要がある値が 1 未満の場合、`spanning-tree vlan vlan-id root` グローバル コンフィギュレーション コマンドは失敗します。



(注) ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。



(注) 各スパニングツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパニングツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間の最大スイッチ ホップ カウント）を指定するには、**diameter** キーワードを指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。



(注) ルート スイッチとして設定した後で、**spanning-tree vlan vlan-id hello-time**、**spanning-tree vlan vlan-id forward-time**、および **spanning-tree vlan vlan-id max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

スイッチが特定の VLAN のルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id root primary [diameter net-diameter [hello-time seconds]]	指定された VLAN のルートになるように、スイッチを設定します。 <ul style="list-style-type: none"> vlan-id には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 (任意) diameter net-diameter には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。 (任意) hello-time seconds には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree detail	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan vlan-id root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値 (32768) から 28672 に変更されます。したがって、プライマリ ルート スイッチで障害が発生した場合に、このスイッチが指定された VLAN のルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree vlan *vlan-id* root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

スイッチが特定の VLAN のセカンダリ ルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	spanning-tree vlan <i>vlan-id</i> root secondary [<i>diameter net-diameter</i> [<i>hello-time</i> <i>seconds</i>]]	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 (任意) <i>diameter net-diameter</i> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です (任意) <i>hello-time seconds</i> には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。 プライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。「 ルート スイッチの設定 」(P.21-15) を参照してください。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show spanning-tree detail	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan *vlan-id* root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、スパンニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値 (小さい数値) を割り当て、最後に選択されるインターフェイスには低いプライオリティ値 (高い数値) を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパンニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス (port-channel <i>port-channel-number</i>) です。
ステップ 3	<code>spanning-tree port-priority priority</code>	インターフェイスにポート プライオリティを設定します。 <i>priority</i> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他すべての値は拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 4	<code>spanning-tree vlan vlan-id port-priority priority</code>	VLAN にポート プライオリティを設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>priority</i> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他すべての値は拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show spanning-tree interface interface-id</code> または <code>show spanning-tree vlan vlan-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree interface interface-id` 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能な状態にある場合に限られます。ポートがリンクアップ動作状態になっていない場合は、`show running-config interface` 特権 EXEC コマンドを使用して設定を確認できます。

デフォルトの設定値に戻す場合は、`no spanning-tree [vlan vlan-id] port-priority` インターフェイス コンフィギュレーション コマンドを使用します。スパニングツリー ポート プライオリティを使用してトランク ポートに負荷分散を設定する手順については、「[トランク ポートの負荷分散の設定](#)」(P.16-22) を参照してください。

パス コストの設定

スパニングツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコスト値が与えられている場合、スパニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス (port-channel port-channel-number) です。
ステップ3	<code>spanning-tree cost cost</code>	インターフェイスにコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <i>cost</i> の範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ4	<code>spanning-tree vlan vlan-id cost cost</code>	VLAN にコストを設定します。 ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>cost</i> の範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show spanning-tree interface interface-id</code> または <code>show spanning-tree vlan vlan-id</code>	設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree interface interface-id` 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能な状態にあるポートに限られます。ポートがリンクアップ動作状態になっていない場合は、`show running-config` 特権 EXEC コマンドを使用して設定を確認できます。

デフォルトの設定値に戻す場合は、**no spanning-tree [vlan vlan-id] cost** インターフェイス コンフィギュレーション コマンドを使用します。スパニングツリー パス コストを使用してトランク ポートに負荷分散を設定する手順については、「トランク ポートの負荷分散の設定」(P.16-22) を参照してください。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定して、スイッチがルート スイッチとして選択されるようにすることができます。



(注)

このコマンドの使用には注意してください。スイッチ プライオリティの変更には、通常は、**spanning-tree vlan vlan-id root primary** および **spanning-tree vlan vlan-id root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id priority priority	VLAN のスイッチ プライオリティを設定します。 <ul style="list-style-type: none"> vlan-id には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 priority の範囲は 0 ~ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他すべての値は拒否されます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan vlan-id priority** グローバル コンフィギュレーション コマンドを使用します。

スパンニングツリー タイマーの設定

表 21-4 で、スパンニングツリーのパフォーマンス全体を左右するタイマーについて説明します。

表 21-4 スパンニングツリー タイマー

変数	説明
hello タイマー	スイッチから他のスイッチへ hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	インターフェイスが受信したプロトコル情報をスイッチに保存させておく時間を制御します。
転送保留カウント	1 秒間停止する前に送信できる BPDU 数を制御します。

以降に設定手順を示します。

hello タイムの設定

hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を設定できます。



(注)

このコマンドの使用には注意してください。hello タイムの変更には、通常、**spanning-tree vlan *vlan-id* root primary** および **spanning-tree vlan *vlan-id* root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN の hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i>	VLAN の hello タイムを設定します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>seconds</i> に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan <i>vlan-id</i>	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan *vlan-id* hello-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i>	VLAN の転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>seconds</i> に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan <i>vlan-id</i>	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan *vlan-id* forward-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i>	VLAN の最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>seconds</i> に指定できる範囲は 6 ~ 40 です。デフォルトは 20 です。
ステップ 3	end	特権 EXEC モードに戻ります。

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

デフォルトの設定値に戻す場合は、`no spanning-tree vlan vlan-id max-age` グローバル コンフィギュレーション コマンドを使用します。

転送保留カウンタの設定

転送保留カウンタ値を変更することで、BPDU のバースト サイズを設定できます。



(注) このパラメータをより高い値に変更すると、CPU の使用率が非常に大きくなります (Rapid PVST モード時に特に顕著に変化します)。逆に、この値を低く設定すると、セッションによってはコンパージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

転送保留カウンタを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>spanning-tree transmit hold-count <i>value</i></code>	1 秒間停止する前に送信できる BPDU 数を設定します。 <i>value</i> に指定できる範囲は 1 ~ 20 です。デフォルト値は 6 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree detail</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、`no spanning-tree transmit hold-count value` グローバル コンフィギュレーション コマンドを使用します。

スパニングツリー ステータスの表示

スパニングツリー ステータスを表示するには、表 21-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 21-5 スパニングツリー ステータス表示用のコマンド

コマンド	目的
<code>show spanning-tree active</code>	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
<code>show spanning-tree detail</code>	インターフェイス情報の詳細サマリーを表示します。
<code>show spanning-tree interface <i>interface-id</i></code>	指定したインターフェイスのスパニングツリー情報を表示します。
<code>show spanning-tree summary [totals]</code>	インターフェイス ステータスのサマリーを表示します。または STP ステータス セクションのすべての行を表示します。

clear spanning-tree [**interface** *interface-id*] 特権 EXEC コマンドを使用して、スパニングツリー カウンタをクリアできます。

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER 22

MSTP の設定

この章では、IE 3000 スイッチ上に IEEE 802.1s Multiple Spanning Tree Protocol (MSTP; マルチ スパニングツリー プロトコル) のシスコ実装を設定する方法について説明します。



(注) Multiple Spanning-Tree (MST; 多重スパニングツリー) 実装は IEEE 802.1s 標準に準拠しています。

MSTP は複数の VLAN を同一のスパニングツリー インスタンスにマッピングできるようにして、多数の VLAN をサポートする場合に必要なスパニングツリー インスタンスの数を減らします。MSTP は、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを可能にします。MSTP を使用すると、1 つのインスタンス (転送パス) で障害が発生しても他のインスタンス (転送パス) は影響を受けないので、ネットワークのフォールトトレランスが向上します。MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の Rapid Spanning-Tree Protocol (RSTP) が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定 ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

RSTP と MSTP は、(オリジナル) IEEE 802.1D スパニングツリー準拠デバイス、既存のシスコ独自の Multiple Instance STP (MISTP)、および既存のシスコ Per-VLAN Spanning-Tree plus (PVST+) との下位互換性を保ちながら、スパニングツリーの動作を向上させます。PVST+ および Rapid PVST+ については、第 21 章「STP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどのその他のスパニングツリーの機能については、第 23 章「オプションのスパニングツリー機能の設定」を参照してください。



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

この章の内容は、次のとおりです。

- 「MSTP の概要」 (P.22-2)
- 「RSTP の概要」 (P.22-9)
- 「MSTP 機能の設定」 (P.22-14)
- 「MST コンフィギュレーションおよびステータスの表示」 (P.22-27)

MSTP の概要

MSTP は、高速コンバージェンスが可能な RSTP を使用し、複数の VLAN を 1 つのスパニングツリーインスタンスにまとめます。各インスタンスのスパニングツリー トポロジは、他のスパニングツリーインスタンスの影響を受けません。このアーキテクチャによって、データ トラフィックに複数の転送パスが提供され、ロード バランシングが可能になり、また多数の VLAN をサポートするのに必要なスパニングツリー インスタンスの数を減らすことができます。

ここでは、MSTP の機能について説明します。

- 「MST リージョン」 (P.22-2)
- 「IST、CIST、CST」 (P.22-2)
- 「ホップ カウント」 (P.22-5)
- 「境界ポート」 (P.22-6)
- 「IEEE 802.1s の実装」 (P.22-6)
- 「IEEE 802.1D STP との相互運用性」 (P.22-8)

設定の詳細については、「MSTP 機能の設定」 (P.22-14) を参照してください。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST コンフィギュレーションを持ち、相互接続されたスイッチの集合を MST リージョンといいます (図 22-1 (P.22-4) を参照)。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって制御されます。MST コンフィギュレーションには、リージョン名、リビジョン番号、MST の VLAN とインスタンスの割り当てマップが保存されています。スイッチにリージョンを設定するには、そのスイッチで **spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用して、MST コンフィギュレーション モードを開始します。このモードでは、**instance MST** コンフィギュレーション コマンドを使用して VLAN を MST インスタンスにマッピングし、**name MST** コンフィギュレーション コマンドを使用してリージョン名を指定し、**revision MST** コンフィギュレーション コマンドを使用してリビジョン番号を設定できます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。さらに、各メンバは、RSTP Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。インスタンスは 0 ~ 4094 の数字で識別されます。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

IST、CIST、CST

すべてのスパニングツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 種類のスパニングツリーを確立して維持します。

- Internal Spanning-Tree (IST) は、1 つの MST リージョン内で稼働するスパニングツリーです。各 MST リージョン内の MSTP は複数のスパニングツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他の MST インスタンスはすべて 1 ~ 4094 まで番号が付けられます。

IST は、BPDU を送受信する唯一のスパニングツリー インスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリー インスタンスをサポートする処理に必要な BPDU の数を大幅に減少できます。

同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ (ルート スイッチ ID、ルート パス コストなど) を持っています。デフォルトでは、すべての VLAN が IST に割り当てられています。

MST インスタンスはリージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されていても、リージョン A の MST インスタンス 1 は、リージョン B の MST インスタンス 1 から独立しています。

- **Common and Internal Spanning-Tree (CIST)** は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニングツリーを相互接続する **Common Spanning-Tree (CST)** の集合です。

1 つのリージョン内で計算されたスパニングツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリー アルゴリズムによって形成されます。

MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「[MST リージョン内の動作](#)」(P.22-3) および「[MST リージョン間の動作](#)」(P.22-4) を参照してください。



(注)

IEEE 802.1s 標準を実装すると、一部の MST 実装関連の用語が変更されます。これらの変更の要約については、[表 21-1 \(P.21-4\)](#) を参照してください。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは、[図 22-1 \(P.22-4\)](#) のように、CIST リージョナルルート (IEEE 802.1s 標準が実装される以前は *IST* マスター) になります。CIST ルートに対してリージョン内で最も低いスイッチ ID とパス コストを持つスイッチがルートになります。また、リージョンがネットワーク内に 1 つしかなければ、CIST リージョナルルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナルルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナルルートであることを主張するため、CIST ルートと CIST リージョナルルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると主張します。スイッチは、ポートに現在保存されているルート情報よりも優位の MST ルート情報 (小さいスイッチ ID、パス コストなど) を受信すると、CIST リージョナルルートとしての主張を撤回します。

初期化中、リージョン内にそれぞれが CIST リージョナルルートである多数のサブリージョンが存在する場合があります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナルルートが含まれている新しいサブリージョンに加入します。このようにして、真の CIST リージョナルルートが含まれているサブリージョン以外のサブリージョンはすべて縮小させます。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナルルートを承認する必要があります。共通の CIST リージョナルルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

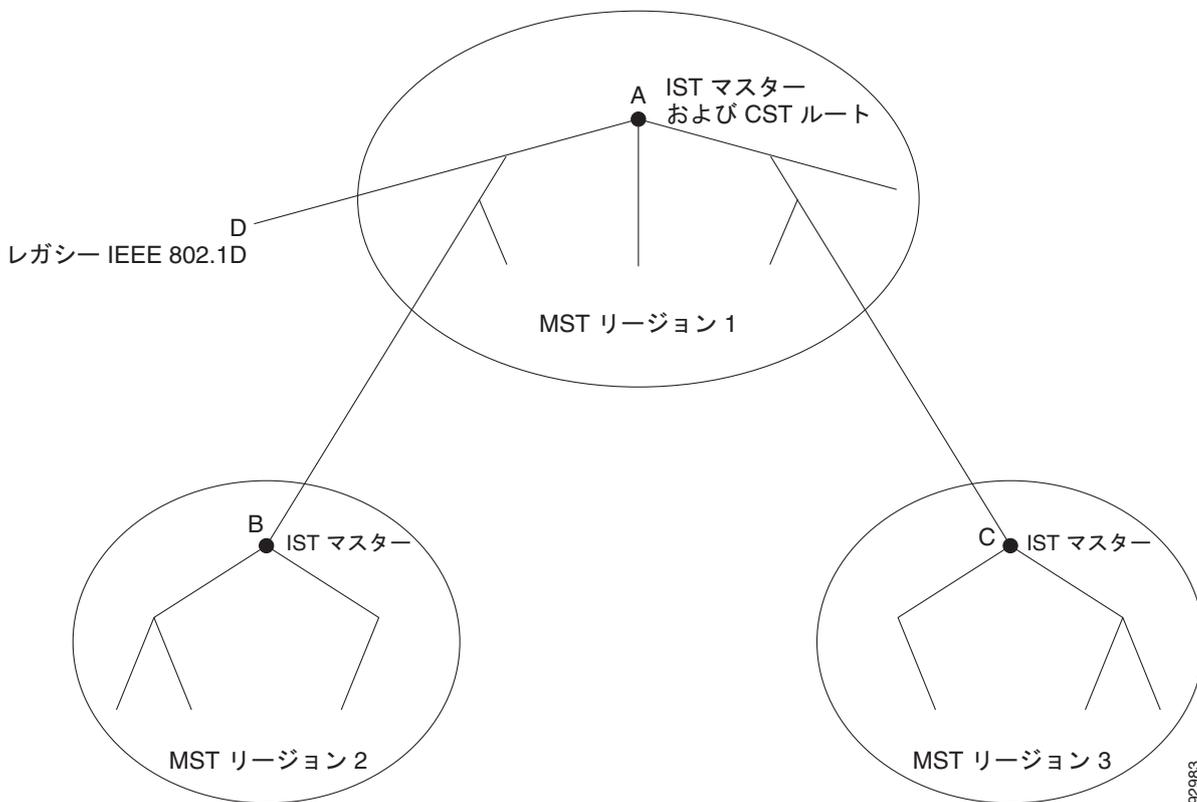
MSTP リージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシー スイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築して維持します。MST インスタンスは、リージョンの境界で IST と結合して CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチド ドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 22-1 は、3 つの MST リージョンと IEEE 802.1D 準拠のレガシー スイッチ (D) からなるネットワークを示しています。リージョン 1 の CIST リージョナル ルート (A) は、CIST ルートでもあります。リージョン 2 の CIST リージョナル ルート (B)、およびリージョン 3 の CIST リージョナル ルート (C) は、CIST 内のそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 22-1 MST リージョン、CIST マスター、および CST ルート



BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニングツリー情報を BPDU に追加して、ネイバー スイッチと通信し、最終的なスパニングツリー トポロジを計算します。そのため、BPDU 送信に関連したスパニングツリー パラメータ (たとえば hello タイム、転送時間、最大エイジング タイム、最大ホップ数など) は、CST インスタンスのみで設定されますが、すべ

での MST インスタンスに影響します。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンス と MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、IEEE 802.1D 準拠のレガシー スイッチと通信します。MSTP スイッチ同士の通信には、MSTP BPDU が使用 されます。

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョン パラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連してい る外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網 羅するスパニングツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾 子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST リージョン 内で変化しません。CIST では、MST リージョンが単一のスイッチのように見えるので注意してく ださい。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないス イッチ間を計算して出したルート パス コストです。
- CIST リージョナル ルートは先行標準の実装では IST マスターと呼ばれていました。CIST ルート がリージョン内にある場合、CIST リージョナル ルートが CIST ルートになります。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リー ジョナル ルートは IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、リージョン内の CIST リージョナル ルートまでのコストです。こ のコストは IST（インスタンス 0）のみに関係します。

表 22-1 (P.22-5) に、IEEE 標準とシスコの先行標準の用語の比較を示します。

表 22-1 先行標準の用語および標準の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST および MST インスタンスは、スパニングツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、ルートへ のパス コスト、および IP Time to Live (TTL; 存続可能時間) メカニズムに似たホップ カウント メカ ニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、 リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST イン スタンスに適用できます。ホップ カウントを設定すると、メッセージ エージング情報を設定するのと同様 の結果が得られます（再構成の開始時期を決定します）。インスタンスのルート スイッチは、常にコス トを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。この BPDU

を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エイジング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパンニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパンニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。また、境界ポートは、指定スイッチが単一のスパンニングツリー スイッチ、または異なる MST コンフィギュレーションを持つスイッチである LAN に接続されます。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートで受信可能な内部（同一リージョンからの）および外部の 2 種類のメッセージを識別します。メッセージが外部のものであれば、CIST によってのみ受信されます。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードのみを受信します。シスコ先行標準の実装では、ポートが境界ポートとして外部メッセージを受信します。つまり、ポートは内部メッセージと外部メッセージを混在させたものを受信できません。

MST リージョンには、スイッチと LAN の両方が含まれています。セグメントは、指定されたポートのリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義を利用すると、リージョン内部にある 2 つのポートのうち一方を、異なるリージョンに属するポートとしてセグメントを共有させることができます。この方法を採用すると、内部および外部の両方からポートでメッセージを受信できる場合があります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。



(注)

レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナルルート スイッチ ID フィールドが加えられたことです。一貫した送信スイッチ ID をネイバー スイッチに送信することで、リージョン全体で 1 つの仮想スイッチのように動作します。この例では、スイッチ A または B がそのセグメントで指定されているかどうかにかかわらず、スイッチ C が、ルートの一貫した送信スイッチ ID を持つ BPDU を受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステータスに必ずしも従うわけではありません。現状、次の 2 通りの事例が考えられます。

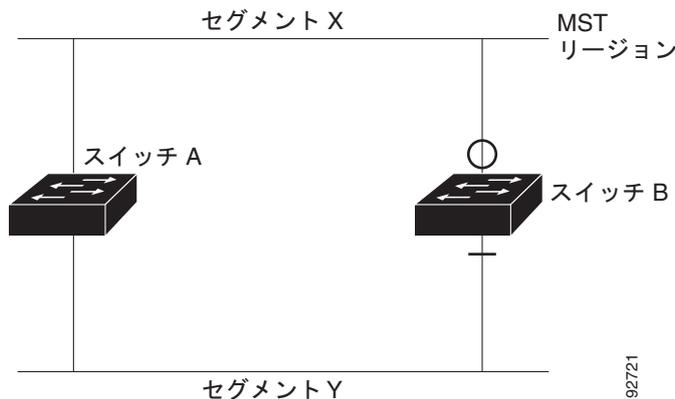
- 境界ポートが CIST リージョナルルートのルートポートである場合：CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステータスに移行できます。MSTI ポートには、特別なマスターの役割があります。
- 境界ポートが CIST リージョナルルートのルートポートでない場合：MSTI ポートは、CIST ポートのステータスと役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU (M レコード) を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシー スイッチと標準スイッチの相互運用

先行標準のスイッチでは先行標準のポートを自動検出できないため、インターフェイス コンフィギュレーション コマンドを使用して認識させます。標準と先行標準の間にあるリージョンは形成できませんが、CIST を使用することで相互運用できます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングのみです。ポートが先行標準の BPDU を受信すると、CLI (コマンドライン インターフェイス) にはポートの設定に応じて異なるフラグが表示されます。また、スイッチが、先行標準の BPDU 転送の設定がされていないポートで先行標準の BPDU を初めて受信すると、Syslog メッセージにも表示されます。

図 22-2 に、このシナリオを示します。A を標準スイッチ、B を先行標準のスイッチと仮定してください。両方とも同じリージョンに設定されています。A が CIST のルートスイッチのため、B にセグメント X のルートポート (BX) とセグメント Y の代替ポート (BY) があります。セグメント Y がフラップして、先行標準の BPDU を送信する前に BY のポートが代替ポートになった場合、AY は Y に接続している先行標準のスイッチを検出できないため、標準の BPDU を送信し続けます。また、BY ポートは境界で固定されるため、AB 間でのロード バランシングができなくなります。同一の問題はセグメント X でも発生しますが、B がトポロジの変更を転送する場合があります。

図 22-2 標準スイッチおよび先行標準のスイッチでの相互運用



(注)

標準と先行標準の MST 実装の間での干渉を少なくすることを推奨します。

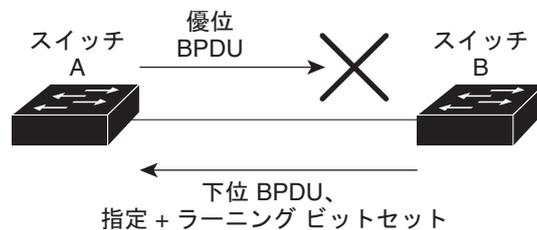
単一方向リンクの失敗の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアを使用することで、受信した BPDU からポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

指定ポートで矛盾が検出された場合、役割には従いますが、ブリッジ処理のループを引き起こすよりは、矛盾による接続中断の方が望ましい状態のため、廃棄ステートへ戻ります。

図 22-3 に、ブリッジ処理のループを引き起こす一般的な単一方向リンクの失敗例を示します。スイッチ A はルートスイッチです。スイッチ B へ向かうリンク上で、BPDU が紛失しています。RSTP と MST BPDU には、送信ポートの役割とステートが含まれています。この情報があれば、スイッチ A は、送信した優位 BPDU にスイッチ B が反応しないこと、さらにスイッチ B はルートスイッチではなく指定スイッチであることを検出できます。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。

図 22-3 単一方向リンクの失敗の検出



92722

IEEE 802.1D STP との相互運用性

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシースイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシースイッチが指定スイッチでない場合、レガシースイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再起動する（ネイバースイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシースイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、指定スイッチがシングル スパニングツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

RSTP の概要

RSTP は、ポイントツーポイントの配線を利用して、スパニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニングツリーを再構成できます (IEEE 802.1D スパニングツリーのデフォルトに設定されている 50 秒とは異なります)。

ここでは、RSTP の機能について説明します。

- 「ポートの役割およびアクティブ トポロジ」 (P.22-9)
- 「高速コンバージェンス」 (P.22-10)
- 「ポート ロールの同期」 (P.22-11)
- 「BPDU のフォーマットおよびプロセス」 (P.22-12)

設定については、「MSTP 機能の設定」 (P.22-14) を参照してください。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。「スパニングツリー トポロジと BPDU」 (P.21-3) で説明したように、RSTP は、IEEE 802.1D STP に基づき、スイッチ プライオリティが最も高い (プライオリティの値が最も小さい) スイッチをルート スイッチに選択します。RSTP はさらに、各ポートに次のいずれか 1 つの役割を割り当てます。

- ルート ポート：スイッチからルート スイッチへパケットを転送する場合の最適パス (最も低コストなパス) を提供します。
- 指定ポート：指定スイッチに接続します。これにより、LAN からルート スイッチへパケットを転送するときのパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。
- バックアップ ポート：指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクによってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。
- ディセーブル ポート：スパニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートの役割を割り当てられたポートは、アクティブ トポロジの一部となります。代替ポートまたはバックアップ ポートの役割を割り当てられたポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルートポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップポートが必ず廃棄ステート（IEEE 802.1D のブロッキング ステートと同じ）になるように保証します。フォワーディング プロセスおよびラーニング プロセスの動作はポート ステートによって制御されます。表 22-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 22-2 ポートステートの比較

動作ステータス	STP ポートステート (IEEE 802.1D)	RSTP ポートステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	No
イネーブル	リスニング	廃棄	No
イネーブル	ラーニング	ラーニング	Yes
イネーブル	フォワーディング	フォワーディング	Yes
ディセーブル	ディセーブル	廃棄	No

シスコの STP 実装製品内で整合性を図るため、このマニュアルでは、ポートの廃棄ステートをブロッキングと定義しています。指定ポートは、リスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチポート、または LAN に障害が発生しても、ただちに接続を回復できます。RSTP は、エッジポート、新しいルートポート、およびポイントツーポイントリンクで接続されているポートに次のような高速コンバージェンスを提供します。

- エッジポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、RSTP スイッチ上の 1 つのポートをエッジポートに設定すると、そのエッジポートはただちにフォワーディング ステートになります。エッジポートは PortFast 対応ポートと同じで、これをイネーブルにできるのは、単一のエンドステーションに接続されているポート上だけです。
- ルートポート：RSTP は、新しいルートポートを選択すると、古いルートポートをブロックして、新しいルートポートをただちにフォワーディング ステートにします。
- ポイントツーポイントリンク：2 つのポートをポイントツーポイントリンクで接続し、ローカルポートが指定ポートになると、その指定ポートは、提案/合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します。

図 22-4 では、スイッチ A とスイッチ B はポイントツーポイントリンクを通じて接続され、すべてのポートがブロッキングステートになっています。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

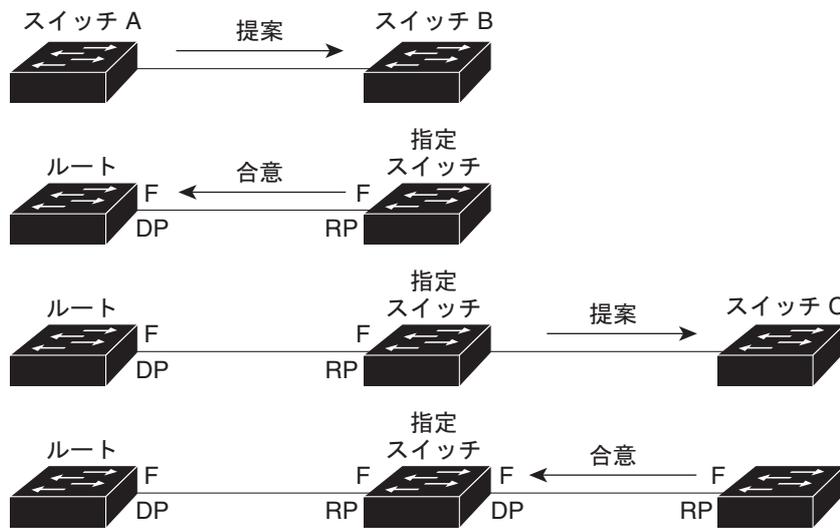
スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルートポートとして選択し、すべての非エッジポートをブロッキングステートにします。さらに、新しいルートポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディングステートにします。スイッチ B はその非エッジポートをすべてブロックし、またスイッチ A とスイッチ B はポイントツーポイントリンクで接続されているので、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイク メッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはただちにフォワーディング ステートに移行します。アクティブ トポロジにスイッチが追加されるたびに、このハンドシェイク プロセスが実行されます。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパンニング ツリーのリーフへと進みます。

スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定で制御されたデフォルトの設定値を上書きできます。

図 22-4 高速コンバージェンスの提案と合意のハンドシェイク



DP = 指定ポート
 RP = ルート ポート
 F = フォワーディング

88760

ポート ロールの同期

スイッチのポートの 1 つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

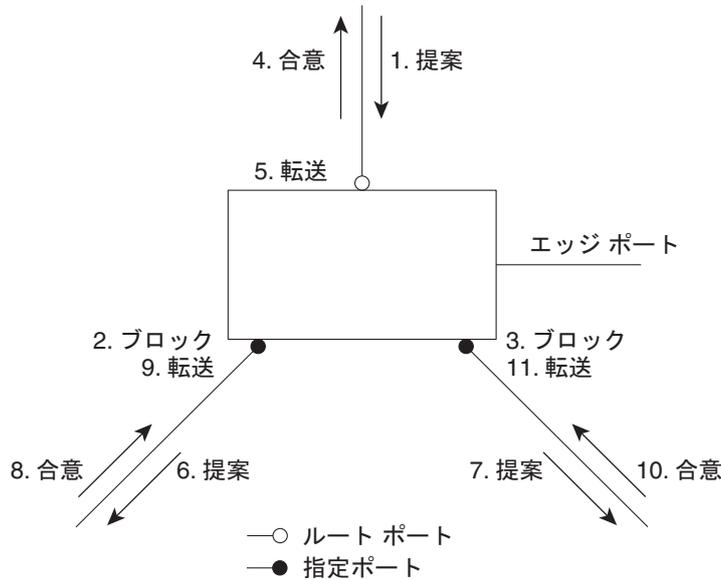
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。スイッチ上の個々のポートは次の場合に同期化された状態となります。

- ブロッキング ステートである場合
- エッジ ポートである場合 (ネットワークのエッジとして設定されているポート)

指定ポートがフォワーディング ステートであり、なおかつエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報で強制的に同期化されると、その指定ポートはブロッキング ステートになります。一般的に、RSTP がポートを新しいルート情報で強制的に同期化する場合に、そのポートが上記のいずれの条件も満たしていない場合、ポートのステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルートポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイントリンクで接続されたスイッチがポートの役割について互いに合意すると、RSTP はポートステートをただちにフォワーディングステートに移行させます。この一連のイベントを図 22-5 に示します。

図 22-5 高速コンバージェンス中のイベントのシーケンス



8876

BPDU のフォーマットおよびプロセス

RSTP BPDU のフォーマットは、プロトコルバージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。表 22-3 に、RSTP のフラグフィールドを示します。

表 22-3 RSTP BPDU フラグ

ビット	機能
0	トポロジの変更 (TC)
1	提案
2 ~ 3	ポートの役割:
00	Unknown
01	代替ポート
10	ルートポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジの変更の確認 (TCA)

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージでは、ポートの役割は常に指定ポートに設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージでは、ポートの役割は常にルートポートに設定されます。

RSTP には個別の Topology Change Notification (TCN; トポロジ変更通知) BPDU はありません。トポロジの変更を示すには、トポロジ変更 (TC) フラグが使用されます。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニングとフォワーディングのフラグは、送信ポートのステートに応じて設定されます。

優位 BPDU 情報の処理

現在保存されているルート情報よりも優位のルート情報 (小さいスイッチ ID、低パスコストなど) をポートが受信すると、RSTP は再構成を開始します。そのポートが新しいルートポートとして提案され、選択されると、RSTP は他のすべてのポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化した後、合意メッセージを送信します。BPDU が IEEE 802.1D BPDU である場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルートポートはフォワーディングステートに移行するために 2 倍の転送遅延時間を必要とします。

ポートで優位の情報が受信されたために、そのポートがバックアップポートまたは代替ポートになる場合、RSTP はそのポートをブロッキングステートに設定し、合意メッセージは送信しません。指定ポートは、転送遅延タイマーが満了するまで提案フラグの設定された BPDU の送信を続けます。タイマーが満了すると、ポートはフォワーディングステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割フラグが設定された下位 BPDU (そのポートに現在保存されている値より大きいスイッチ ID、高いパスコストなど) を指定ポートが受信した場合、その指定ポートは、ただちに現在の自身の情報を応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出: IEEE 802.1D ではブロッキングとフォワーディングステート間でのすべての移行によってトポロジの変更が生じますが、RSTP ではトポロジの変更が生じるのは、ブロッキングからフォワーディングにステートが移行する場合のみです (トポロジの変更と見なされるのは、相互接続性が向上する場合だけです)。エッジポートでステートが変更されても、トポロジの変更は生じません。RSTP スイッチは、トポロジの変更を検出すると、そのスイッチのすべての非エッジポート (TC 通知を受信したポートを除く) で学習した情報を削除します。
- 通知: IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

- **確認** : RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルートポートで TC 時間タイマー (IEEE 802.1D のトポロジ変更タイマーと同じ) がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。RSTP BPDU では、TCA ビットは設定されません。

- **伝播** : RSTP スイッチは、指定ポートまたはルートポートを介して別のスイッチから TC メッセージを受信すると、自身のすべての非エッジポート、指定ポート、およびルートポート (この TC メッセージを受信したポートを除く) に変更を伝播します。スイッチは、これらのすべてのポートの TC 時間タイマーを起動し、これらのポート上で学習した情報を削除します。
- **プロトコルの移行** : IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

ポートが初期化されると、移行遅延タイマーが起動され (RSTP BPDU を送信する最小時間を指定)、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコルタイプを無視します。

スイッチはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用を開始されます。

MSTP 機能の設定

ここでは、次の設定について説明します。

- 「MSTP のデフォルト設定」 (P.22-15)
- 「MSTP 設定時の注意事項」 (P.22-15)
- 「MST リージョンの設定および MSTP のイネーブル化」 (P.22-16) (必須)
- 「ルートスイッチの設定」 (P.22-18) (任意)
- 「セカンダリ ルートスイッチの設定」 (P.22-19) (任意)
- 「ポートプライオリティの設定」 (P.22-20) (任意)
- 「パスコストの設定」 (P.22-21) (任意)
- 「スイッチのプライオリティの設定」 (P.22-22) (任意)
- 「hello タイムの設定」 (P.22-23) (任意)
- 「転送遅延時間の設定」 (P.22-24) (任意)
- 「最大経過時間の設定」 (P.22-24) (任意)
- 「最大ホップカウントの設定」 (P.22-25) (任意)
- 「リンクタイプの指定による高速移行の保証」 (P.22-25) (任意)
- 「ネイバータイプの指定」 (P.22-26) (任意)
- 「プロトコル移行プロセスの再起動」 (P.22-26) (任意)

MSTP のデフォルト設定

表 22-4 に、MSTP のデフォルト設定を示します。

表 22-4 MSTP のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	PVST+ (Rapid PVST+ と MSTP はディセーブル)
スイッチ プライオリティ (CIST ポート単位で設定可能)	32768
スパニングツリー ポート プライオリティ (CIST ポート単位で設定可能)	128
スパニングツリー ポート コスト (CIST ポート単位で設定可能)	1000 Mbps : 4 100 Mbps : 19 10 Mbps : 100
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

サポートされるスパニングツリー インスタンス数については、「サポートされるスパニングツリー インスタンス」(P.21-10) を参照してください。

MSTP 設定時の注意事項

ここでは、MSTP の設定時の注意事項を説明します。

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- 2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/ インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです (たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります)。詳細については、「スパニングツリーの相互運用性と下位互換性」(P.21-10) を参照してください。推奨するトランク ポート設定の詳細については、「他の機能との相互作用」(P.16-18) を参照してください。
- MST コンフィギュレーションの VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) 伝播機能はサポートされません。ただし、コマンドライン インターフェイス (CLI) または SNMP (簡易ネットワーク管理プロトコル) サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション (リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング) を手動で設定することは可能です。

- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンス マッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。
- PVST+ クラウドと MST クラウドの間、または rapid-PVST+ クラウドと MST クラウドの間でロード バランシングを実現するには、すべての MST 境界ポートがフォワーディング ステートでなければなりません。そのためには、MST クラウドの IST マスターが CST のルートを兼ねている必要があります。MST クラウドが複数の MST リージョンで構成されている場合は、MST リージョンの 1 つに CST ルートが含まれており、他のすべての MST リージョンにおいて、MST クラウドに含まれているルートへのパスの方が PVST+ または rapid-PVST+ クラウド経由のパスよりも優れている必要があります。クラウド内のスイッチを手動で設定しなければならない場合もあります。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- UplinkFast および BackboneFast の設定時の注意事項については、「[オプションのスパニングツリー設定時の注意事項](#)」(P.23-10) を参照してください。

MST リージョンの設定および MSTP のイネーブル化

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバで構成されます。リージョンの各メンバは RSTP BPDU を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニングツリー インスタンスの数は 65 までです。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

MST リージョンの設定を行い、MSTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst configuration</code>	MST コンフィギュレーション モードを開始します。
ステップ 3	<code>instance instance-id vlan vlan-range</code>	<p>VLAN を MST インスタンスに対応付けます。</p> <ul style="list-style-type: none"> <code>instance-id</code> に指定できる範囲は、0 ~ 4094 です。 <code>vlan vlan-range</code> に指定できる範囲は、1 ~ 4094 です。 <p>MST インスタンスに VLAN をマッピングする場合、マッピングはインクリメンタルに行われ、コマンドで指定された VLAN がすでにマッピング済みの VLAN に対して追加または削除されます。</p> <p>VLAN の範囲を指定する場合は、ハイフンを使用します。たとえば、<code>instance 1 vlan 1-63</code> と入力すると、VLAN 1 ~ 63 が MST インスタンス 1 にマッピングされます。</p> <p>一連の VLAN を指定する場合は、カンマを使用します。たとえば、<code>instance 1 vlan 10, 20, 30</code> と入力すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。</p>

	コマンド	目的
ステップ 4	name <i>name</i>	コンフィギュレーション名を指定します。 <i>name</i> ストリングには最大 32 文字使用でき、大文字と小文字が区別されます。
ステップ 5	revision <i>version</i>	コンフィギュレーション リビジョン番号を指定します。指定できる範囲は 0 ~ 65535 です
ステップ 6	show pending	入力した設定を表示して、確認します。
ステップ 7	exit	変更を適用し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	spanning-tree mode mst	MSTP をイネーブルにします。RSTP もイネーブルになります。  注意 スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show running-config	設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの MST リージョン コンフィギュレーションに戻すには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。VLAN インスタンス マッピングをデフォルトの設定に戻すには、**no instance instance-id [vlan vlan-range] MST** コンフィギュレーション コマンドを使用します。デフォルトの名前に戻すには、**no name MST** コンフィギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、**no revision MST** コンフィギュレーション コマンドを使用し、PVST+ をイネーブルに戻すには、**no spanning-tree mode** または **spanning-tree mode pvst** グローバル コンフィギュレーション コマンドを使用します。

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ~ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、コンフィギュレーション リビジョンを 1 に設定します。その後、変更確認前の設定を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----  -----
0         1-9,21-4094
1         10-20
-----

Switch(config-mst)# exit
Switch(config)#
```

ルート スイッチの設定

スイッチは、スパンニングツリー インスタンスを VLAN グループとマッピングして維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるスイッチ ID が対応付けられます。最小のスイッチ ID を持つスイッチがその VLAN グループのルート スイッチになります。

特定のスイッチがルートになるように設定するには、**spanning-tree mst instance-id root** グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値 (32768) からきわめて小さい値に変更します。これにより、そのスイッチが指定されたスパンニングツリー インスタンスのルート スイッチになることができます。このコマンドを入力すると、スイッチは、ルート スイッチのスイッチ プライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定されたインスタンスについて、自身のプライオリティを 24576 に設定します (この値によって、このスイッチが指定されたスパンニングツリー インスタンスのルートになる場合)。

指定されたインスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です。表 21-1 (P.21-4) を参照)。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

各スパンニングツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパンニングツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径 (つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ カウント) を指定するには、**diameter** キーワードを指定します (MST インスタンス 0 の場合のみ使用可)。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きすることができます。



(注)

スイッチをルート スイッチとして設定した後に、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

スイッチをルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>spanning-tree mst instance-id root primary</code> <code>[diameter net-diameter [hello-time seconds]]</code>	スイッチをルート スイッチに設定します。 <ul style="list-style-type: none"> • <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です • (任意) <i>diameter net-diameter</i> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。 • (任意) <i>hello-time seconds</i> には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 秒です。デフォルトは 2 秒です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst instance-id root` グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリティはデフォルト値 (32768) から 28672 に変更されます。その結果、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが、指定されたインスタンスのルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。`spanning-tree mst instance-id root primary` グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

スイッチをセカンダリ ルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst instance-id root secondary [diameter net-diameter [hello-time seconds]]</code>	<p>スイッチをセカンダリ ルート スイッチに設定します。</p> <ul style="list-style-type: none"> <code>instance-id</code> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です (任意) <code>diameter net-diameter</code> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。このキーワードは、MST インスタンス 0 にだけ使用できます。 (任意) <code>hello-time seconds</code> には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 秒です。デフォルトは 2 秒です。 <p>プライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。「ルート スイッチの設定」(P.22-18) を参照してください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst instance-id root` グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値 (小さい数値) を割り当て、最後に選択されるインターフェイスには低いプライオリティ値 (高い数値) を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスの MSTP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	<p>設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。ポート チャネルの範囲は 1 ~ 6 です。</p>

	コマンド	目的
ステップ3	<code>spanning-tree mst instance-id port-priority priority</code>	<p>ポート プライオリティを設定します。</p> <ul style="list-style-type: none"> <code>instance-id</code> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です <code>priority</code> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルトは 128 です。値が小さいほど、プライオリティが高くなります。 <p>プライオリティ値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。その他すべての値は拒否されます。</p>
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show spanning-tree mst interface interface-id</code> または <code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree mst interface interface-id` 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。ポートがリンクアップ動作状態になっていない場合は、`show running-config interface` 特権 EXEC コマンドを使用して設定を確認できます。

インターフェイスをデフォルト設定に戻すには、`no spanning-tree mst instance-id port-priority` インターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスの MSTP コストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。ポート チャネルの範囲は 1 ~ 6 です。

	コマンド	目的
ステップ 3	<code>spanning-tree mst instance-id cost cost</code>	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <ul style="list-style-type: none"> <code>instance-id</code> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です <code>cost</code> の範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree mst interface interface-id</code> または <code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree mst interface interface-id` 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。ポートがリンクアップ動作状態になっていない場合は、`show running-config` 特権 EXEC コマンドを使用して設定を確認できます。

インターフェイスをデフォルト設定に戻すには、`no spanning-tree mst instance-id cost` インターフェイス コンフィギュレーション コマンドを使用します。

スイッチのプライオリティの設定

スイッチ プライオリティを設定して、スイッチがルート スイッチとして選択されるようにすることができます。



(注) このコマンドの使用には注意してください。スイッチ プライオリティの変更には、通常は、`spanning-tree vlan vlan-id root primary` および `spanning-tree vlan vlan-id root secondary` グローバル コンフィギュレーション コマンドを使用することを推奨します。

スイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>spanning-tree mst instance-id priority priority</code>	<p>スイッチ プライオリティを設定します。</p> <ul style="list-style-type: none"> <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です <i>priority</i> の範囲は 0 ~ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルート スイッチとして選択される可能性が高くなります。 <p>プライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他すべての値は拒否されます。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst instance-id priority` グローバル コンフィギュレーション コマンドを使用します。

hello タイムの設定

hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を設定できます。

すべての MST インスタンスの hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>spanning-tree mst hello-time seconds</code>	<p>すべての MST インスタンスの hello タイムを設定します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。</p> <p><i>seconds</i> に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst hello-time** グローバル コンフィギュレーション コマンドを使用します。

転送遅延時間の設定

すべての MST インスタンスの転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst forward-time seconds	すべての MST インスタンスの転送遅延時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 <i>seconds</i> に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用します。

最大経過時間の設定

すべての MST インスタンスの最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst max-age seconds	すべての MST インスタンスの最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 <i>seconds</i> に指定できる範囲は 6 ~ 40 です。デフォルトは 20 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用します。

最大ホップ カウントの設定

すべての MST インスタンスの最大ホップ カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>spanning-tree mst max-hops hop-count</code>	BPDU が廃棄され、ポートに維持されていた情報が期限切れになるまでの、リージョン内でのホップ カウントを指定します。 <i>hop-count</i> に指定できる範囲は 1 ~ 255 です。デフォルト値は 20 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst max-hops` グローバル コンフィギュレーション コマンドを使用します。

リンク タイプの指定による高速移行の保証

2つのポートをポイントツーポイント リンクで接続し、ローカル ポートが指定ポートになると、RSTP は提案/合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します（「[高速コンバージェンス](#)」(P.22-10)を参照）。

デフォルトでは、リンク タイプは、インターフェイスのデュプレックス モードによって制御されます。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。MSTP が稼働しているリモートスイッチ上の1つのポートと物理的にポイントツーポイントで接続されている半二重リンクが存在する場合は、リンク タイプのデフォルト設定値を変更して、フォワーディング ステートへの高速移行をイネーブルにできます。

リンク タイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範囲は 1 ~ 4094 です。ポート チャネルの範囲は 1 ~ 6 です。
ステップ3	<code>spanning-tree link-type point-to-point</code>	ポートのリンク タイプをポイントツーポイントに指定します。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show spanning-tree mst interface interface-id</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、`no spanning-tree link-type` インターフェイス コンフィギュレーション コマンドを使用します。

ネイバー タイプの指定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトでは、ポートは自動的に先行標準のデバイスを検出します。ただし、ポート自体は、標準と先行標準の BPDU を両方受信できます。デバイスとネイバーの間に不一致があれば、CIST のみがインターフェイス上で動作します。

ポートを選択して、先行標準の BPDU のみ送信するように設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての `show` コマンドで表示されます。

リンク タイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	<code>spanning-tree mst pre-standard</code>	先行標準の BPDU のみ送信するようにポートを指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree mst interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、`no spanning-tree mst prestandard` インターフェイス コンフィギュレーション コマンドを使用します。

プロトコル移行プロセスの再起動

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU (プロトコルバージョンが 0 に設定されている BPDU) を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MST BPDU (バージョン 3)、または RST BPDU (バージョン 2) を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシー スイッチが指定スイッチでない場合、レガシー スイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

スイッチでプロトコル移行プロセスを再起動する (ネイバー スイッチとの再ネゴシエーションを強制する) には、`clear spanning-tree detected-protocols` 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再開するには、`clear spanning-tree detected-protocols interface interface-id` 特権 EXEC コマンドを使用します。

MST コンフィギュレーションおよびステータスの表示

スパニングツリー ステータスを表示するには、表 22-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 22-5 MST ステータスを表示するコマンド

コマンド	目的
<code>show spanning-tree mst configuration</code>	MST リージョンの設定を表示します。
<code>show spanning-tree mst configuration digest</code>	現在の MSTCI に含まれている Message Digest 5 (MD5) ダイジェストを表示します。
<code>show spanning-tree mst <i>instance-id</i></code>	指定したインスタンスの MST 情報を表示します。
<code>show spanning-tree mst interface <i>interface-id</i></code>	指定したインターフェイスの MST 情報を表示します。

`show spanning-tree` 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 23

オプションのスパニングツリー機能の設定

この章では、IE 3000 スイッチでオプションのスパニングツリー機能を設定する方法について説明します。スイッチが Per-VLAN Spanning-Tree Plus (PVST+) を実行している場合、これらのすべての機能を設定できます。スイッチが Multiple Spanning-Tree Protocol (MSTP) または Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルを稼働している場合は、明記した機能だけを設定できます。

PVST+ および Rapid PVST+ の詳細については、[第 21 章「STP の設定」](#)を参照してください。MSTP の詳細および複数の VLAN を同一スパニングツリー インスタンスにマッピングする方法については、[第 22 章「MSTP の設定」](#)を参照してください。



(注)

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

この章の内容は、次のとおりです。

- 「オプションのスパニングツリー機能の概要」 (P.23-1)
- 「オプションのスパニングツリー機能の設定」 (P.23-9)
- 「スパニングツリー ステータスの表示」 (P.23-17)

オプションのスパニングツリー機能の概要

ここでは、次の概要について説明します。

- 「PortFast の概要」 (P.23-2)
- 「BPDU ガードの概要」 (P.23-2)
- 「BPDU フィルタリングの概要」 (P.23-3)
- 「UplinkFast の概要」 (P.23-3)
- 「BackboneFast の概要」 (P.23-5)
- 「EtherChannel ガードの概要」 (P.23-7)
- 「ルート ガードの概要」 (P.23-8)
- 「ループ ガードの概要」 (P.23-9)

PortFast の概要

PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。単一のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます (図 23-1 を参照)。

1 台のワークステーションまたはサーバに接続されたインターフェイスが Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) を受信しないようにする必要があります。スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニングツリーステータスの遷移をたどります。

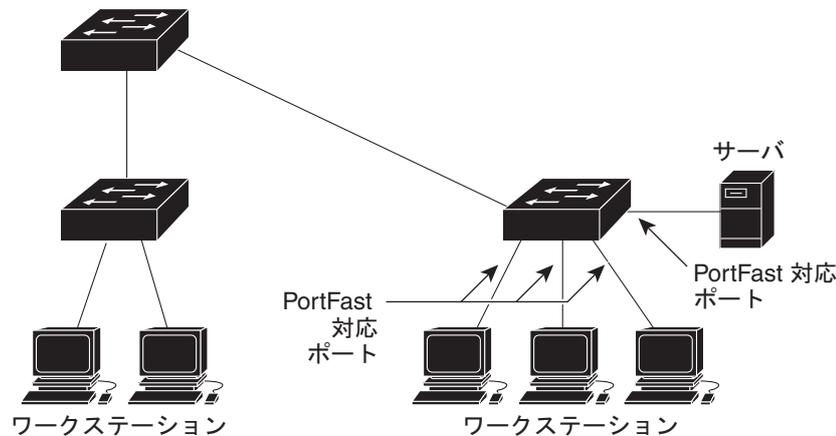


(注)

PortFast の目的は、インターフェイスがスパニングツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はエンドステーションに接続されたインターフェイス上で使用する場合にのみ有効です。他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニングツリーのループが生じるおそれがあります。

この機能をイネーブルにするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンド、または **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。

図 23-1 PortFast 対応インターフェイス



101225

BPDU ガードの概要

BPDU ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応ポート上で BPDU ガードをイネーブルにできます。これらのポート上で BPDU が受信されると、スパニングツリーは、PortFast で動作しているポートをシャットダウンします。設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは **errdisable** ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

インターフェイス レベルの場合は、PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポート上で BPDU ガードをイネーブルにできます。BPDU を受信したポートは、**errdisable** ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU フィルタリングの概要

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpdupfilter default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応インターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを使用すると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

インターフェイス レベルの場合は、PortFast 機能をイネーブルにしなくても、**spanning-tree bpdupfilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。



注意

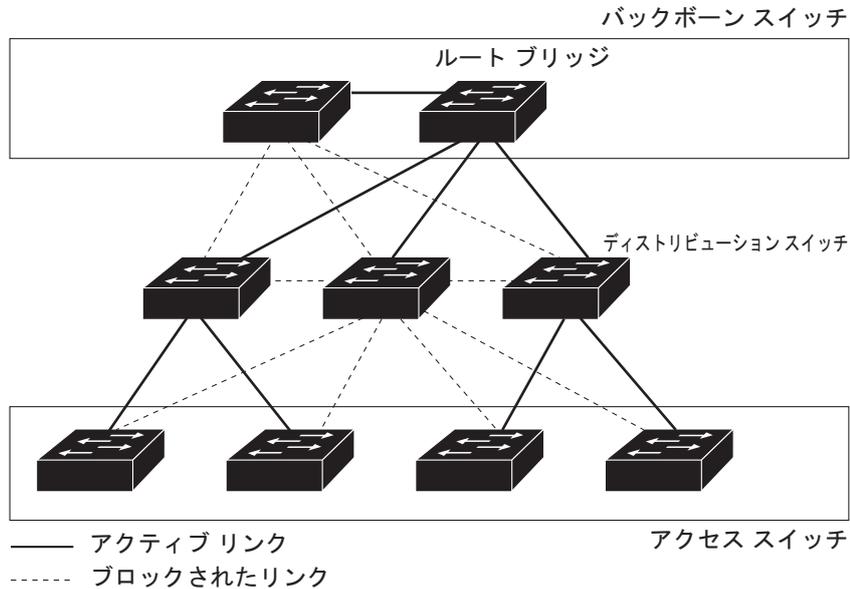
BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

UplinkFast の概要

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。図 23-2 に、ディストリビューション スイッチおよびアクセス スイッチに少なくとも 1 つの冗長リンクが確保されている複雑なネットワークの例を示します。冗長リンクは、ループを防止するために、スパニングツリーによってブロックされています。

図 23-2 階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルートポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーが再設定された場合は、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して UplinkFast をイネーブルにすることにより、新しいルートポートを短時間で選択できます。ルートポートは、通常のスパニングツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニングツリーが新規ルートポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます (このパラメータはデフォルトで毎秒 150 パケットです)。ただし、0 を入力すると、ステーション学習フレームが生成されないため、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。



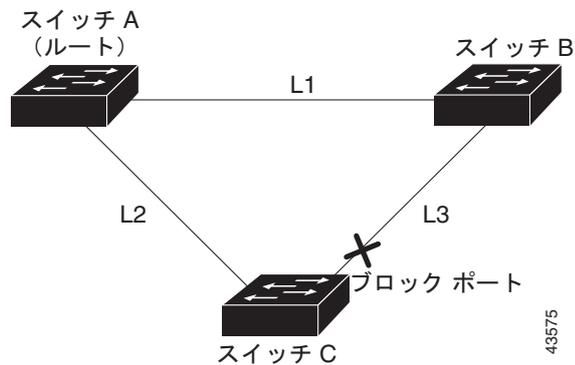
(注)

UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、(VLAN ごとの) レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。具体的には、アップリンク グループは (転送を行う) ルートポートと 1 組のブロックポートからなります (セルフ ループポートは除く)。アップリンク グループは、転送中のリンクで障害が発生した場合に、代替パスを提供します。

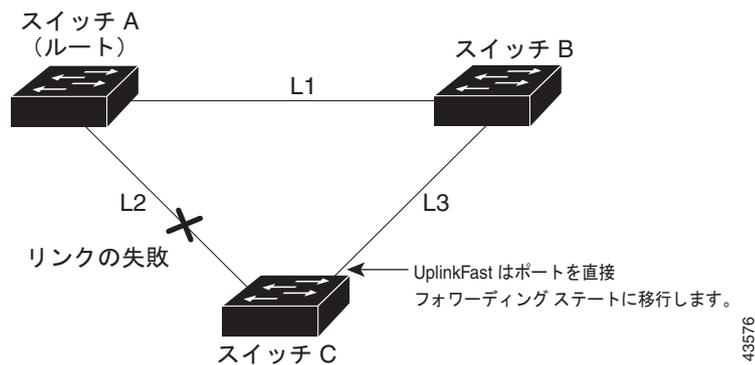
図 23-3 に、リンク障害が発生していないトポロジの例を示します。ルートスイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 23-3 直接リンク障害発生前の UplinkFast の例



C が、ルートポートの現在アクティブリンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング状態およびラーニング状態を経由せずに、直接フォワーディング状態に移行させます（図 23-4 を参照）。この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 23-4 直接リンク障害発生後の UplinkFast の例



BackboneFast の概要

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセススイッチに直接接続されたリンクの障害に対応します。BackboneFast は、最大エージングタイマーを最適化します。最大エージングタイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDU は他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパスを見つけようとします。

BackboneFast をイネーブルにするには、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。スイッチ上のルートポートまたはブロックインターフェイスが指定スイッチから下位 BPDU を受信すると、BackboneFast が開始します。下位 BPDU は、ルートブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルートスイッチ間の接続が切断されています）。スパニングツリーのルールとして、**spanning-tree vlan vlan-id max-age** グローバル コンフィギュレーション コマンドによって設定された最大エージングタイムの間、スイッチは下位 BPDU を無視します。

スイッチは、ルートスイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルートポートおよび他のブロック インターフェイスがルートスイッチへの代替パスになります（セルフループポートは、ルートスイッチへの代替パスとは見なされません）。下位 BPDU がルートポートに到達した場合、すべてのブロック インターフェイスがルートスイッチへの代替パスになります。下位 BPDU がルートポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージングタイムが経過するまで待ち、通常のスパニングツリールールに従ってルートスイッチになります。

スイッチが代替パスでルートスイッチに到達できる場合、スイッチはその代替パスを使用して、**Root Link Query (RLQ)** 要求を送信します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネットワーク内の他のスイッチからの RLQ 応答を待機します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージングタイムが経過するまで待ちます。ルートスイッチへのすべての代替パスが、スイッチとルートスイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージングタイムを満了させます。1 つまたは複数の代替パスからルートスイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 23-5 に、リンク障害が発生していないトポロジの例を示します。ルートスイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 23-5 間接リンク障害発生前の BackboneFast の例

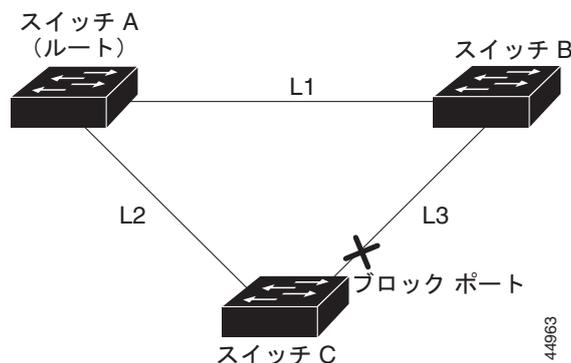


図 23-6 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、その障害を検出できません。一方スイッチ B は、L1 によってルートスイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージングタイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。図 23-6 では、リンク L1 で障害が発生した場合 BackboneFast がどのようにトポロジを再構成するかを示します。

図 23-6 間接リンク障害発生後の BackboneFast の例

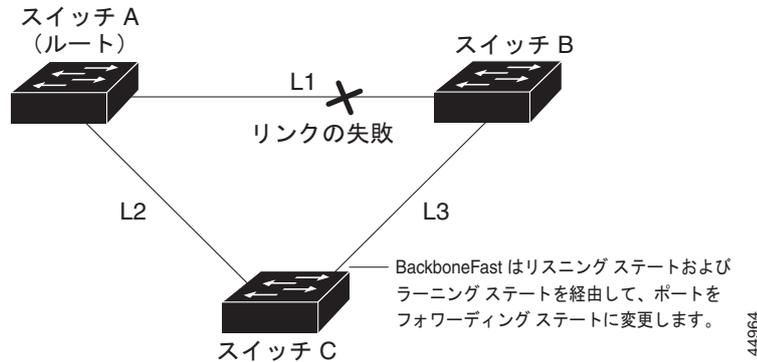
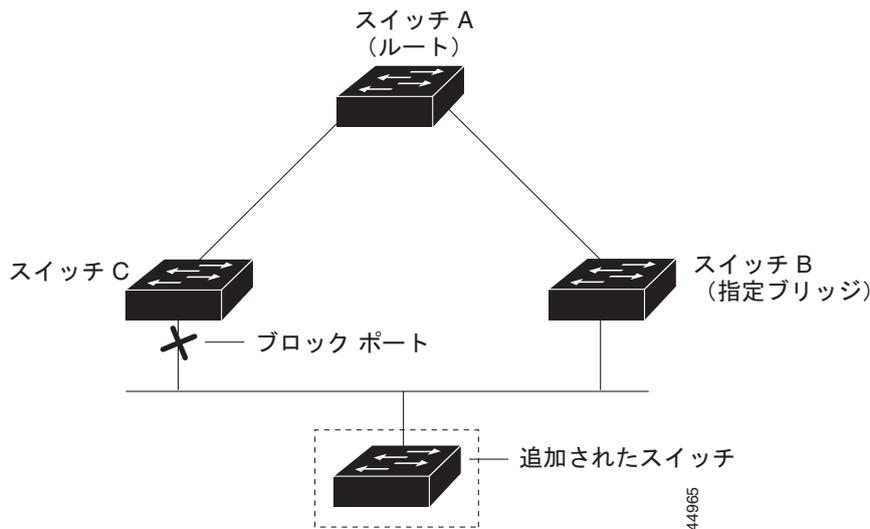


図 23-7 のように、新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルートスイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルートスイッチであるスイッチ A への指定スイッチであることを学習します。

図 23-7 メディア共有型トポロジにおけるスイッチの追加



EtherChannel ガードの概要

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。EtherChannel 設定時の注意事項については、「EtherChannel 設定時の注意事項」(P.40-10) を参照してください。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

spanning-tree etherchannel guard misconfig グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

ルート ガードの概要

Service Provider (SP; サービス プロバイダー) のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります (図 23-8)。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを **root-inconsistent** (ブロック) ステートにして、カスタマーのスイッチがルート スイッチにならないように、またはルートへのパスに組み込まれないようにします。

SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ (**root-inconsistent** ステートになり)、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはなく、ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって **Internal Spanning-Tree (IST)** インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが **IEEE 802.1D** スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。

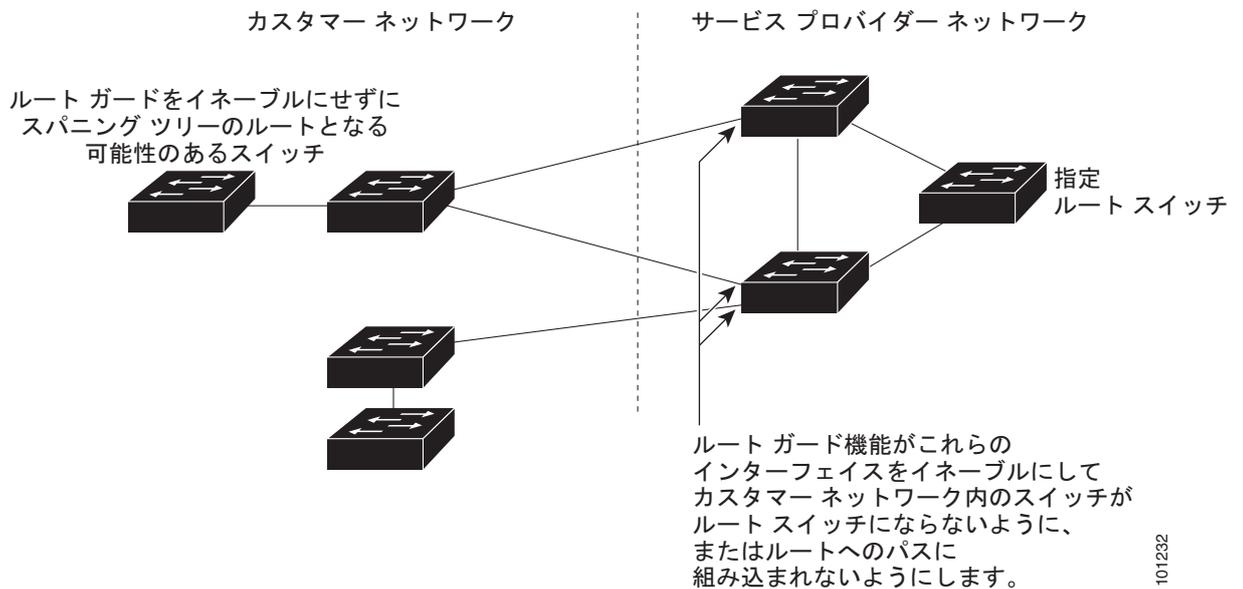
spanning-tree guard root インターフェイス コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。



注意

ルート ガード機能は使い方を誤ると、接続が切断されることがあります。

図 23-8 サービス プロバイダー ネットワークのルート ガード



101232

ループ ガードの概要

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体でイネーブルにした場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニングツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合にのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

オプションのスパニングツリー機能の設定

ここでは、次の設定について説明します。

- 「オプションのスパニングツリー機能のデフォルト設定」 (P.23-10)
- 「オプションのスパニングツリー設定時の注意事項」 (P.23-10)
- 「PortFast のイネーブル化」 (P.23-10) (任意)
- 「BPDU ガードのイネーブル化」 (P.23-11) (任意)
- 「BPDU フィルタリングのイネーブル化」 (P.23-12) (任意)
- 「冗長リンク用 UplinkFast のイネーブル化」 (P.23-14) (任意)

- 「BackboneFast のイネーブル化」(P.23-14) (任意)
- 「EtherChannel ガードのイネーブル化」(P.23-15) (任意)
- 「ルート ガードのイネーブル化」(P.23-16) (任意)
- 「ループ ガードのイネーブル化」(P.23-16) (任意)

オプションのスパニングツリー機能のデフォルト設定

表 23-1 に、オプションのスパニングツリー機能のデフォルト設定を示します。

表 23-1 オプションのスパニングツリー機能のデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル (インターフェイス単位で個別に設定する場合を除く)
UplinkFast	グローバルにディセーブル
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル
ルート ガード	すべてのインターフェイスでディセーブル
ループ ガード	すべてのインターフェイスでディセーブル

オプションのスパニングツリー設定時の注意事項

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、PortFast、BPDU ガード、BPDU フィルタリング、EtherChannel ガード、ルート ガード、またはループ ガードを設定できます。

Rapid PVST+ または MSTP 用に、UplinkFast または BackboneFast 機能を設定できます。ただし、スパニングツリー モードを PVST+ に変更するまで、この機能はディセーブル (非アクティブ) のままです。

PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行されます。



注意

PortFast を使用するのには、単一エンドステーションをアクセスポートまたはトランクポートに接続する場合に限定してください。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニングツリーがネットワークループを検出または阻止できなくなり、その結果、ブロードキャストストームおよびアドレスラーニングの障害が起きる可能性があります。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。詳細については、[第 18 章「音声 VLAN の設定」](#)を参照してください。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできません。

PortFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>spanning-tree portfast [trunk]</code>	<p>単一ワークステーションまたはサーバに接続されたアクセスポート上で PortFast をイネーブルにします。trunk キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。</p> <p>(注) トランク ポートで PortFast をイネーブルにするには、spanning-tree portfast trunk インターフェイス コンフィギュレーション コマンドを使用する必要があります。spanning-tree portfast コマンドは、トランク ポート上では機能しないためです。</p> <p> 注意 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。</p> <p>デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree interface interface-id portfast</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

PortFast 機能をディセーブルにするには、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU ガードのイネーブル化

PortFast 対応ポート (PortFast 動作ステートのポート) で BPDU ガードをグローバルにイネーブルにすると、スパニングツリーは、そのポートでの動作を継続します。そのポートは、BPDU を受信しなければ起動したままになります。

設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは `errdisable` ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

手動でポートを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。



注意

PortFast は、エンド ステーションに接続するポートに限って設定します。そうしないと、偶発的なトポロジループが原因でデータ パケット ループが発生し、スイッチおよびネットワークの動作が妨げられるおそれがあります。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、**errdisable** ステートになります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

BPDU ガード機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree portfast bpduguard default	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 3	interface interface-id	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BPDU ガードをディセーブルにするには、**no spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU フィルタリングのイネーブル化

PortFast 対応インターフェイスで BPDU フィルタリングをグローバルにイネーブルにすると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないよう

にするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。


注意

PortFast は、エンドステーションに接続するインターフェイスに限って設定します。そうしないと、予期しないトポロジループが原因でデータの packets ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpdudfilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。


注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

BPDU フィルタリング機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	spanning-tree portfast bpdudfilter default	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ3	interface interface-id	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BPDU フィルタリングをディセーブルにするには、**no spanning-tree portfast bpdudfilter default** グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpdudfilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdudfilter enable** インターフェイス コンフィギュレーション コマンドを使用します。

冗長リンク用 UplinkFast のイネーブル化

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan *vlan-id* priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。



(注) UplinkFast をイネーブルにすると、スイッチのすべての VLAN に影響します。個々の VLAN に UplinkFast を設定することはできません。

Rapid PVST+ または MSTP 用に、UplinkFast 機能を設定できます。ただし、スパニングツリー モードを PVST+ に変更するまで、この機能はディセーブル (非アクティブ) のままです。

UplinkFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree uplinkfast [max-update-rate <i>pkts-per-second</i>]	UplinkFast をイネーブルにします。 (任意) <i>pkts-per-second</i> に指定できる範囲は毎秒 0 ~ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないため、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上の値に変更した場合、パス コストは変更されません)。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

アップデート パケット レートをデフォルトの設定値に戻す場合は、**no spanning-tree uplinkfast max-update-rate** グローバル コンフィギュレーション コマンドを使用します。UplinkFast をディセーブルにする場合は、**no spanning-tree uplinkfast** コマンドを使用します。

BackboneFast のイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。



(注) BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルにする必要があります。BackboneFast は、トークンリング VLAN 上ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

Rapid PVST+ または MSTP 用に、BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

BackboneFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree backbonefast	BackboneFast をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BackboneFast 機能をディセーブルにするには、**no spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

EtherChannel ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree etherchannel guard misconfig	EtherChannel ガードをイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel ガード機能をディセーブルにするには、**no spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているスイッチ ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。



(注) ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできません。

インターフェイス上でルート ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree guard root	インターフェイスでルート ガードをイネーブルに設定します。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート ガードをディセーブルにするには、**no spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。

ループ ガードのイネーブル化

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。



(注) ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできません。

ループ ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>show spanning-tree active</code> または <code>show spanning-tree mst</code>	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。
ステップ2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>spanning-tree loopguard default</code>	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ループ ガードをグローバルにディセーブルにするには、`no spanning-tree loopguard default` グローバル コンフィギュレーション コマンドを使用します。`no spanning-tree loopguard default` グローバル コンフィギュレーション コマンドの設定を上書きするには、`spanning-tree guard loop` インターフェイス コンフィギュレーション コマンドを使用します。

スパニングツリー ステータスの表示

スパニングツリー ステータスを表示するには、表 23-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-2 スパニングツリー ステータスを表示するためのコマンド

コマンド	目的
<code>show spanning-tree active</code>	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
<code>show spanning-tree detail</code>	インターフェイス情報の詳細サマリーを表示します。
<code>show spanning-tree interface interface-id</code>	指定したインターフェイスのスパニングツリー情報を表示します。
<code>show spanning-tree mst interface interface-id</code>	指定したインターフェイスの MST 情報を表示します。
<code>show spanning-tree summary [totals]</code>	インターフェイス ステートのサマリーを表示します。またはスパニングツリー ステート セクションのすべての行を表示します。

`clear spanning-tree [interface interface-id]` 特権 EXEC コマンドを使用して、スパニングツリー カウンタをクリアできます。

`show spanning-tree` 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンドリファレンスを参照してください。

■ スパニングツリー ステータスの表示



CHAPTER 24

Resilient Ethernet Protocol の設定

この章では、IE 3000 スイッチで Resilient Ethernet Protocol (REP) を使用する方法について説明します。REP はシスコ独自のプロトコルで、スパニングツリー プロトコル (STP) に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジンググループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

この章で説明する内容は、次のとおりです。

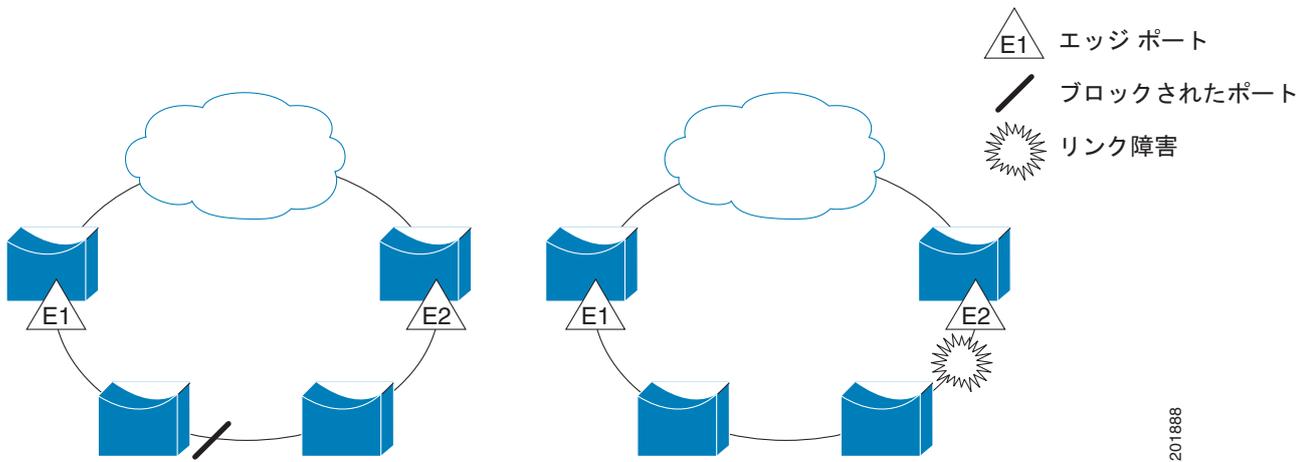
- 「REP の概要」 (P.24-1)
- 「REP の設定」 (P.24-6)
- 「REP のモニタ」 (P.24-15)

REP の概要

1 REP セグメントは、相互接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準 (非エッジ) セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは 2 つまでで、各セグメント ポートにある外部ネイバーは 1 つだけです。セグメントは共有メディアを通過できますが、どのリンクであっても同じセグメントに属することができるのは 2 ポートだけです。REP は、レイヤ 2 トランク インターフェイスだけでサポートされます。

図 24-1 に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。(左側のセグメントのように) すべてのポートが動作可能な場合、斜線で表しているように単一ポートがブロックされます。右側の図のようにネットワークに障害が発生すると、ブロックされたポートがフォワーディング ステートに復帰して、ネットワークの中断を最小限にします。

図 24-1 REP オープン セグメント

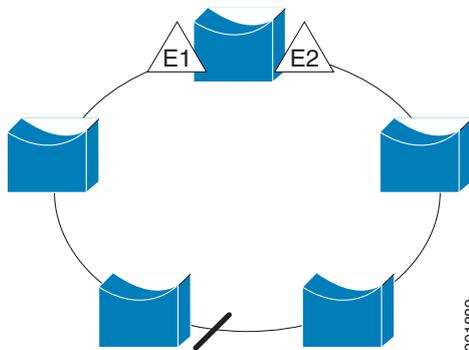


201888

図 24-1 に示されたセグメントは、オープン セグメントで、2 つのエッジ ポート間は接続されていません。REP セグメントは、ブリッジング グループとなる可能性がなく、セグメント エッジが安全に任意のネットワークに接続されます。セグメント内のスイッチに接続されているすべてのホストには、エッジポートを通じて残りのネットワークに接続する方法が 2 つありますが、いつでもアクセス可能なのは 1 つだけです。障害により、ホストが通常のゲートウェイにアクセスできない場合、REP がすべてのポートのブロックを解除して、他のゲートウェイを通じた接続を確保します。

図 24-2 で示しているセグメントは、両方のエッジ ポートが同じスイッチ内にあるリング セグメントです。この設定では、セグメントを通じてエッジ ポートと接続します。この設定を使用すると、セグメント内の任意の 2 スイッチ間で冗長接続を形成することができます。

図 24-2 REP リング セグメント



201889

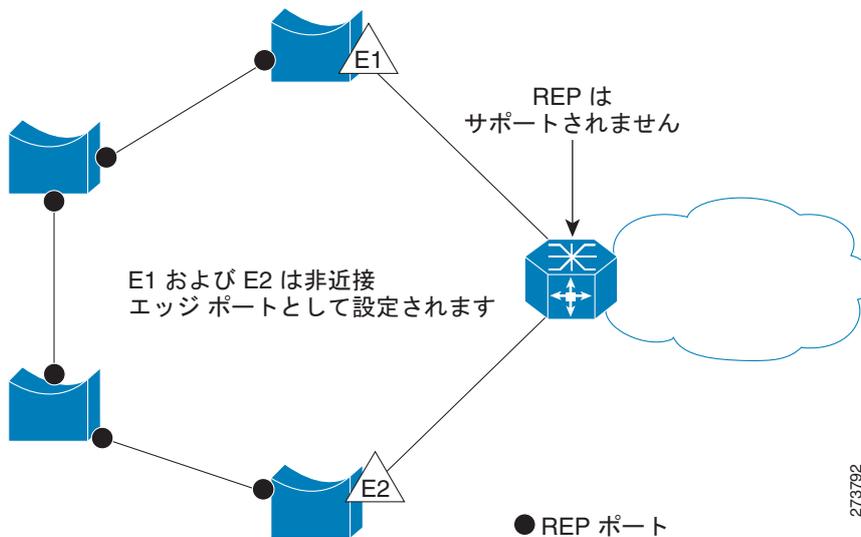
REP セグメントには次のような特徴があります。

- セグメント内の全ポートが動作可能な場合、1 ポート（代替ポートと呼ばれる）が各 VLAN でブロック ステートとなります。VLAN ロード バランシングが設定されている場合は、セグメント内の 2 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えながら論理的にブロックされるポートが VLAN ごとに選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。また REP は、プライマリ エッジ ポートで制御されているが、セグメント内の任意のポートで発生する、VLAN ロード バランシングをサポートしています。

アクセス リング トポロジでは、ネイバー スイッチで REP がサポートされていない場合があります (図 24-3 を参照)。この場合、そのスイッチ側のポート (E1 と E2) を非ネイバー エッジ ポートとして設定できます。これらのポートは、エッジ ポートのすべての特性を継承するため、他のエッジ ポートと同じように設定できます。たとえば、STP や REP のトポロジ変更通知を集約スイッチに送信するように設定することもできます。その場合、送信される STP トポロジ変更通知 (TCN) は、マルチ スパニング ツリー (MST) STP メッセージになります。

図 24-3 非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ボーリング メカニズムを使用していません。ローカル リンク障害検出を実装しています。REP Link Status Layer (LSL; リンクステータス レイヤ) が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。すべての VLAN は、ネイバーが検出されるまでインターフェイス上でブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパンニング ツリー アルゴリズムで使用されるものと類似しており、ポート番号 (ブリッジ上で一意) と、関連 MAC アドレス (ネットワーク内で一意) から構成されます。セグメント ポートが起動すると、

ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されません。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない。
- 複数のネイバーに同じセグメント ID がある。
- ネイバーがピアとして、ローカル ポートに確認応答しない。

各ポートは、直近のネイバーと隣接関係を確立します。ネイバー関係が確立されると、ポートがセグメントの 1 つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。その他のポートのブロックは解除されます。デフォルトで、REP パケットは Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) クラス MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信できますが、セグメントに障害が発生した場合に Blocked Port Advertisement (BPA; ブロックされたポートのアドバタイズ) メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

短時間でのコンバージェンス

REP が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、必要なのは全 VLAN で 1 Hello メッセージだけなので、プロトコルの負荷が低減します。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッドすることも可能です。これらのメッセージは Hardware Flood Layer (HFL; ハードウェア フラッド レイヤ) で動作し、REP セグメントだけではなくネットワーク全体にフラッドされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッドを制御することができます。

ファイインターフェイスのコンバージェンス復旧時間の推定値は、200 の VLAN が設定されたローカル セグメントで 200 ミリ秒未満です。VLAN ロード バランシングのコンバージェンスは 300 ミリ秒以下です。

VLAN ロード バランシング

REP セグメント内の 1 エッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの `show interface rep detail` インターフェイス コンフィギュレーション コマンドを入力します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ~ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

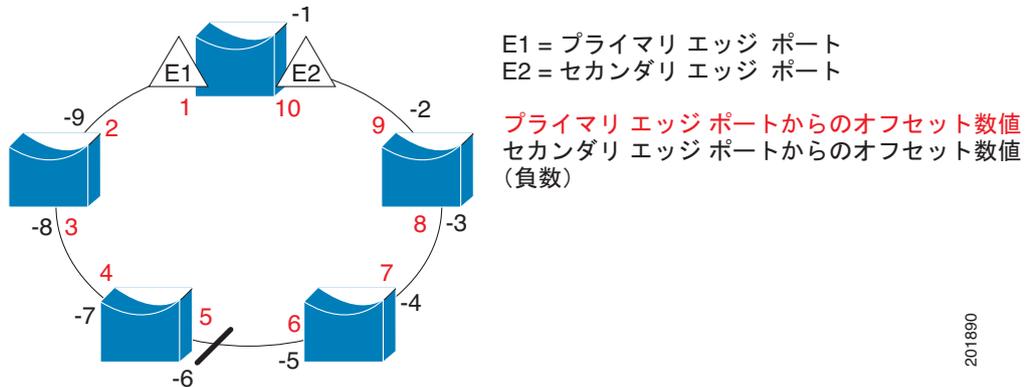


(注) プライマリ (またはセカンダリ) エッジ ポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

図 24-4 に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメント内のネイバー オフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号 (プライマリ エッジ ポートからのダウンストリーム位置) または負のオフセット番号 (セカンダリ エッジ ポートからのダウンストリーム位置) のいずれかにより、(プライマリ エッジ ポートを除く) 全ポートを識別することができます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

- **preferred** キーワードを入力します。これにより、**rep segment segment-id preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。

図 24-4 セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定するには、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要があります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment segment-id** 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay seconds** インターフェイス コンフィギュレーション コマンドを入力すると、プリエンブション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンブション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。



(注) VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンブションについて警告します。メッセージがセカンダリポートで受信されると、これがネットワークに反映され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジ ポートでは、再び **rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロード バランシングステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は、STP とともに Flex Link 機能とも対話しませんが、どちらとも共存できます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

REP ポート

REP セグメント内のポートは、障害、オープン、代替のいずれかになります。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが発生して、セグメントが安定すると、ブロックされたポートのうちの 1 つが代替ロールのままになって他のすべてのポートがオープン ポートになります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジ ポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディング ステートになります。

REP の設定

セグメントは、チェーンで相互接続しているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、1 つをプライマリ エッジ ポート、もう 1 つをデフォル

トでセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。オプションで、Segment Topology Change Notice (STCN; セグメント トポロジ変更通知) および VLAN ロード バランシングを送信する場所を設定することもできます。

- 「REP のデフォルト設定」 (P.24-7)
- 「REP 設定時の注意事項」 (P.24-7)
- 「REP 管理 VLAN の設定」 (P.24-9)
- 「REP インターフェイスの設定」 (P.24-10)
- 「VLAN ロード バランシングの手動によるプリエンブションの設定」 (P.24-14)
- 「REP の SNMP トラップ設定」 (P.24-14)

REP のデフォルト設定

REP はすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジ ポートとして設定されていない場合はインターフェイスは通常セグメント ポートになります。

REP をイネーブルにする際に、STCN の送信はディセーブルで、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。

VLAN ロード バランシングがイネーブルの場合、デフォルトは手動でのプリエンブションで、遅延タイマーはディセーブルになっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンブション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- まず 1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では 3 つ以上のポートに障害が発生した場合、1 ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。show rep interface 特権 EXEC コマンド出力では、このポートのポート ロールは *Fail Logical Open* と表示され、他の障害ポートのポート ロールは *Fail No Ext Neighbor* と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選定メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 トランク ポートである必要があります。
- Telnet 接続を通じて REP を設定する際には注意してください。別の REP インターフェイスがメッセージを送信してブロック解除するまで REP はすべての VLAN をブロックするため、同じインターフェイスを通じてスイッチにアクセスする Telnet セッションで REP をイネーブルにすると、スイッチへの接続が失われる可能性があります。
- REP と STP または REP と Flex Link を同じセグメントやインターフェイスで実行できません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていない STP 接続は、REP セグメントでは STP が実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。

- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP ポートは以下の規則に従います。
 - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
 - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジポートとなります。
 - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメントポートであるか、一方が通常ポートでもう一方が非ネイバーエッジポートである必要があります。スイッチ上のエッジポートと通常セグメントポートが同じセグメントに属することはできません。
 - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジポートとして設定され、もう 1 つが通常セグメントポートに設定されている場合（設定ミス）、エッジポートは通常セグメントポートとして扱われます。
- REP インターフェイスがブロック状態になり、ブロック解除しても安全であると通知されるまでブロック状態のままになります。突然の接続切断を避けるために、これを意識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコマルチキャストアドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。`rep lsl-age-timer value` インターフェイス コンフィギュレーション コマンドを使用して、120 ~ 10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピアスイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。
 - Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ~ 10000 ミリ秒 (500 ミリ秒単位) から 120 ~ 10000 ミリ秒 (40 ミリ秒単位) に変更されています。REP ネイバー装置で Cisco IOS release 12.2(52)SE 以降が実行されていない場合は、タイマーの値を 3000 ミリ秒未満に設定しないでください。3000 ミリ秒未満の値を設定すると、要求されている時間内にネイバースイッチが応答しないため、ポートがシャットダウンします。
 - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポートチャネルで 1000 ミリ秒未満の値を設定しようとすると、エラーメッセージが表示されてコマンドが拒否されます。
- REP LSL エージング タイマーを設定するときには、リンクの両端で同じ値を設定するようにしてください。リンクの両端で同じ値が設定されていないと、REP リンクフラップが発生します。
- REP ポートは、これらのポートタイプのいずれかに設定できません。
 - SPAN 宛先ポート
 - トンネルポート
 - アクセスポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大で 64 REP セグメントです。

REP 管理 VLAN の設定

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- スイッチとセグメントで 1 つの管理 VLAN だけが可能です。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>rep admin vlan <i>vlan-id</i></code>	管理 VLAN を指定します。指定できる範囲は 2 ~ 4094 です。デフォルトは VLAN 1 です。管理 VLAN を 1 に設定するには、 <code>no rep admin vlan</code> グローバル コンフィギュレーション コマンドを実行します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show interface [<i>interface-id</i>] rep detail</code>	REP インターフェイスのいずれか 1 つの設定を確認します。
ステップ 5	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、管理 VLAN を VLAN 100 として設定して、REP インターフェイスの 1 つに `show interface rep detail` コマンドを入力して設定を確認する例を示します。

```
Switch# configure terminal
Switch (conf)# rep admin vlan 100
Switch (conf-if)# end
Switch# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
```

```

BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190

```

REP インターフェイスの設定

REP 動作の場合、各セグメント インターフェイスでこれをイネーブルにして、セグメント ID を指定します。このステップは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

インターフェイス上で REP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネル範囲は 1 ~ 48 です。
ステップ 3	switchport mode trunk	インターフェイスをレイヤ 2 トランク ポートとして設定します。

コマンド	目的
ステップ4 <code>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</code>	<p>インターフェイスで REP をイネーブルにして、セグメント番号を指定します。指定できるセグメント ID の範囲は 1 ~ 1024 です。これらの任意のキーワードは利用可能です。</p> <p>(注) 各セグメントに 1 つのプライマリ エッジポートを含めて、2 つのエッジポートを設定する必要があります。</p> <ul style="list-style-type: none"> • edge を入力して、ポートをエッジポートとして設定します。primary キーワードなしで edge を入力すると、ポートがセカンドリ エッジポートとして設定されます。各セグメントにあるエッジポートは 2 つだけです。 • (任意) エッジポート上で、primary を入力してポートをプライマリ エッジポートとして設定し、VLAN ロード バランシングを設定するポートを設定することができます。 • (任意) no-neighbor を入力して、外部 REP ネイバーを持たないポートをエッジポートとして設定します。そのポートはエッジポートのすべての特性を継承するため、他のエッジポートと同じように設定できます。 <p>(注) 各セグメントにあるプライマリ エッジポートは 1 つですが、2 つの異なるスイッチにエッジポートを設定して primary キーワードを両方のスイッチに入力しても、その設定は許容されます。ただし、REP ではセグメントプライマリ エッジポートとして 1 つのポートだけが選択されます。show rep topology 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジポートを指定することができます。</p> <ul style="list-style-type: none"> • (任意) preferred を入力して、ポートが優先代替ポートであるか、VLAN ロード バランシングの優先ポートであるのかを示します。 <p>(注) ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。</p>
ステップ5 <code>rep stcn {interface interface-id segment id-list stp}</code>	<p>(任意) STCN を送信するようにエッジポートを設定します。</p> <ul style="list-style-type: none"> • interface interface-id を入力して、STCN を受信するための物理インターフェイスまたはポートチャネルを指定します。 • segment id-list を入力して、STCN を受信するための 1 つまたは複数のセグメントを指定します。有効範囲は 1 ~ 1024 です。 • stp を入力して、STCN を STP ネットワークに送信します。

コマンド	目的
ステップ 6 <code>rep block port {id port-id neighbor_offset preferred} vlan {vlan-list all}</code>	<p>(任意) プライマリ エッジ ポートに VLAN ロード バランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し、代替ポートでブロックされるように VLAN を設定します。</p> <ul style="list-style-type: none"> • <code>id port-id</code> を入力して、ポート ID で代替ポートを指定します。セグメント内の各ポートにポート ID が自動的に生成されます。<code>show interface interface-id rep [detail]</code> 特権 EXEC コマンドを入力して、インターフェイス ポート ID を表示できます。 • <code>neighbor_offset</code> 番号を入力して、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして指定します。有効範囲は -256 ~ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。値 0 は無効です。-1 を入力して、セカンダリ エッジ ポートを代替ポートとして識別します。ネイバー オフセット番号付けの例については、図 24-4 (P.24-5) を参照してください。 <p>(注) プライマリ エッジ ポート (オフセット番号 1) にこのコマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力しません。</p> <ul style="list-style-type: none"> • <code>preferred</code> を入力して、すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。 • <code>vlan vlan-list</code> を入力して、1 VLAN または VLAN 範囲をブロックします。 • <code>vlan all</code> を入力して、すべての VLAN をブロックします。 <p>(注) REP プライマリ エッジ ポート上にのみこのコマンドを入力します。</p>
ステップ 7 <code>rep preempt delay seconds</code>	<p>(任意) リンク障害および回復後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力して、プリエンプシジョン遅延時間を設定する必要があります。遅延時間の範囲は 15 ~ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプシジョンです。</p> <p>(注) REP プライマリ エッジ ポート上にのみこのコマンドを入力します。</p>
ステップ 8 <code>rep lsl-age-timer value</code>	<p>(任意) ネイバーからの hello が受信されないままのくらいの時間 (ミリ秒) が経過すると REP インターフェイスがダウンするかを設定します。</p> <p>指定できる範囲は 120 ~ 10000 ミリ秒 (40 ミリ秒単位) です。デフォルト値は 5000 ミリ秒 (5 秒) です。</p> <p>(注) ネイバー装置で Cisco IOS Release 12.2(52)SE 以降が実行されていない場合は、指定できる範囲が 3000 ~ 10000 ミリ秒 (500 ミリ秒単位) になります。EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。</p>
ステップ 9 <code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 10	<code>show interface [interface-id] rep [detail]</code>	REP インターフェイス コンフィギュレーションを確認します。
ステップ 11	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーションファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。 **show rep topology** 特権 EXEC コマンドを入力して、セグメント内のどのポートがプライマリ エッジ ポートなのかを確認します。

次に、インターフェイスをセグメント 1 のプライマリ エッジ ポートに設定し、STCN をセグメント 2 ~ 5 に送信し、代替ポートをポート ID 0009001818D68700 のポートとして設定して、セグメント ポート障害および回復後の 60 秒のプリエンブション遅延後にすべての VLAN をブロックする例を示します。このインターフェイスは、ネイバーからの hello が受信されないまま 6000 ミリ秒が経過するとダウンするように設定されています。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end
```

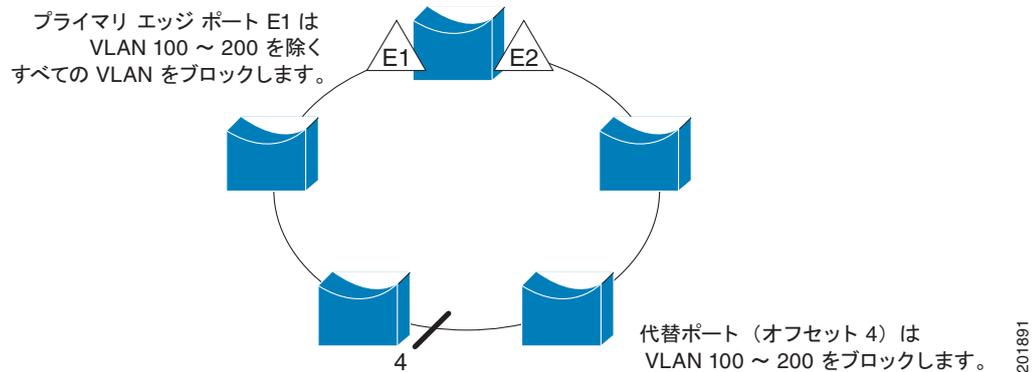
次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
```

次に、[図 24-5](#) の、VLAN ブロッキング コンフィギュレーションを設定する例を示します。代替ポートは、ネイバー オフセット番号 4 のネイバーです。手動によるプリエンブションのあとに、VLAN 100 ~ 200 がこのポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1 (ギガビットイーサネット ポート 1/0/1) でブロックされます。

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end
```

図 24-5 VLAN ブロッキングの例



VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリ エッジ ポートでプリエンプション遅延時間を設定する `rep preempt delay seconds` インターフェイス コンフィギュレーション コマンドを入力しない場合、デフォルトでは、セグメントでの VLAN ロード バランシングのトリガーは手動になっています。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。 `rep preempt segment segment-id` コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

コマンド	目的
ステップ1 <code>rep preempt segment segment-id</code>	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ2 <code>show rep topology</code>	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

リンク動作ステータス変更およびポート ロール変更について SNMP サーバに通知するために、REP 固有のトラップの送信をスイッチに設定できます。REP トラップを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>snmp mib rep trap-rate value</code>	REP トラップを送信するようにスイッチでイネーブルにして、1 秒あたりのトラップの送信数を設定します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 (制限なし、発生するたびにトラップが送信される) です。
ステップ3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ4 <code>show running-config</code>	REP トラップ コンフィギュレーションを確認します。
ステップ5 <code>copy running-config startup config</code>	(任意) スwitchのスタートアップ コンフィギュレーション ファイルに設定を保存します。

トラップを削除するには、**no snmp mib rep trap-rate** グローバル コンフィギュレーション コマンドを入力します。

1 秒あたり 10 の割合で REP トラップを送信するようにスイッチを設定する例を示します。

```
Switch(config)# snmp mib rep trap-rate 10
```

REP のモニタ

表 24-1 REP モニタ コマンド

コマンド	目的
show interface [<i>interface-id</i>] rep [detail]	特定のインターフェイスまたはすべてのインターフェイスの REP の設定とステータスを表示します。
show rep topology [segment <i>segment_id</i>] [archive] [detail]	セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 セグメントまたは全セグメントの REP トポロジ情報を表示します。



CHAPTER 25

Flex Link および MAC アドレス テーブル移動更新機能の設定

この章では、Flex Link の設定方法について説明します。これは、相互バックアップを提供する IE 3000 スイッチ上のインターフェイスのペアです。また、MAC Address-Table Move Update Feature (MAC アドレス テーブル移動更新機能、Flex Links の双方向高速コンバージェンス機能とも呼ばれます) の設定方法も説明します。



(注)

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

この章の内容は、次のとおりです。

- 「Flex Link および MAC アドレス テーブル移動更新機能の概要」 (P.25-1)
- 「Flex Link および MAC アドレス テーブル移動更新の設定」 (P.25-7)
- 「Flex Link および MAC アドレス テーブル移動更新機能のモニタ」 (P.25-15)

Flex Link および MAC アドレス テーブル移動更新機能の概要

ここでは、次の情報について説明します。

- 「Flex Link」 (P.25-1)
- 「VLAN Flex Link ロード バランシングおよびサポート」 (P.25-2)
- 「Flex Link マルチキャスト高速コンバージェンス」 (P.25-3)
- 「MAC アドレス テーブル移動更新」 (P.25-6)

Flex Link

Flex Link は、レイヤ 2 インターフェイス (スイッチ ポートまたはポート チャネル) のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、Spanning Tree Protocol (STP; スパニングツリー プロトコル) の代替ソリューションです。ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。Flex Link は、通常、お客

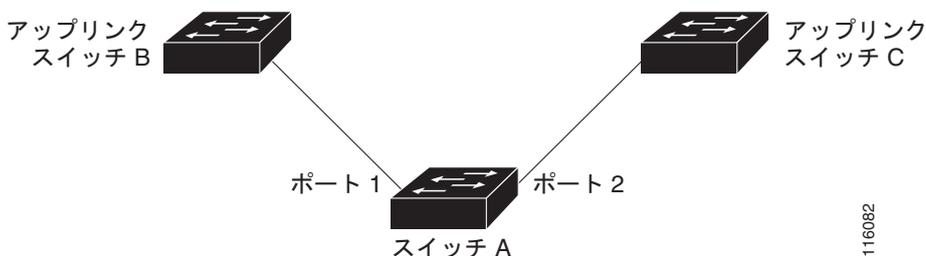
様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。スイッチが STP を実行中の場合は、STP がすでにリンクレベルの冗長性またはバックアップを提供しているため、Flex Link は不要です。

別のレイヤ 2 インターフェイスを Flex Link またはバックアップリンクとして割り当てることで、1 つのレイヤ 2 インターフェイス (アクティブリンク) に Flex Link を設定します。リンクの 1 つがアップでトラフィックを転送しているときは、もう一方のリンクがスタンバイモードで、このリンクがシャットダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスのみがリンクアップ状態でトラフィックを転送しています。プライマリリンクがシャットダウンされると、スタンバイリンクがトラフィックの転送を始めます。アクティブリンクがアップに戻った場合はスタンバイモードになり、トラフィックが転送されません。STP は Flex Link インターフェイスでディセーブルです。

図 25-1 では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これらのスイッチは Flex Link として設定されているので、どちらかのインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイモードになります。ポート 1 がアクティブリンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転送を開始し、ポート 2 (バックアップリンク) とスイッチ C との間のリンクでは、トラフィックは転送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。ポート 1 は、再び動作を開始するとスタンバイモードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、優先してトラフィックの転送に使用するポートを指定して、プリエンプトメカニズムを設定することもできます。たとえば、図 25-1 では、Flex Link ペアをプリエンプトモードで設定することにより、ポート 2 より帯域幅の大きいポート 1 が再び動作を開始した後、ポート 1 が 60 秒後にトラフィックの転送を開始し、ポート 2 がスタンバイとなります。これを行うには、**switchport backup interface preemption mode bandwidth** および **switchport backup interface preemption delay** インターフェイス コンフィギュレーション コマンドを入力します。

図 25-1 Flex Link の設定例



プライマリ (転送) リンクがダウンすると、トラップによってネットワーク管理ステーションが通知を受けます。スタンバイリンクがダウンすると、トラップによってユーザが通知を受けます。

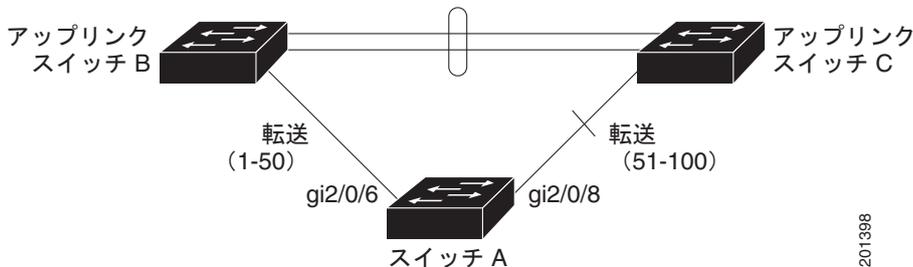
Flex Link はレイヤ 2 ポートおよびポート チャネルだけでサポートされ、VLAN またはレイヤ 3 ポートではサポートされません。

VLAN Flex Link ロード バランシングおよびサポート

VLAN Flex Link ロード バランシングにより、ユーザは相互に排他的な VLAN のトラフィックを両方のポートで同時に転送するように Flex Link ペアを設定できます。たとえば、Flex Link ポートが 1 ~ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。どちらかのポートで障害が発生した場合には、もう一方のアクティブポートがすべてのトラフィックを転送します。障害が発生

したポートが元に戻ると、優先 VLAN のトラフィックの転送を再開します。このように、Flex Link のペアは冗長性を提供するだけでなく、ロード バランシングの用途に使用できます。また、Flex Link VLAN ロード バランシングによってアップリンク スイッチが制約を受けることはありません。

図 25-2 VLAN Flex Link ロード バランシングの設定例



201398

Flex Link マルチキャスト高速コンバージェンス

Flex Link マルチキャスト高速コンバージェンスにより、Flex Link の障害発生後のマルチキャストトラフィック コンバージェンス時間が短縮されます。Flex Link マルチキャスト高速コンバージェンスは、次の各ソリューションを組み合わせることにより実装されます。

- 「その他の Flex Link ポートを mrouter ポートとして学習」 (P.25-3)
- 「IGMP レポートの生成」 (P.25-4)
- 「IGMP レポートのリーク」 (P.25-4)
- 「設定例」 (P.25-4)

その他の Flex Link ポートを mrouter ポートとして学習

通常のマルチキャスト ネットワークでは、個々の VLAN について 1 つのクエリアが選定されます。ネットワーク エッジに展開されたスイッチには、クエリーを受信するいずれかの Flex Link ポートが存在します。Flex Link ポートは常に、転送状態になります。

クエリーを受信するポートが、スイッチの *mrouter* ポートとして追加されます。*mrouter* ポートは、スイッチが学習したすべてのマルチキャスト グループの 1 つとして認識されます。切り替えの後、クエリーは別の Flex Link ポートによって受信されます。この別の Flex Link ポートは *mrouter* ポートとして認識されるようになります。切り替えの後、マルチキャストトラフィックは別の Flex Link ポートを介して流れます。トラフィック コンバージェンスを高速化するために、いずれか一方の Flex Link ポートが *mrouter* ポートとして学習されると、両方の Flex Link ポートが *mrouter* ポートとして認識されず、いずれの Flex Link ポートも常に、マルチキャスト グループの一部として扱われます。

通常の動作モードではいずれの Flex Link ポートもグループの一部として認識されますが、バックアップポートを通過するトラフィックはすべてブロックされます。したがって、*mrouter* ポートとしてバックアップポートを追加しても、通常のマルチキャストデータフローに影響を受けることはありません。切り替えが生じると、バックアップポートのブロックが解除され、トラフィックが流れるようになります。この場合、バックアップポートのブロックが解除されるとただちに、アップストリームデータが流れ始めます。

IGMP レポートの生成

切り替えの後、バックアップリンクがアップ状態になると、アップストリームでの新しいディストリビューションスイッチでのマルチキャストデータの転送は開始されません。これは、ブロックされた Flex Link ポートに接続されているアップストリームルータのポートが、いずれのマルチキャストグループの一部としても認識されないからです。マルチキャストグループのレポートは、バックアップリンクがブロックされているため、ダウンストリームスイッチでは転送されません。このポートのデータは、マルチキャストグループが学習されるまで流れません。マルチキャストグループの学習は、レポートを受信した後にだけ行われます。

レポートは、一般クエリーを受信されると、ホストより送信されます。一般クエリーは、通常のシナリオであれば 60 秒以内に送信されます。バックアップリンクが転送を開始し、マルチキャストデータを高速で収束できるようになると、ダウンストリームスイッチが一般クエリーを待つことなく、ただちにこのポート上のすべての学習済みグループに対し、プロキシレポートを送信します。

IGMP レポートのリーク

マルチキャストトラフィックを最小限の損失で収束させるために、Flex Link のアクティブリンクがダウンする前に冗長データパスを設定しておく必要があります。マルチキャストトラフィックのコンバージェンスは、Flex Link バックアップリンクに IGMP レポートパケットだけをリークさせれば行えます。こうしてリークさせた IGMP レポートメッセージがアップストリームのディストリビューションルータで処理されるため、マルチキャストデータのトラフィックはバックアップインターフェイスに転送されます。バックアップインターフェイスの着信トラフィックはすべてアクセススイッチの入り口部分でドロップされるため、ホストが重複したマルチキャストトラフィックを受信することはありません。Flex Link のアクティブリンクに障害が発生した場合、ただちにアクセススイッチがバックアップリンクからのトラフィックを受け入れ始めます。このスキームの唯一の欠点は、ディストリビューションスイッチ間のリンク、およびディストリビューションスイッチとアクセススイッチの間のバックアップリンクで帯域幅が大幅に消費される点です。この機能はデフォルトでディセーブルになっています。 `switchport backup interface interface-id multicast fast-convergence` コマンドを使用して、設定を変更できます。

切り替え時にこの機能がイネーブルになっている場合、スイッチでは転送ポートに設定されたバックアップポート上でプロキシレポートは生成されません。

設定例

次に、Flex Link ポートを設定したときに他の Flex Link ポートを mrouter ポートとして学習する例と、`show interfaces switchport backup` コマンドの出力を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface GigabitEthernet1/2
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
Preemption Mode : off
Multicast Fast Convergence : Off
Mac Address Move Update Vlan : auto
```

次の出力は、特定のポートを介してスイッチに到達するクエリーを持つ、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan    IP Address      IGMP Version    Port
-----
1       1.1.1.1         v2              Gi0/1
401     41.41.41.1     v2              Gi0/1
```

次に、VLAN 1 および VLAN 401 用の `show ip igmp snooping mrouter` コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -
1       Gi1/1(dynamic), Gi1/2(dynamic)
401     Gi1/1(dynamic), Gi1/2(dynamic)
```

同様に、両方の Flex Link ポートは学習されたグループに属しています。この例では、`GigabitEthernet1/1` は VLAN 1 のレシーバ/ホストであり、2 つのマルチキャスト グループに関連しています。

```
Switch# show ip igmp snooping groups
Vlan    Group           Type    Version    Port List
-----
1       228.1.5.1       igmp    v2         Gi1/1, Gi1/2, Fa2/1
1       228.1.5.2       igmp    v2         Gi1/1, Gi1/2, Fa2/1
```

ホストが一般クエリーに応答するときに、スイッチはすべてのマルチキャスト ルータ ポートに関するこのレポートを転送します。この例では、ホストがグループ 228.1.5.1 のレポートを送信するとき、バックアップ ポート `GigabitEthernet1/2` はブロックされているので、レポートは `GigabitEthernet1/1` でだけ送信されます。アクティブ リンクの `GigabitEthernet1/1` がダウンすると、バックアップ ポートの `GigabitEthernet1/2` が転送を開始します。

このポートが転送を開始すると、ただちにホストに代わり、228.1.5.1 と 228.1.5.2 のグループにプロキシ レポートを送信します。アップストリーム ルータはグループを学習し、マルチキャスト データの転送を開始します。これは、Flex Link のデフォルトの動作です。ユーザが `switchport backup interface GigabitEthernet1/2 multicast fast-convergence` コマンドを使用して高速コンバージェンスを設定すると、この動作は変更されます。次に、この機能を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport backup interface GigabitEthernet1/2 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
```

```
Switch Backup Interface Pairs:
Active          Interface          Backup Interface State
-----
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Mac Address Move Update Vlan : auto
```

次の出力は、設定されたポートを介してスイッチに到達するクエリーを持つ、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan    IP Address      IGMP Version    Port
-----
```

```

1          1.1.1.1          v2          Gi1/1
401       41.41.41.1      v2          Gi1/1

```

次に VLAN 1 と 401 に対する `show ip igmp snooping mrouter` コマンドの出力を示します。

```

Switch# show ip igmp snooping mrouter
Vlan      ports
-----
1         Gi1/1 (dynamic), Gi1/2 (dynamic)
401      Gi1/1 (dynamic), Gi1/2 (dynamic)

```

同様に、両方の Flex Link ポートは学習されたグループに属しています。この例では、ポートは VLAN 1 のレシーバ/ホストであり、2 つのマルチキャストグループに関連しています。

```

Switch# show ip igmp snooping groups
Vlan  Group      Type      Version  Port List
-----
1     228.1.5.1  igmp     v2       Gi1/1, Gi1/2, Gi1/1
1     228.1.5.2  igmp     v2       Gi1/1, Gi1/2, Gi1/1

```

一般クエリーに対してあるホストが応答すると必ず、スイッチがすべての mrouter ポートに関するこのレポートを転送します。コマンドライン ポートを通じてこの機能をオンにし、設定された GigabitEthernet1/1 上のスイッチによってレポートが転送されると、レポートはバックアップ ポート GigabitEthernet1/2 にもリークされます。アップストリーム ルータはグループを学習し、マルチキャストデータの転送を開始します。GigabitEthernet1/2 はブロックされているので、このデータは入力で廃棄されます。アクティブリンクの GigabitEthernet1/1 がダウンすると、バックアップ ポートの GigabitEthernet1/2 が転送を開始します。マルチキャストデータはすでにアップストリーム ルータにより転送されているため、いずれのプロキシ レポートも送信する必要はありません。バックアップ ポートにレポートをリークさせることにより、冗長マルチキャストパスが設定されるため、マルチキャストトラフィック コンバージェンスに要する時間が最小限に抑えられます。

MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能により、プライマリ (転送) リンクがダウンしてスタンバイリンクがトラフィックの転送を開始したときに、スイッチで高速双方向コンバージェンスが提供されます。

図 25-3 では、スイッチ A がアクセススイッチで、スイッチ A のポート 1 および 2 が Flex Link ペア経由でアップリンクスイッチの B と D に接続されます。ポート 1 はトラフィックの転送中で、ポート 2 はバックアップステートです。PC からサーバへのトラフィックはポート 1 からポート 3 に転送されます。PC の MAC アドレスが、スイッチ C のポート 3 で学習されています。サーバから PC へのトラフィックはポート 3 からポート 1 に転送されます。

MAC アドレス テーブル移動更新機能が設定されておらず、ポート 1 がダウンした場合は、ポート 2 がトラフィックの転送を開始します。しかし、少しの間、スイッチ C がポート 3 経由でサーバから PC にトラフィックを転送し続けるため、ポート 1 がダウンしていることにより、PC へのトラフィックが途切れます。スイッチ C がポート 3 で PC の MAC アドレスを削除し、ポート 4 で再度学習した場合は、トラフィックはポート 2 経由でサーバから PC へ転送される可能性があります。

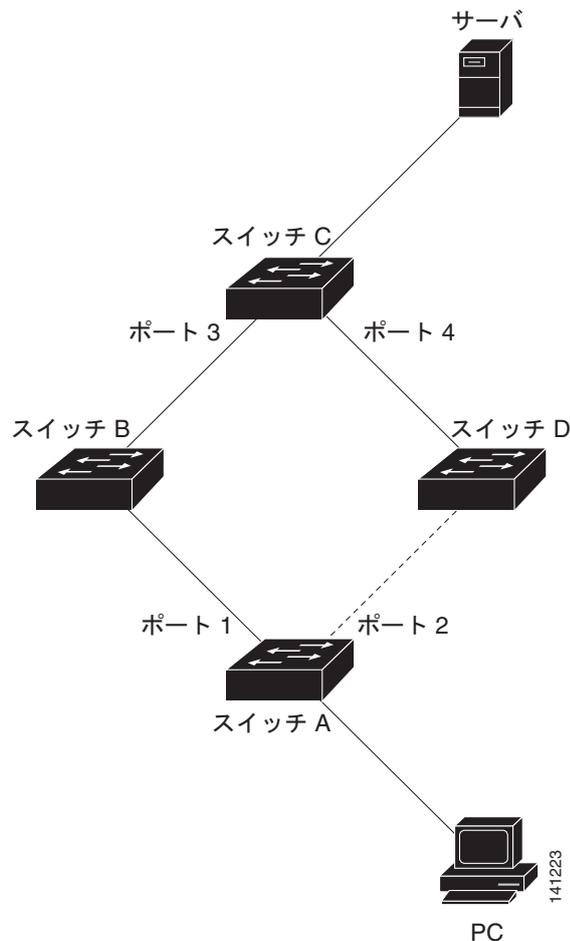
図 25-3 で MAC アドレス テーブル移動更新機能が設定され、各スイッチでイネーブルになっていて、ポート 1 がダウンした場合は、ポート 2 が PC からサーバへのトラフィックの転送を開始します。スイッチは、ポート 2 から MAC アドレス テーブル移動更新パケットを送出します。スイッチ C はこのパケットをポート 4 で受信し、ただちに PC の MAC アドレスをポート 4 で学習します。これにより、再収束時間が短縮されます。

アクセススイッチであるスイッチ A を設定し、MAC アドレス テーブル移動更新メッセージを送信 (send) することができます。また、アップリンクスイッチ B、C、および D を設定して、MAC アドレス テーブル移動更新メッセージの取得 (get) および処理を行うこともできます。スイッチ C がス

スイッチ A から MAC アドレス テーブル移動更新メッセージを受信すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブル エントリを含め、MAC アドレス テーブルをアップデートします。

スイッチ A が、MAC アドレス テーブル移動更新を待機する必要はありません。スイッチはポート 1 上の障害を検出すると、ただちに、新しい転送ポートであるポート 2 からのサーバトラフィックの転送を開始します。この変更は、100 ミリ秒 (ms) 以内に行われます。PC はスイッチ A に直接接続され、その接続状態に変更はありません。スイッチ A による、MAC アドレス テーブルでの PC エントリの更新は必要ありません。

図 25-3 MAC アドレス テーブル移動更新の例



Flex Link および MAC アドレス テーブル移動更新の設定

ここでは、次の情報について説明します。

- 「デフォルト設定」 (P.25-8)
- 「設定時の注意事項」 (P.25-8)
- 「Flex Link の設定」 (P.25-9)
- 「Flex Link の VLAN ロード バランシングの設定」 (P.25-11)

- 「MAC アドレス テーブル移動更新機能の設定」(P.25-12)

デフォルト設定

Flex Link は設定されておらず、バックアップ インターフェイスは定義されていません。

プリエンブト モードはオフです。

プリエンブト遅延は 35 秒です。

MAC アドレス テーブル移動更新機能は、スイッチで設定されていません。

設定時の注意事項

Flex Link の設定時には、次の注意事項に従ってください。

- 最大 16 のバックアップ リンクを設定できます。
- 任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは別の Flex Link ペアに属することはできません。
- どちらのリンクも EtherChannel に属するポートにすることができません。ただし、2 つのポートチャンネル (EtherChannel 論理インターフェイス) を Flex Link として設定でき、ポート チャンネルおよび物理インターフェイスを Flex Link として設定して、ポート チャンネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- バックアップ リンクはアクティブ リンクと同じタイプ (ファストイーサネット、ギガビットイーサネット、またはポート チャンネル) にする必要はありません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- STP は Flex Link ポートでディセーブルです。ポート上にある VLAN が STP 用に設定されている場合でも、Flex Link ポートは STP に参加しません。STP がイネーブルでない場合は、設定されているトポロジーでループが発生しないようにしてください。Flex Link 設定が削除されると、そのポートの STP は再びイネーブルになります。

Flex Link 機能による VLAN ロード バランシングを設定するときには、次の注意事項に従ってください。

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイス上で優先される VLAN を選択する必要があります。
- 同じ Flex Link ペアに対して、プリエンブト メカニズムと VLAN ロード バランシングを設定することはできません。

MAC アドレス テーブル移動更新機能の設定時には、次の注意事項に従ってください。

- アクセス スイッチでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を送信 (*send*) することができます。
- アップリンク スイッチでこの機能のイネーブル化と設定を行うと、MAC アドレス テーブル移動更新を受信 (*receive*) することができます。

Flex Link の設定

Flex Link のペアを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。指定できるポートチャネルの範囲は 1 ~ 6 です。
ステップ3	<code>switchport backup interface interface-id</code>	物理レイヤ 2 インターフェイス（ポートチャネル）をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show interfaces [interface-id] switchport backup</code>	設定を確認します。
ステップ6	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

Flex Link バックアップ インターフェイスをディセーブルにするには、**no switchport backup interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスをバックアップ インターフェイスに設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2
Switch(conf-if)# end
```

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
```

```
Vlans Preferred on Active Interface: 1-3,5-4094
```

```
Vlans Preferred on Backup Interface: 4
```

Flex Link ペアのプリエンプト方式を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポートチャネルの範囲は 1 ~ 6 です。

	コマンド	目的
ステップ 3	switchport backup interface <i>interface-id</i>	物理レイヤ 2 インターフェイス (ポート チャネル) をインターフェイスがある Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ 4	switchport backup interface <i>interface-id</i> preempt mode [forced bandwidth off]	Flex Link インターフェイス ペアのプリエンプト メカニズムとプリエンプト遅延を設定します。次のプリエンプト モードを設定することができます。 <ul style="list-style-type: none"> • Forced : アクティブ インターフェイスが常にバックアップ インターフェイスより先に使用されます。 • Bandwidth : より大きい帯域幅のインターフェイスが常にアクティブ インターフェイスとして動作します。 • Off : アクティブ インターフェイスとバックアップ インターフェイスのどちらも優先されません。
ステップ 5	switchport backup interface <i>interface-id</i> preempt delay <i>delay-time</i>	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 (注) 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [<i>interface-id</i>] switchport backup	設定を確認します。
ステップ 8	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

プリエンプト方式を削除するには、**no switchport backup interface *interface-id* preempt mode** インターフェイス コンフィギュレーション コマンドを使用します。遅延時間をデフォルトにリセットするには、**no switchport backup interface *interface-id* preempt delay** インターフェイス コンフィギュレーション コマンドを使用します。

次に、バックアップ インターフェイスのペアに対してプリエンプト モードを *forced* に設定し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preempt mode forced
Switch(conf-if)#switchport backup interface gigabitethernet1/2 preempt delay 50
Switch(conf-if)# end
```

```
Switch# show interfaces switchport backup detail
Active Interface Backup Interface State
-----
GigabitEthernet1/1 GigabitEthernet1/2 Active Up/Backup Standby
Interface Pair : Gi1/1, Gi1/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/1), 100000 Kbit (Gi1/2)
Mac Address Move Update Vlan : auto
```

Flex Link の VLAN ロード バランシングの設定

Flex Link の VLAN ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。指定できるポートチャネルの範囲は 1 ~ 6 です。
ステップ3	<code>switchport backup interface interface-id prefer vlan vlan-range</code>	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある Flex Link ペアの一部として設定します。VLAN ID の範囲は 1 ~ 4094 です。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show interfaces [interface-id] switchport backup</code>	設定を確認します。
ステップ6	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシング機能をディセーブルにするには、**no switchport backup interface interface-id prefer vlan vlan-range** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチに VLAN 1 ~ 50、60、および 100 ~ 120 を設定する例を示します。

```
Switch(config)# interface gigabitEthernet 1/2
Switch(config-if)# switchport backup interface gigabitEthernet 1/2 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合、GigabitEthernet1/1 は VLAN 60 および 100 ~ 120 のトラフィックを転送し、GigabitEthernet1/2 は VLAN 1 ~ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet1/1   GigabitEthernet1/2   Active Up/Backup Standby
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると (LINK_DOWN)、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gigabit Ethernet1/1 がダウンした場合、Gigabit Ethernet1/2 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet1/1   GigabitEthernet1/2   Active Down/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gigabit Ethernet1/1 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gigabit Ethernet1/2 上でブロックされ、Gigabit Ethernet1/1 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet1/1   GigabitEthernet1/2   Active Down/Backup Up
```

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

```
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
FastEthernet1/3       FastEthernet1/4      Active Down/Backup Up
```

```
Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode      : off
Bandwidth : 10000 Kbit (Fa1/3), 100000 Kbit (Fa1/4)
Mac Address Move Update Vlan : auto
```

MAC アドレス テーブル移動更新機能の設定

ここでは、次の情報について説明します。

- MAC アドレス テーブル移動更新を送信するためのスイッチの設定
- MAC アドレス テーブル移動更新を受信するためのスイッチの設定

MAC アドレス テーブル移動更新を送信するようにアクセス スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 interface interface-id	インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。ポート チャネルの範囲は 1 ～ 6 です。

	コマンド	目的
ステップ3	<code>switchport backup interface <i>interface-id</i></code> または <code>switchport backup interface <i>interface-id</i> mmu primary vlan <i>vlan-id</i></code>	物理レイヤ 2 インターフェイス (ポート チャネル) をインターフェイスがある Flex Link ペアの一部として設定します。MAC アドレス テーブル移動更新 VLAN はインターフェイスで最も低い VLAN ID です。 物理レイヤ 2 インターフェイス (ポート チャネル) を設定し、MAC アドレス テーブル移動更新の送信に使用されるインターフェイスの VLAN ID を指定します。 1 つのリンクがトラフィックを転送している場合、もう一方のインターフェイスはスタンバイ モードです。
ステップ4	<code>end</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ5	<code>mac address-table move update transmit</code>	プライマリ リンクがダウンし、スイッチがスタンバイ リンク経由でトラフィックの転送を開始した場合は、アクセス スイッチをイネーブルにして、MAC アドレス テーブル移動更新をネットワーク上の他のスイッチに送信します。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show mac address-table move update</code>	設定を確認します。
ステップ8	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、**no mac address-table move update transmit** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移動更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch(conf)# interface gigabitethernet1/1
Switch(conf-if)# switchport backup interface gigabitethernet1/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

MAC アドレス テーブル移動更新メッセージの受信および処理を行うようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table move update receive	スイッチをイネーブルにして、MAC アドレス テーブル移動更新の受信および処理を行います。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table move update	設定を確認します。
ステップ 5	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、**no mac address-table move update receive** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移動更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次に、スイッチを設定して、MAC アドレス テーブル移動更新メッセージの受信と処理を行う例を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

Flex Link および MAC アドレス テーブル移動更新機能のモニタ

表 25-1 は、Flex Link 設定と MAC アドレス テーブル移動更新情報をモニタする特権 EXEC コマンドを示します。

表 25-1 Flex Link および MAC アドレス テーブル移動更新のモニタ コマンド

コマンド	目的
<code>show interfaces [interface-id] switchport backup</code>	あるインターフェイス用に設定された Flex Link バックアップ インターフェイス、または設定されたすべての Flex Link と、各アクティブ インターフェイスおよびバックアップ インターフェイスの状態（アップまたはスタンバイ モード）を表示します。VLAN ロード バランシングがイネーブルであると、出力には、アクティブ インターフェイスおよびバックアップ インターフェイスの優先 VLAN が表示されます。
<code>show mac address-table move update</code>	スイッチに MAC アドレス テーブル移行更新情報を表示します。



CHAPTER 26

DHCP 機能と IP ソース ガード機能の設定

この章では、IE 3000 スイッチに、DHCP (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) スヌーピング機能、DHCP Option 82 データ挿入機能、および DHCP サーバのポートベースのアドレス割り当て機能を設定する方法について説明します。また、IP ソース ガード機能の設定方法についても説明します。



(注) この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンス、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2』の「DHCP Commands」を参照してください。

この章の内容は、次のとおりです。

- 「DHCP スヌーピングの理解」 (P.26-1)
- 「DHCP スヌーピングの設定」 (P.26-9)
- 「DHCP スヌーピング情報の表示」 (P.26-16)
- 「IP ソース ガードの概要」 (P.26-17)
- 「IP ソース ガードの設定」 (P.26-19)
- 「IP ソース ガード情報の表示」 (P.26-28)
- 「DHCP サーバ ポートベースのアドレス割り当ての概要」 (P.26-28)
- 「DHCP サーバ ポートベースのアドレス割り当ての設定」 (P.26-28)
- 「DHCP サーバ ポートベースのアドレス割り当ての表示」 (P.26-31)

DHCP スヌーピングの理解

DHCP は、中央のサーバからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。DHCP では、ネットワークに接続されたホストだけが IP アドレスを使用し、IP アドレスを永続的にホストに割り当てる必要がなくなるため、限られた IP アドレス空間を節約できます。

ここでは、次の情報について説明します。

- 「DHCP サーバ」 (P.26-2)
- 「DHCP リレー エージェント」 (P.26-2)
- 「DHCP Snooping」 (P.26-2)

- 「Option 82 データ挿入」(P.26-4)
- 「Cisco IOS DHCP サーバ データベース」(P.26-7)
- 「DHCP スヌーピング バインディング データベース」(P.26-7)

DHCP クライアントの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の「Configuring DHCP」を参照してください。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP Snooping

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース (DHCP スヌーピング バインディング テーブルとも呼ばれる) の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンド ユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。



(注) DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外側から送信されたメッセージのことです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク上にないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信頼できないインターフェイスとなります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCP OFFER パケット、DHCP ACK パケット、DHCP NAK パケット、DHCP LEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スwitchが DHCP RELEASE または DHCP DECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジ スイッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジ スイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジ スイッチによって挿入された Option 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジ スイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

Option 82 データ挿入

住宅地域にあるメトロポリタンイーサネットアクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。サブスクリバ LAN 上の複数のホストをアクセススイッチの同じポートに接続できます。これらのホストは一意に識別されます。

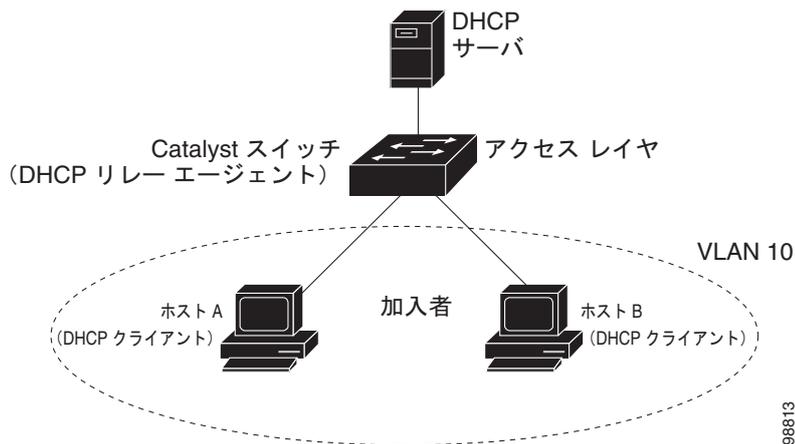


(注)

DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、この機能を使用する加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 26-1 に、一元的な DHCP サーバがアクセスレイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタンイーサネットネットワークの例を示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント (Catalyst スイッチ) にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 26-1 メトロポリタンイーサネットネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、次のイベントがこの順序で発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションは、パケットの受信ポートの ID である **vlan-mod-port** です。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、[図 26-2](#) にある次のフィールドの値は変化しません。

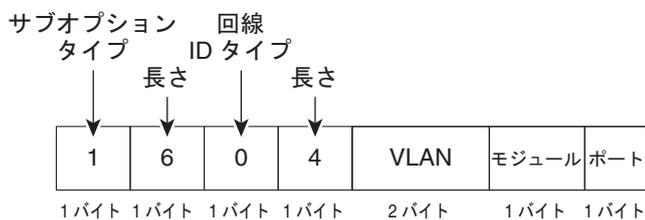
- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、8 つの 10/100 ポートと Small Form-Factor Pluggable (SFP) モジュール スロットを備えたスイッチでは、ポート 3 が Fast Ethernet 1/1 ポート、ポート 4 が Fast Ethernet 1/2 ポートなどのようになります。ポート 11 は SFP モジュール スロット 1/1 などのようになります。

[図 26-2](#) に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット フォーマットを示します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合です。

図 26-2 サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット



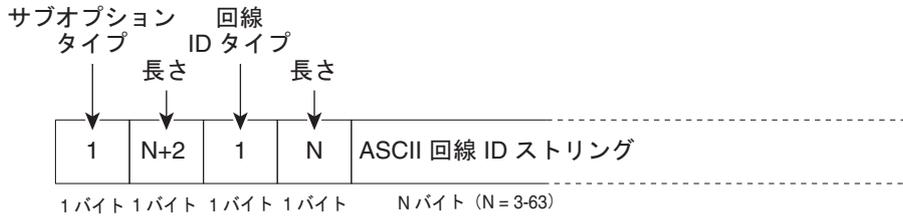
図 26-3 は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケットが使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

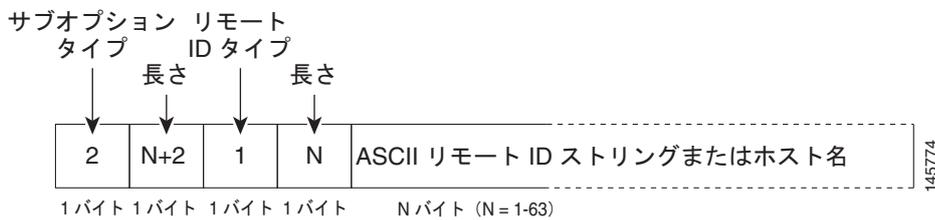
- 回線 ID サブオプション フィールド
 - 回線 ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
 - リモート ID タイプが 1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。

図 26-3 ユーザ設定のサブオプションの packets 形式

回線 ID サブオプション フレーム フォーマット (ユーザ設定の string)



リモート ID サブオプション フレーム フォーマット (ユーザ設定の string)



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てるのが可能です。手動および自動アドレス バインディングの詳細については、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] の下にある Cisco.com のページから『Cisco IOS IP Configuration Guide, Release 12.2』の「Configuring DHCP」の章を参照してください。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、8192 のバインディングを含めることができます。

各データベース エントリ (バインディング) は、IP アドレス、それに関連付けられた MAC アドレス、リース期間 (16 進形式)、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースが

ダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スwitchがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッドインターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

DHCP スヌーピングの設定

ここでは、次の設定について説明します。

- 「DHCP スヌーピングのデフォルト設定」 (P.26-9)
- 「DHCP スヌーピング設定時の注意事項」 (P.26-10)
- 「DHCP リレー エージェントの設定」 (P.26-11)
- 「パケット転送アドレスの指定」 (P.26-11)
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」 (P.26-13)
- 「プライベート VLAN での DHCP スヌーピングのイネーブル化」 (P.26-14)
- 「Cisco IOS DHCP サーバ データベースのイネーブル化」 (P.26-15)
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」 (P.26-15)

DHCP スヌーピングのデフォルト設定

表 26-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 26-1 DHCP スヌーピングのデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。 ¹
DHCP リレー エージェント	イネーブル ²
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル (無効なメッセージは廃棄)。 ²
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。 ²
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション ³	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 (注) スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。

2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。

3. この機能は、スイッチがエッジスイッチによって Option 82 が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

ここでは、DHCP の設定時の注意事項を説明します。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN で DHCP スヌーピングがイネーブルになるまでアクティブになりません。
- スwitch上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スwitchで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- スwitch上で文字数の多いサーキット ID を設定する場合、Nonvolatile Random-Access Memory (NVRAM; 不揮発性 RAM) またはフラッシュ メモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わせられた場合、NVRAM またはフラッシュ メモリの容量を超えてしまい、エラー メッセージが表示されます。
- スwitchで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルである場合、DHCP Option 82 データ挿入機能はサポートされません。
- スwitch ポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スwitch ポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- DHCP スヌーピング バインディング データベースを設定するときには、次の注意事項に従ってください。
 - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
 - ネットワーク ベースの URL (TFTP や FTP など) については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
 - データベースに正しいリース期間が記録されるように、NTP をイネーブルにし、設定することを推奨します。詳細については、「[手動での日時の設定](#)」(P.7-4) を参照してください。
 - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。
- 信頼できないデバイスが接続されたアグリゲーション スwitchに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、信頼できないデバイスが Option 82 情報をスプーフィングする可能性があります。

- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。



(注) RSPAN VLAN では、Dynamic Host Configuration Protocol (DHCP) スヌーピングをイネーブルにしないでください。RSPAN VLAN で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN 宛先ポートに届かない可能性があります。

DHCP リレー エージェントの設定

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

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	service dhcp	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。この機能はデフォルトでイネーブルです。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP サーバおよび DHCP リレー エージェントをディセーブルにするには、**no service dhcp** グローバル コンフィギュレーション コマンドを使用します。

次の手順については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の「Configuring DHCP」を参照してください。

- リレー エージェント情報のチェック (検証)
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address address** インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface vlan <i>vlan-id</i>	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip address <i>ip-address subnet-mask</i>	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 4	ip helper-address <i>address</i>	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバアドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	interface range <i>port-range</i> または interface <i>interface-id</i>	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	switchport mode access	ポートの VLAN メンバーシップ モードを定義します。
ステップ 8	switchport access vlan <i>vlan-id</i>	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show running-config	入力内容を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP パケット転送アドレスを削除するには、**no ip helper-address *address*** インターフェイス コンフィギュレーション コマンドを使用します。

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip dhcp snooping</code>	DHCP スヌーピングをグローバルにイネーブル化します。
ステップ3	<code>ip dhcp snooping vlan <i>vlan-range</i></code>	1 つの VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ~ 4094 です。 VLAN ID 番号によって特定される単一の VLAN ID、それぞれをカンマで区切った一連の VLAN ID、ハイフンを間に挿入した VLAN ID の範囲、または先頭および末尾の VLAN ID で区切られた VLAN ID の範囲を入力することができます。これらはスペースで区切ります。
ステップ4	<code>ip dhcp snooping information option</code>	スイッチが DHCP サーバへの DHCP 要求メッセージにおいて DHCP リレー情報 (Option 82 フィールド) を挿入および削除できるようにします。これがデフォルトの設定です。
ステップ5	<code>ip dhcp snooping information option format remote-id [string <i>ASCII-string</i> <i>hostname</i>]</code>	(任意) リモート ID サブオプションを設定します。 次のようにリモート ID を設定できます。 <ul style="list-style-type: none"> 63 文字までの ASCII 文字列 (スペースなし) スイッチに設定されたホスト名 (注) ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID はスイッチ MAC アドレスです。
ステップ6	<code>ip dhcp snooping information option allow-untrusted</code>	(任意) スwitchがエッジスイッチに接続された集約スイッチである場合、スイッチがエッジスイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを受け入れるようにします。 デフォルト設定はディセーブルです。 (注) このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ7	<code>interface <i>interface-id</i></code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ8	<code>ip dhcp snooping vlan <i>vlan</i> information option format-type circuit-id [override] string <i>ASCII-string</i></code>	(任意) 指定したインターフェイスで回線 ID サブオプションを設定します。 1 ~ 4094 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、フォーマットは vlan-mod-port です。 回線 ID は 3 ~ 63 の ASCII 文字列 (スペースなし) を設定できます。 (任意) override キーワードは、加入者情報を定義するための TLV 形式に回線 ID サブオプションを挿入したくない場合に使用します。
ステップ9	<code>ip dhcp snooping trust</code>	(任意) インターフェイスを信頼できるインターフェイスまたは信頼できないインターフェイスとして設定します。信頼できないクライアントからのメッセージを受信するようにインターフェイスを設定するには、 no キーワードを使用します。デフォルト設定は untrusted です。

	コマンド	目的
ステップ 10	<code>ip dhcp snooping limit rate rate</code>	(任意) インターフェイスが受信できる 1 秒あたりの DHCP パケット数を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは、レート制限は設定されません。 (注) 信頼できないインターフェイスのレート制限を 1 秒あたり 100 パケット以下に設定することを推奨します。信頼できるインターフェイスのレート制限を設定する場合、DHCP スヌーピングを使った複数の VLAN に割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になることがあります。
ステップ 11	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	<code>ip dhcp snooping verify mac-address</code>	(任意) 信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show running-config</code>	設定を確認します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用します。1 つの VLAN または VLAN の範囲で DHCP スヌーピングをディセーブルにするには、**no ip dhcp snooping vlan vlan-range** グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、**no ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを使用します。エッジスイッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットをドロップするように集約スイッチを設定するには、**no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを使用します。

次に、DHCP スヌーピングをグローバルおよび VLAN 10 でイネーブルにし、ポートのレート制限を 1 秒あたり 100 パケットに設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN および関連付けられているセカンダリ VLAN の両方に伝播します。DHCP スヌーピングがプライマリ VLAN でイネーブルの場合、セカンダリ VLAN でもイネーブルに設定されています。

DHCP スヌーピングがすでにプライマリ VLAN に設定されていて DHCP スヌーピングをセカンダリ VLAN とは異なるように設定した場合、セカンダリ VLAN の設定は有効になりません。プライマリ VLAN に DHCP スヌーピングを設定する必要があります。プライマリ VLAN に DHCP スヌーピングが設定されていない場合は、VLAN 200 などのセカンダリ VLAN に DHCP スヌーピングを設定するときに、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take effect on secondary vlan 200.DHCP Snooping configuration on secondary vlan is derived from its primary vlan.
```

show ip dhcp snooping 特権 EXEC コマンド出力では、DHCP スヌーピングがイネーブルであるプライマリおよびセカンダリ プライベート VLAN を含む、すべての VLAN を表示します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『Cisco IOS IP Configuration Guide, Release 12.2』の「Configuring DHCP」の「DHCP Configuration Task List」を参照してください。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip dhcp snooping database { flash:/filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}[/directory] /image-name.tar rtp://user@host/filename } tftp://host/filename	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 <ul style="list-style-type: none"> • flash:/filename • ftp://user:password@host/filename • http://[[username:password]@]{hostname host-ip}[/directory]/image-name.tar • rtp://user@host/filename • tftp://host/filename
ステップ3	ip dhcp snooping database timeout <i>seconds</i>	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ~ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。
ステップ4	ip dhcp snooping database write-delay <i>seconds</i>	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ~ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ5	end	特権 EXEC モードに戻ります。

DHCP スヌーピング情報の表示

	コマンド	目的
ステップ 6	<code>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</code>	(任意) DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。 <i>vlan-id</i> の範囲は 1 ~ 4904 です。 <i>seconds</i> の範囲は 1 ~ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 (注) このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 7	<code>show ip dhcp snooping database [detail]</code>	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、**no ip dhcp snooping database** グローバル コンフィギュレーション コマンドを使用します。タイムアウトまたは遅延時間の値を再セットするには、**ip dhcp snooping database timeout seconds** または **ip dhcp snooping database write-delay seconds** グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアするには、**clear ip dhcp snooping database statistics** 特権 EXEC コマンドを使用します。データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからバインディング エントリを削除するには、**no ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id** 特権 EXEC コマンドを使用します。このコマンドは、削除するエントリごとに入力します。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 26-2 に示す特権 EXEC コマンドを使用します。

表 26-2 DHCP 情報を表示するためのコマンド

コマンド	目的
<code>show ip dhcp snooping</code>	スイッチの DHCP スヌーピング設定を表示します。
<code>show ip dhcp snooping binding</code>	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
<code>show ip dhcp snooping database</code>	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
<code>show ip dhcp snooping statistics</code>	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
<code>show ip source binding</code>	動的および静的に設定されたバインディングを表示します。



(注) DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

IP ソース ガードの概要

IPSG は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッドレイヤ 2 インターフェイスでの IP トラフィックを制限するセキュリティ機能です。IP ソース ガードを使用して、ホストが、そのネイバーの IP アドレスの使用を試みた場合のトラフィック攻撃を防ぐことができます。

IP ソース ガードは、信頼できないインターフェイス上で DHCP スヌーピングがイネーブルにされている場合にイネーブルにできます。インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。ポート アクセス コントロール リスト (ACL) は、このインターフェイスに適用されます。ポート ACL は、IP ソース バインディング テーブルに送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他のトラフィックはすべて拒否します。



(注)

ポート ACL は、同じインターフェイスに影響を与えるその他のルータ ACL や VLAN マップよりも優先されます。

IP ソース バインディング テーブル バインディングは、DHCP スヌーピングにより学習されるか、または手動で設定されます (スタティック IP ソース バインディング)。このテーブルのエントリはすべて、MAC アドレスと VLAN 番号が関連付けられた IP アドレスを持ちます。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSG がサポートされているのは、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけです。送信元 IP アドレス フィルタリングや、送信元 IP および MAC アドレス フィルタリングを使用して、IPSG を設定することができます。

- 「送信元 IP アドレスのフィルタリング」 (P.26-17)
- 「送信元 IP アドレスおよび MAC アドレスのフィルタリング」 (P.26-17)
- 「スタティック ホスト用 IP ソース ガード」 (P.26-18)

送信元 IP アドレスのフィルタリング

IPSG でこのオプションがイネーブルにされている場合、IP トラフィックは、送信元 IP アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP が DHCP スヌーピング バインディング データベースのエントリ、または IP ソース バインディング テーブルのバインディングと一致する場合に、IP トラフィックを転送します。

インターフェイス上で、DHCP スヌーピング バインディング、またはスタティック IP ソース バインディングが追加、変更、または削除された場合、スイッチは IP ソース バインディングの変更を使用して、ポート ACL を変更し、このポート ACL をインターフェイスに再度適用します。

IP ソース バインディング (DHCP スヌーピングにより動的に学習された、または手動で設定されたもの) が設定されていないインターフェイス上で IPSG をイネーブルにした場合、スイッチはこのインターフェイス上で IP トラフィックすべてを拒否するポート ACL を作成し、適用します。IP ソース ガードをディセーブルにした場合、スイッチはインターフェイスからポート ACL を削除します。

送信元 IP アドレスおよび MAC アドレスのフィルタリング

IP トラフィックは、送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスと MAC アドレスが IP ソース バインディング テーブルのエントリと一致する場合だけ、トラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP トラフィックと非 IP トラフィックをフィルタリングします。IP パケット、または非 IP パケットの送信元 MAC アドレスが有効な IP ソース バインディングと一致する場合、スイッチはこのパケットを転送します。DHCP パケットを除き、その他の種類のパケットはすべて、スイッチによりドロップされます。

スイッチは、送信元 MAC アドレスのフィルタリングにポート セキュリティを使用します。ポート セキュリティ違反が発生した場合、インターフェイスはシャットダウンします。

スタティック ホスト用 IP ソース ガード



(注)

アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード (IPSG) を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。show ip device tracking all 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。



(注)

複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソース アドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティングシステムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用

できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定

- 「デフォルトの IP ソース ガード設定」(P.26-19)
- 「IP ソース ガード設定時の注意事項」(P.26-19)
- 「IP ソース ガードのイネーブル化」(P.26-20)
- 「スタティック ホスト用 IP ソース ガードの設定」(P.26-21)

デフォルトの IP ソース ガード設定

IP ソース ガードは、デフォルトではディセーブルに設定されています。

IP ソース ガード設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding mac-address vlan vlan-id ip-address interface interface-id** グローバル コンフィギュレーション コマンドを入力すると、次のエラー メッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```
- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。



(注) IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、インターフェイスの DHCP スヌーピングとポート セキュリティをイネーブルにする必要があります。また、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力して、DHCP サーバに確実に Option 82 をサポートさせる必要もあります。MAC アドレス フィルタリングとともに IP ソース ガードをイネーブルにした場合、DHCP ホストによりリースが認可されるまで、このホストの MAC アドレスは学習されません。サーバからホストにパケットを転送する場合、DHCP スヌーピングは Option 82 データを使用して、ホスト ポートを識別します。
- プライベート VLAN が設定されているインターフェイスに IP ソース ガードを設定した場合、ポート セキュリティはサポートされません。
- EtherChannels では、IP ソース ガードはサポートされません。
- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。

- Ternary Content Addressable Memory (TCAM) エントリの数が最大値を超えた場合、CPU の使用率は増加します。

IP ソース ガードのイネーブル化

特権 EXEC モードで開始します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip verify source または ip verify source port-security	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 (注) ip verify source port-security インターフェイス コンフィギュレーション コマンドを使用して、IP ソース ガードとポートセキュリティの両方をイネーブルにする場合は次の 2 点に注意してください。 <ul style="list-style-type: none"> • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 • DHCP パケットの MAC アドレスが、セキュアアドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュアアドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ip source binding mac-address vlan vlan-id ip-address interface interface-id	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip verify source [interface interface-id]	IP ソース ガードの設定を確認します。
ステップ 8	show ip source binding [ip-address] [mac-address] [dhcp-snooping static] [interface interface-id] [vlan vlan-id]	スイッチ、特定の VLAN、または特定のインターフェイス上に IP ソース バインディングを表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

送信元 IP アドレス フィルタリングによる IP ソース ガードをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP ソース バインディング エントリを削除するには、**no ip source** グローバル コンフィギュレーション コマンドを使用します。

次に、IP ソース ガードと送信元 IP および MAC フィルタリングを VLAN 10 および VLAN 11 でイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/1
Switch(config)# end
```

スタティック ホスト用 IP ソース ガードの設定

- 「レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定」(P.26-21)
- 「プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定」(P.26-25)

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定



(注)

スタティック ホスト用 IPSG を動作させるには、**ip device tracking maximum limit-number** インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または **ip device tracking maximum** をそのインターフェイスに対して設定していない場合は、スタティックホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティックホストの IPSG がプライベート VLAN ホスト ポート上で使用される場合にも適用されます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip device tracking	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switchport mode access	ポートをアクセスとして設定します。
ステップ 5	switchport access vlan vlan-id	このポート用の VLAN を設定します。

	コマンド	目的
ステップ 6	<code>ip verify source tracking port-security</code>	<p>MAC アドレス フィルタリングとともにスタティック ホスト用 IPSG をイネーブルにします。</p> <p>(注) <code>ip verify source port-security</code> インターフェイス コンフィギュレーション コマンドを使用し、IP ソース ガードとポート セキュリティの両方をイネーブルにする場合、</p> <ul style="list-style-type: none"> • DHCP サーバは Option 82 をサポートする必要があります。サポートしていない場合、クライアントには IP アドレスを割り当てるできません。 • DHCP パケットの MAC アドレスが、セキュアアドレスとして学習されることはありません。DHCP クライアントの MAC アドレスがセキュアアドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。
ステップ 7	<code>ip device tracking maximum number</code>	<p>そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ~ 10 です。最大値は 10 です。</p> <p>(注) <code>ip device tracking maximum limit-number</code> インターフェイス コンフィギュレーション コマンドを設定する必要があります。</p>
ステップ 8	<code>switchport port-security</code>	(任意) このポートのポート セキュリティをアクティブにします。
ステップ 9	<code>switchport port-security maximum value</code>	(任意) このポートに対する MAC アドレスの最大値を設定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show ip verify source interface interface-id</code>	設定を確認し、スタティック ホストに対する IPSG 許可 ACL を表示します。
ステップ 12	<code>show ip device track all [active inactive] count</code>	<p>スイッチ インターフェイス上の指定されたホストに対する IP/MAC バインディングを表示して、設定を確認します。</p> <ul style="list-style-type: none"> • all active : アクティブな IP または MAC バインディング エントリだけを表示します • all inactive : 非アクティブな IP または MAC バインディング エントリだけを表示します • all : アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します

次に、インターフェイス上でスタティック ホストを使って IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、ポート上でスタティック ホストを使って IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
```

```
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポートで IP フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end
```

```
Switch# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Gi0/3	ip trk	active	40.1.1.24		10
Gi0/3	ip trk	active	40.1.1.20		10
Gi0/3	ip trk	active	40.1.1.21		10

次に、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用してスタティック ホスト用 IPSG をイネーブルにし、インターフェイス Gi0/3 で有効な IP-MAC バインディングを確認してから、このインターフェイス上で上限に達したバインディングの数を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

```
Switch# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Gi0/3	ip-mac trk	active	40.1.1.24	00:00:00:00:03:04	1
Gi0/3	ip-mac trk	active	40.1.1.20	00:00:00:00:03:05	1
Gi0/3	ip-mac trk	active	40.1.1.21	00:00:00:00:03:06	1
Gi0/3	ip-mac trk	active	40.1.1.22	00:00:00:00:03:07	1
Gi0/3	ip-mac trk	active	40.1.1.23	00:00:00:00:03:08	1

この例は、すべてのインターフェイスに対する IP または MAC バインディング エントリをすべて表示します。CLI はアクティブ エントリと非アクティブ エントリの両方を表示します。インターフェイスでホストが学習されると、この新しいエントリは、アクティブとマークされます。このホストをこのインターフェイスから切断し、別のインターフェイスに接続すると、ホストを検出すると同時に、新しい IP または MAC バインディング エントリがアクティブとして表示されます。以前のインターフェイスでは、このホストに対する古いエントリが非アクティブとマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE

```

200.1.1.10      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.1      0001.0600.0000  9   GigabitEthernet0/2   ACTIVE
200.1.1.1      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.2      0001.0600.0000  9   GigabitEthernet0/2   ACTIVE
200.1.1.2      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.3      0001.0600.0000  9   GigabitEthernet0/2   ACTIVE
200.1.1.3      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.4      0001.0600.0000  9   GigabitEthernet0/2   ACTIVE
200.1.1.4      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.5      0001.0600.0000  9   GigabitEthernet0/2   ACTIVE
200.1.1.5      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.6      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE
200.1.1.7      0001.0600.0000  8   GigabitEthernet0/1   INACTIVE

```

この例は、すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリをすべて表示します。

```
Switch# show ip device tracking all active
```

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.1	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE

この例は、すべてのインターフェイスに対する非アクティブな IP または MAC バインディング エントリをすべて表示します。このホストはまず、GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 で移動されます。GigabitEthernet 0/1 で学習された IP または MAC バインディング エントリは非アクティブとマークされます。

```
Switch# show ip device tracking all inactive
```

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.10	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.1	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE

この例は、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの総数を表示します。

```
Switch# show ip device tracking all count
```

```
Total IP Device Tracking Host entries: 5
```

Interface	Maximum Limit	Number of Entries
Gi0/3	5	

プライベート VLAN ホスト ポート上のスタティック ホストの IP ソース ガードの設定



(注) スタティック ホストの IPSG を機能させるには、**ip device tracking maximum limit-number** インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルにイネーブルにしていない、または **ip device tracking maximum** をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。この要件は、スタティック ホストの IPSG がレイヤ 2 アクセス ポート上で使用される場合にも適用されます。

特権 EXEC モードで、次に示す手順を実行してレイヤ 2 アクセス ポート上のスタティック ホストの IPSG と IP フィルタを設定します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan vlan-id1	VLAN コンフィギュレーション モードを開始します。
ステップ 3	private-vlan primary	プライマリ VLAN をプライベート VLAN ポート上に設定します。
ステップ 4	exit	VLAN コンフィギュレーション モードを終了します。
ステップ 5	vlan vlan-id2	別の VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 6	private-vlan isolated	独立 VLAN をプライベート VLAN ポート上に設定します。
ステップ 7	exit	VLAN コンフィギュレーション モードを終了します。
ステップ 8	vlan vlan-id1	VLAN コンフィギュレーション モードを開始します。
ステップ 9	private-vlan association 201	VLAN を独立プライベート VLAN ポートに関連付けます。
ステップ 10	exit	VLAN コンフィギュレーション モードを終了します。
ステップ 11	interface fastEthernet interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	switchport mode private-vlan host	(任意) ポートをプライベート VLAN ホストとして設定します。
ステップ 13	switchport private-vlan host-association vlan-id1 vlan-id2	(任意) このポートに、対応するプライベート VLAN を関連付けます。
ステップ 14	ip device tracking maximum number	このポートに対して IP デバイス トラッキング テーブルに保持できるスタティック IP の数の上限を設定します。最大値は 10 です。 (注) スタティック ホストの IPSG を機能させるには、 ip device tracking maximum number インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	ip verify source tracking [port-security]	このポート上のスタティック ホストの IPSG と MAC アドレス フィルタリングをアクティブにします。

■ IP ソース ガードの設定

	コマンド	目的
ステップ 16	end	インターフェイス コンフィギュレーション モードを終了します。
ステップ 17	show ip device tracking all	設定を確認します。
ステップ 18	show ip verify source interface <i>interface-id</i>	IP ソース ガードの設定を確認します。スタティック ホストの IPSG の許可 ACL を表示します。

次に、プライベート VLAN ホスト ポート上でスタティック ホストの IPSG と IP フィルタをイネーブルにする例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking
```

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
40.1.1.24	0000.0000.0304	200	FastEthernet0/3	ACTIVE
40.1.1.20	0000.0000.0305	200	FastEthernet0/3	ACTIVE
40.1.1.21	0000.0000.0306	200	FastEthernet0/3	ACTIVE
40.1.1.22	0000.0000.0307	200	FastEthernet0/3	ACTIVE
40.1.1.23	0000.0000.0308	200	FastEthernet0/3	ACTIVE

出力には、インターフェイス Fa0/3 上で学習された 5 つの有効な IP-MAC バインディングが表示されています。プライベート VLAN の場合は、バインディングにはプライマリ VLAN ID が関連付けられます。したがって、この例ではプライマリ VLAN ID である 200 が表に表示されています。

```
Switch# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Fa0/3	ip trk	active	40.1.1.23		200
Fa0/3	ip trk	active	40.1.1.24		200
Fa0/3	ip trk	active	40.1.1.20		200
Fa0/3	ip trk	active	40.1.1.21		200
Fa0/3	ip trk	active	40.1.1.22		200
Fa0/3	ip trk	active	40.1.1.23		201
Fa0/3	ip trk	active	40.1.1.24		201
Fa0/3	ip trk	active	40.1.1.20		201
Fa0/3	ip trk	active	40.1.1.21		201
Fa0/30/3	ip trk	active	40.1.1.22		201

この出力からは、5 つの有効な IP-MAC バインディングはプライマリとセカンダリの両方の VLAN 上にあることがわかります。

IP ソース ガード情報の表示

IP ソース ガード情報を表示するには、表 26-3 の特権 EXEC コマンドを 1 つ以上使用します。

表 26-3 IP ソース ガード情報を表示するためのコマンド

コマンド	目的
show ip device tracking	すべてのインターフェイスに対してアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチ上の IP ソース バインディングを表示します。
show ip verify source	スイッチ上の IP ソース ガード設定を表示します。

DHCP サーバ ポートベースのアドレス割り当ての概要

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代替りのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代替りのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

DHCP サーバ ポートベースのアドレス割り当ての設定

ここでは、次の設定情報について説明します。

- 「ポートベースのアドレス テーブルのデフォルト設定」 (P.26-29)
- 「ポートベースのアドレス割り当て設定時の注意事項」 (P.26-29)
- 「DHCP サーバ ポートベースのアドレス割り当てのイネーブル化」 (P.26-29)

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当て設定時の注意事項を説明します。

- 1つのポートにつき割り当てることができる IP アドレスは 1 つだけです。
- 専用アドレス（事前に設定されたアドレス）は、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドではクリアできません。
- 事前に設定されたアドレスは、通常の動的な IP アドレス割り当てからは自動的に除外されます。ホスト プールでは、事前に設定されたアドレスは使用できませんが、1 つの DHCP アドレス プールに対して複数のアドレスを事前に設定することはできます。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip dhcp use subscriber-id client-id	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ3	ip dhcp subscriber-id interface-name	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。
ステップ4	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ5	ip dhcp server use subscriber-id client-id	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show running config	入力内容を確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP サーバポートベースのアドレス割り当ての設定

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。DHCP プールから事前に設定された予約への割り当てを制限するために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。このコマンドの入力により、ユーザは、共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視する DHCP プールを持つスイッチのグループを設定できます。

IP アドレスを事前に割り当て、これをインターフェイス名で識別されるクライアントに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dhcp pool poolname	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。
ステップ 3	network network-number [mask /prefix-length]	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。
ステップ 4	address ip-address client-id string [ascii]	インターフェイス名で指定された DHCP クライアントの IP アドレスを予約します。 <i>string</i> : ASCII 値、または 16 進数値のいずれかです。
ステップ 5	reserved-only	(任意) DHCP アドレス プールでは、予約されたアドレスだけを使用します。デフォルトでは、プールアドレスは制限されません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip dhcp pool	DHCP プール設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP ポートベースのアドレス割り当てをディセーブルにするには、**no ip dhcp use subscriber-id client-id** グローバル コンフィギュレーション コマンドを使用します。加入者 ID の自動生成をディセーブルにするには、**no ip dhcp subscriber-id interface-name** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で加入者 ID をディセーブルにするには、**no ip dhcp server use subscriber-id client-id** インターフェイス コンフィギュレーション コマンドを使用します。

DHCP プールから IP アドレスの予約を削除するには、**no address ip-address client-id string** DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを非制限に変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージ内のクライアント ID フィールドを一切無視して、その代わりに、加入者の ID を使用しています。加入者 ID はインターフェイスのショート名に基づきます。また、クライアントの事前割り当てされた IP アドレスは 10.1.1.7 です。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
```

```

version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
  address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>

```

次に、事前割り当てされたアドレスが DHCP プールに正常に予約された例を示します。

```

switch# show ip dhcp pool dhcppool
Pool dhcp pool:
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 0
  Excluded addresses : 4
  Pending event : none
  1 subnet is currently in the pool:
  Current index  IP address range      Leased/Excluded/Total
  10.1.1.1       10.1.1.1 - 10.1.1.254    0 / 4 / 254
  1 reserved address is currently in the pool
  Address      Client
  10.1.1.7    Et1/0

```

DHCP サーバポートベースのアドレス割り当て機能の設定の詳細については、Cisco.com にアクセスし、[Search] フィールドに「Cisco IOS IP Addressing Services」と入力して、Cisco IOS ソフトウェア マニュアルを参照してください。マニュアルは次の URL から入手できます。

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバポートベースのアドレス割り当ての表示

DHCP サーバポートベースのアドレス割り当て情報を表示するには、表 26-4 の特権 EXEC コマンドを 1 つ以上使用します。

表 26-4 DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
<code>show interface interface id</code>	特定のインターフェイスのステータスおよび設定を表示します。
<code>show ip dhcp pool</code>	DHCP アドレス プールを表示します。
<code>show ip dhcp binding</code>	Cisco IOS DHCP サーバでのアドレス バインディングを表示します。

■ DHCP サーバポートベースのアドレス割り当ての表示



CHAPTER 27

ダイナミック ARP インспекションの設定



(注)

この章では、IE 3000 スイッチにダイナミック アドレス解決プロトコル インспекション (ダイナミック ARP インспекション) を設定する方法について説明します。この機能により、同じ VLAN (仮想 LAN) 内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

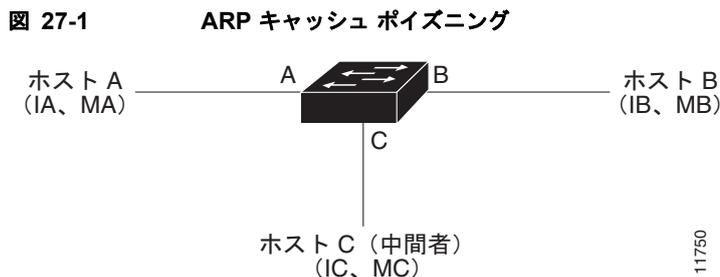
この章の内容は、次のとおりです。

- 「[ダイナミック ARP インспекションの概要](#)」 (P.27-1)
- 「[ダイナミック ARP インспекションの設定](#)」 (P.27-5)
- 「[ダイナミック ARP インспекション情報の表示](#)」 (P.27-15)

ダイナミック ARP インспекションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求を受信されなかった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 27-1 に、ARP キャッシュ ポイズニングの例を示します。



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA (または IB) で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。おなじみの 中間者攻撃です。

ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の間接攻撃から保護することができます。

ダイナミック ARP インспекションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

ダイナミック ARP インспекションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

ip arp inspection vlan vlan-range グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インспекションをイネーブルにすることができます。設定の詳細については、「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.27-7) を参照してください。

非 DHCP 環境では、ダイナミック ARP インспекションは、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP Access Control List (ACL; アクセス コントロール リスト) と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list acl-name** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.27-9) を参照してください。スイッチはドロップされたパケットをログに記録します。ログ バッファの詳細については、「廃棄パケットのロギング」(P.27-5) を参照してください。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インспекションを設定することができます。このためには、**ip arp inspection validate {[src-mac] [dst-mac] [ip]}** グローバル コンフィギュレーション コマンドを使用します。詳細については、「確認検査の実行」(P.27-12) を参照してください。

インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インспекションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インспекションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インспекションの検証プロセスを受けます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

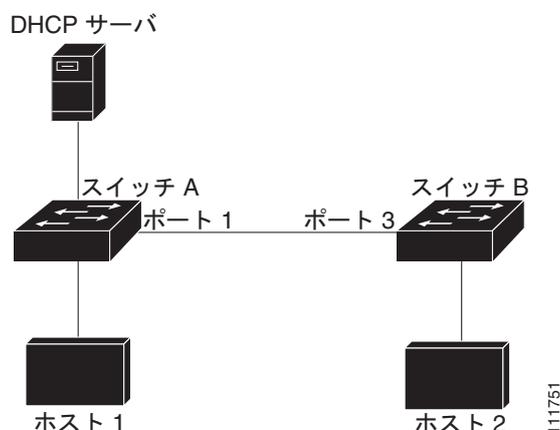


注意

信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 27-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インспекションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットは、スイッチ B によりドロップされます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 27-2 ダイナミック ARP インспекションのためにイネーブルにされた VLAN 上の ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティホールが生じます。スイッチ A でダイナミック ARP インспекションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インспекションを実行している場合でも発生します。

ダイナミック ARP インспекションは、ダイナミック ARP インспекションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インспекションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インспекションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インспекションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インспекションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インспекションを実行するスイッチを設定します。そのようなバインディングをレイヤ 3 で判別できない場合、ダイナミック ARP インспекションを実行しているスイッチを、ダイナミック ARP インспекションを実行していないスイッチから分離します。設定の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.27-9) を参照してください。



(注) DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒 (pps) です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、`ip arp inspection limit` インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを `errdisable` ステートにします。ユーザが介入するまで、ポートはこの状態を維持します。`errdisable recovery` グローバル コンフィギュレーション コマンドを使用すると、`errdisable` ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。

設定の詳細については、「[着信 ARP パケットのレート制限](#)」(P.27-11) を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が `ip arp inspection filter vlan` グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄パケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

`ip arp inspection log-buffer` グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、`ip arp inspection vlan logging` グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「[ログ バッファの設定](#)」(P.27-13) を参照してください。

ダイナミック ARP インспекションの設定

ここでは、次の設定について説明します。

- 「[ダイナミック ARP インспекションのデフォルト設定](#)」(P.27-6)
- 「[ダイナミック ARP インспекション設定時の注意事項](#)」(P.27-6)
- 「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.27-7) (DHCP 環境では必須)
- 「[非 DHCP 環境での ARP ACL の設定](#)」(P.27-9) (非 DHCP 環境では必須)
- 「[着信 ARP パケットのレート制限](#)」(P.27-11) (任意)
- 「[確認検査の実行](#)」(P.27-12) (任意)
- 「[ログ バッファの設定](#)」(P.27-13) (任意)

ダイナミック ARP インспекションのデフォルト設定

表 27-1 に、ダイナミック ARP インспекションのデフォルト設定を示します。

表 27-1 ダイナミック ARP インспекションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インспекション。	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは <code>untrusted</code> 。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	ダイナミック ARP インспекションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギングレート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

ダイナミック ARP インспекション設定時の注意事項

ダイナミック ARP インспекション設定時の注意事項は次のとおりです。

- ダイナミック ARP インспекションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インспекションは、ダイナミック ARP インспекションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インспекションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インспекションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。コンフィギュレーションについては、[第 26 章「DHCP 機能と IP ソース ガード機能の設定」](#)を参照してください。

DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。

- ダイナミック ARP インспекションは、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポート上でサポートされています。



(注) RSPAN VLAN では、ダイナミック ARP インспекションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インспекションをイネーブルにすると、ダイナミック ARP インспекション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャンネルに結合するには、この物理ポートとチャンネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャンネル内で中断状態のままとなります。ポート チャンネルは、チャンネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャンネルの信頼状態と一致する必要はありません。

逆に、ポート チャンネルで信頼状態を変更すると、スイッチは、チャンネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- ポート チャンネルの動作レートは、チャンネル内のすべての物理ポートによる累積値です。たとえば、ポート チャンネルの ARP レート制限を 400 pps に設定すると、このチャンネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートの着信 ARP パケットのレートは、全チャンネル メンバーからのパケットの着信レートを合計したものです。EtherChannel ポートのレート制限は、各チャンネル ポート メンバが受信する ARP パケットのレートを確認してから設定してください。

物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャンネルの設定に照合して検査されます。ポート チャンネル上のレート制限設定は、物理ポートの設定に依存しません。

EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャンネル（すべての物理ポートを含む）は `errdisable` ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インспекションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、`ip arp inspection limit none` インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが `errdisable` ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。
- スイッチで、ダイナミック ARP インспекションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

DHCP 環境でのダイナミック ARP インспекションの設定

この手順では、2 つのスイッチがダイナミック ARP インспекションをサポートしているときに、この機能を設定する方法を示します。図 27-2 (P.27-4) に示すとおり、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています。スイッチは両方とも、ホストの配置されている VLAN 1 でダイナミック ARP インспекションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。



(注) 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション DHCP スヌーピング バインディング データベースのエントリに依存します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。コンフィギュレーションについては、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。

スイッチの 1 つだけがこの機能をサポートしている場合にダイナミック ARP インспекションを設定する方法の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.27-9) を参照してください。

ダイナミック ARP インспекションを設定するには、特権 EXEC モードで次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	<code>show cdp neighbors</code>	スイッチ間の接続を確認します。
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>ip arp inspection vlan <i>vlan-range</i></code>	VLAN 単位で、ダイナミック ARP インспекションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インспекションはディセーブルになっています。 <i>vlan-range</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	<code>interface <i>interface-id</i></code>	もう 1 つのスイッチに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>ip arp inspection trust</code>	スイッチ間の接続を、信頼できるものに設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、 <code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」(P.27-13) を参照してください。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip arp inspection interfaces</code> <code>show ip arp inspection vlan <i>vlan-range</i></code>	ダイナミック ARP インспекションの設定を確認します。
ステップ 8	<code>show ip dhcp snooping binding</code>	DHCP バインディングを確認します。
ステップ 9	<code>show ip arp inspection statistics vlan <i>vlan-range</i></code>	ダイナミック ARP インспекション統計情報を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP インспекションをディセーブルにするには、**no ip arp inspection vlan vlan-range** グローバル コンフィギュレーション コマンドを使用します。インターフェイスを **untrusted** ステータスに戻すには、**no ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、VLAN 1 のスイッチ A でダイナミック ARP インспекションを設定する方法を示します。スイッチ B でも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境での ARP ACL の設定

この手順は、[図 27-2 \(P.27-4\)](#) に示すスイッチ B がダイナミック ARP インспекション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インспекションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定して VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A 上で ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境では必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	arp access-list acl-name	ARP ACL を定義し、ARP アクセス リスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されません。 (注) ARP アクセス リストの末尾に暗黙的な deny ip any mac any コマンドが指定されています。
ステップ 3	permit ip host sender-ip mac host sender-mac [log]	指定されたホスト（ホスト 2）からの ARP パケットを許可します。 <ul style="list-style-type: none"> • <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。 • <i>sender-mac</i> には、ホスト 2 の MAC アドレスを入力します。 • (任意) パケットが Access Control Entry (ACE; アクセスコントロール エントリ) と一致するときに、ログ バッファにこのパケットをログするには、log を指定します。 ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで matchlog キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「ログ バッファの設定」(P.27-13) を参照してください。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 5 <code>ip arp inspection filter arp-acl-name vlan vlan-range [static]</code>	<p>ARP ACL を VLAN に適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。</p> <ul style="list-style-type: none"> • <code>arp-acl-name</code> には、ステップ 2 で作成した ACL の名前を指定します。 • <code>vlan-range</code> には、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 • (任意) <code>static</code> を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 <p>このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。</p> <p>IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセスリストで許可された場合だけに許可されます。</p>
ステップ 6 <code>interface interface-id</code>	<p>スイッチ B に接続するスイッチ A インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。</p>
ステップ 7 <code>no ip arp inspection trust</code>	<p>スイッチ B に接続されたスイッチ A インターフェイスを信頼できないものとして設定します。</p> <p>デフォルトでは、すべてのインターフェイスは信頼できません。</p> <p>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、<code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」(P.27-13) を参照してください。</p>
ステップ 8 <code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ 9 <code>show arp access-list [acl-name]</code> <code>show ip arp inspection vlan vlan-range</code> <code>show ip arp inspection interfaces</code>	<p>設定を確認します。</p>
ステップ 10 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に接続された ARP ACL を削除するには、**no ip arp inspection filter arp-acl-name vlan vlan-range** グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A で ARP ACL *host2* を設定して、ホスト 2 (IP アドレス 1.1.1.1、および MAC アドレス 0001.0001.0001) からの ARP パケットを許可し、この ACL を VLAN 1 に適用してから、スイッチ A のポート 1 を信頼できないものに設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを **errdisable** ステートにします。**errdisable** 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。



(注)

インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポート、および EtherChannel ポートに対するレート制限設定時の注意事項については、「[ダイナミック ARP インспекション設定時の注意事項](#)」(P.27-6) を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	レート制限されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	ip arp inspection limit {rate <i>pps</i> [<i>burst interval seconds</i>] none}	<p>インターフェイスでの着信 ARP 要求および応答のレートを制限します。</p> <p>デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • rate pps には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ~ 2048 pps です。 • (任意) burst interval seconds は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔 (秒) を指定します。指定できる範囲は 1 ~ 15 です。 • rate none では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	errdisable recovery cause arp-inspection interval interval	<p>(任意) ダイナミック ARP インспекション errdisable ステートからのエラー回復をイネーブルにします。</p> <p>デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。</p> <p>interval interval には、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ~ 86400 です。</p>
ステップ 6	exit	特権 EXEC モードに戻ります。
ステップ 7	show ip arp inspection interfaces show errdisable recovery	設定値を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのレート制限設定に戻るには、**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP インспекションのエラー回復をディセーブルにするには、**no errdisable recovery cause arp-inspection** グローバル コンフィギュレーション コマンドを使用します。

確認検査の実行

ダイナミック ARP インспекションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定の検証を実行するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip arp inspection validate</code> <code>{[src-mac] [dst-mac] [ip]}</code>	<p>着信 ARP パケットに対して特定の検証を実行します。デフォルトでは、検証は実行されません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • src-mac では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • dst-mac では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • ip では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 <p>少なくとも 1 つのキーワードを指定する必要があります。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番目のコマンドによって src および dst mac の検証がディセーブルになります。</p>
ステップ3	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ip arp inspection vlan</code> <code>vlan-range</code>	設定値を確認します。
ステップ5	<code>copy running-config</code> <code>startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

検証をディセーブルにするには、`no ip arp inspection validate [src-mac] [dst-mac] [ip]` グローバル コンフィギュレーション コマンドを使用します。転送されたパケット、ドロップされたパケット、MAC および IP 検証に失敗したパケットの統計を表示するには、`show ip arp inspection statistics` 特権 EXEC コマンドを使用します。

ログ バッファの設定

スイッチがパケットをドロップすると、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

ログバッファ エントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同じ ARP パラメータを使用して同じ VLAN 上で多数のパケットを受信した場合、スイッチはこれらのパケットを組み合わせて 1 つのエントリとしてログ バッファに格納し、エントリとして 1 つのシステム メッセージを生成します。

ログバッファでオーバーフローが生じた場合は、1つのログイベントがログバッファ内に収まらなかったことを意味し、**show ip arp inspection log** 特権 EXEC コマンドによる出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに -- が表示されます。このエントリに対しては、その他の統計情報は表示されません。出力にこのようなエントリが表示される場合、ログバッファ内のエントリ数を増やすか、ロギングレートを増やします。

ログバッファを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 ip arp inspection log-buffer {entries number logs number interval seconds}	<p>ダイナミック ARP インспекション ログバッファを設定します。</p> <p>デフォルトでは、ダイナミック ARP インспекションがイネーブル化されると、拒否またはドロップされた ARP パケットが記録されます。ログエントリ数は、32 です。システム メッセージ数は、毎秒 5 つに制限されます。ロギングレート インターバルは、1 秒です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • entries number は、バッファに記録されるエントリ数を表します。指定できる範囲は 0 ~ 1024 です • logs number interval seconds は、指定されたインターバルでシステムメッセージを生成するエントリの数を表します。 <p>logs number に指定できる範囲は 0 ~ 1024 です。0 は、エントリはログバッファ内に入力されますが、システムメッセージが生成されないことを意味します。</p> <p>指定できる interval seconds の範囲は 0 ~ 86400 秒 (1 日) です。0 は、システムメッセージがただちに生成されることを意味します。この場合、ログバッファは常に空となります。</p> <p>インターバル値を 0 に設定すると、ログ値 0 は上書きされます。</p> <p>logs および interval の設定は、相互に作用します。logs number X が interval seconds Y より大きい場合、X 割る Y (X/Y) のシステムメッセージが毎秒送信されます。そうでない場合、1 つのシステムメッセージが Y 割る X (Y/X) 秒ごとに送信されます。</p>

コマンド	目的
ステップ3 <code>ip arp inspection vlan <i>vlan-range</i> logging {<i>acl-match</i> {<i>matchlog</i> <i>none</i>} <i>dhcp-bindings</i> {<i>all</i> <i>none</i> <i>permit</i>}}</code>	<p>VLAN 単位で記録するパケットのタイプを制御します。デフォルトでは、拒否またはドロップされたパケットは、すべて記録されます。ログに記録されるという表現は、エントリがログバッファに格納され、システムメッセージが生成されることを意味しています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <code>vlan-range</code> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <code>acl-match matchlog</code> は、ACE ログ設定に基づいてパケットをログに記録します。このコマンドに <code>matchlog</code> キーワードを指定して、さらに <code>permit</code> または <code>deny</code> ARP アクセス リスト コンフィギュレーション コマンドに <code>log</code> キーワードを指定すると、ACL によって許可または拒否された ARP パケットが記録されます。 <code>acl-match none</code> では、ACL に一致するパケットは記録されません。 <code>dhcp-bindings all</code> では、DHCP バインディングに一致するパケットがすべて記録されます。 <code>dhcp-bindings none</code> では、DHCP バインディングに一致するパケットは記録されません。 <code>dhcp-bindings permit</code> では、DHCP バインディングが許可されたパケットが記録されます。
ステップ4 <code>exit</code>	特権 EXEC モードに戻ります。
ステップ5 <code>show ip arp inspection log</code>	設定値を確認します。
ステップ6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのログ バッファ設定に戻るには、`no ip arp inspection log-buffer {entries | logs}` グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻るには、`no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}` グローバル コンフィギュレーション コマンドを使用します。ログ バッファをクリアするには、`clear ip arp inspection log` 特権 EXEC コマンドを使用します。

ダイナミック ARP インспекション情報の表示

ダイナミック ARP インспекション情報を表示するには、表 27-2 に記載された特権 EXEC コマンドを使用します。

表 27-2 ダイナミック ARP インспекション情報を表示するためのコマンド

コマンド	説明
<code>show arp access-list [<i>acl-name</i>]</code>	ARP ACL についての詳細情報を表示します。
<code>show ip arp inspection interfaces [<i>interface-id</i>]</code>	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
<code>show ip arp inspection vlan <i>vlan-range</i></code>	指定された VLAN のダイナミック ARP インспекションの設定および動作ステータスを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた (アクティブ) VLAN だけの情報を表示します。

■ ダイナミック ARP インспекション情報の表示

ダイナミック ARP インспекションの統計をクリア、または表示するには、表 27-3 に記載された特権 EXEC コマンドを使用します。

表 27-3 ダイナミック ARP インспекション統計をクリアまたは表示するためのコマンド

コマンド	説明
<code>clear ip arp inspection statistics</code>	ダイナミック ARP インспекション統計情報をクリアします。
<code>show ip arp inspection statistics [vlan vlan-range]</code>	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた (アクティブ) VLAN だけの情報を表示します。

`show ip arp inspection statistics` コマンドでは、スイッチは信頼されたダイナミック ARP インспекション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP インспекションのログ情報をクリア、または表示するには、表 27-4 に記載された特権 EXEC コマンドを使用します。

表 27-4 ダイナミック ARP インспекション ログ情報をクリアまたは表示するためのコマンド

コマンド	説明
<code>clear ip arp inspection log</code>	ダイナミック ARP インспекション ログ バッファをクリアします。
<code>show ip arp inspection log</code>	ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。

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



CHAPTER 28

IGMP スヌーピングおよび MVR の設定

この章では、ローカルの IGMP スヌーピング アプリケーション、マルチキャスト VLAN レジストレーション (MVR) などの IE 3000 スイッチにインターネット グループ管理プロトコル (IGMP) スヌーピングを設定する手順について説明します。また、IGMP フィルタリングを使用したマルチキャスト グループ メンバーシップの制御と、IGMP スロットリング アクションの設定手順についても説明します。



(注) IP Version 6 (IPv6) トラフィックでは、Multicast Listener Discovery (MLD) スヌーピングが IPv4 トラフィックに対する IGMP スヌーピングと同じ機能を実行します。MLD スヌーピングの詳細については、[第 44 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。



(注) この章で使用されるコマンドの構文と使用方法の詳細については、このリリースのスイッチ コマンド リファレンスと、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』の「IP Multicast Routing Commands」を参照してください。このリリースは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にあります。

この章で説明する内容は、次のとおりです。

- [「IGMP スヌーピングの概要」 \(P.28-2\)](#)
- [「IGMP スヌーピングの設定」 \(P.28-7\)](#)
- [「IGMP スヌーピング情報の表示」 \(P.28-16\)](#)
- [「MVR の概要」 \(P.28-18\)](#)
- [「MVR の設定」 \(P.28-20\)](#)
- [「MVR 情報の表示」 \(P.28-24\)](#)
- [「IGMP フィルタリングおよびスロットリングの設定」 \(P.28-25\)](#)
- [「IGMP フィルタリングおよび IGMP スロットリング設定の表示」 \(P.28-30\)](#)



(注) IGMP スヌーピング、MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理することもできますし、スタティック IP アドレスを使用することもできます。

IGMP スヌーピングの概要

レイヤ 2 スイッチは IGMP スヌーピングを使用して、レイヤ 2 インターフェイスを動的に設定し、マルチキャストトラフィックが IP マルチキャストデバイスと対応付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャストトラフィックのフラッディングを制限できます。名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャストグループとメンバーポートを追跡する必要があります。特定のマルチキャストグループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブルエントリからホストポートを削除します。マルチキャストクライアントから IGMP メンバーシップレポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。



(注) IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャストルータは、すべての VLAN に一般クエリを定期的送信します。このマルチキャストトラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC アドレスに基づくグループではなく、IP マルチキャストグループに基づくブリッジをサポートしています。マルチキャスト MAC アドレスに基づくグループの場合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。スイッチでは IP マルチキャストグループを使用するので、アドレスエイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャストグループは動的に学習されます。ただし、`ip igmp snooping vlan vlan-id static ip_address interface interface-id` グローバル コンフィギュレーション コマンドを使用すると、マルチキャストグループを静的に設定できます。グループメンバーシップをマルチキャストグループアドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャストグループメンバーシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャストトラフィックはルーティングする必要がないのでマルチキャストインターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピングクエリを設定できます。IGMP スヌーピングクエリアの詳細については、「[IGMP スヌーピングクエリアの設定](#)」(P.28-14) を参照してください。

ポートスパンニングツリー、ポートグループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャストグループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

- 「[IGMP のバージョン](#)」(P.28-3)
- 「[マルチキャストグループへの加入](#)」(P.28-3)
- 「[マルチキャストグループからの脱退](#)」(P.28-5)
- 「[即時脱退](#)」(P.28-5)
- 「[IGMP 脱退タイマーの設定](#)」(P.28-6)
- 「[IGMP レポート抑制](#)」(P.28-6)

IGMP のバージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これら 3 つのバージョンは、スイッチ上でそれぞれ相互運用できます。たとえば、IGMPv2 スイッチ上で IGMP スヌーピングがイネーブルの場合、このスイッチが IGMPv3 レポートをホストから受信すると、この IGMPv3 レポートをマルチキャスト ルータへ転送できます。



(注) スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support (BISS) をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッドは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。



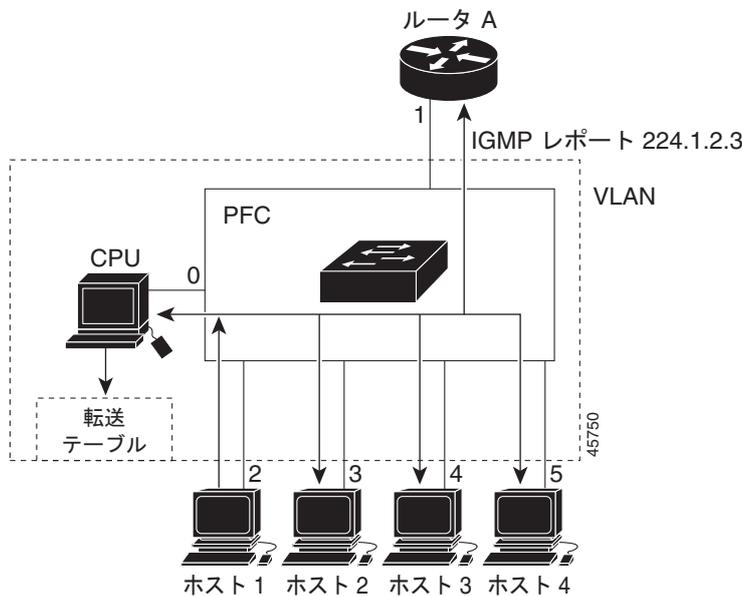
(注) IGMP フィルタリングまたは MVR が実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの送受信を行うことができます。

マルチキャスト グループへの加入

スイッチに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリーを受信したスイッチは、そのクエリーを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはスイッチに Join メッセージを送信することによって応答します。スイッチの CPU は、そのグループのマルチキャスト転送テーブル エントリがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。図 28-1 を参照してください。

図 28-1 最初の IGMP Join メッセージ



ルータ A がスイッチに一般クエリを送り、スイッチはそのクエリをポート 2 ~ 5、つまり同一 VLAN のすべてのメンバに転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート (IGMP Join メッセージ) をマルチキャストします。スイッチの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します (表 28-1 を参照)。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 28-1 IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

スイッチのハードウェアは、マルチキャスト グループの他のパケットと IGMP 情報パケットを区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛での、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

別のホスト (たとえば、ホスト 4) が同じグループに非送信請求の IGMP Join メッセージを送信する場合 (図 28-2 を参照)、CPU はメッセージを受信して、転送テーブルにホスト 4 のポート番号を追加します (表 28-2 を参照)。転送テーブルによって、CPU だけに IGMP メッセージが転送されるので、スイッチ上の他のポートにメッセージがフラッドされることはありません。既知のマルチキャストトラフィックはすべて、CPU ではなくグループに転送されます。

図 28-2 2 番めのホストのマルチキャスト グループへの加入

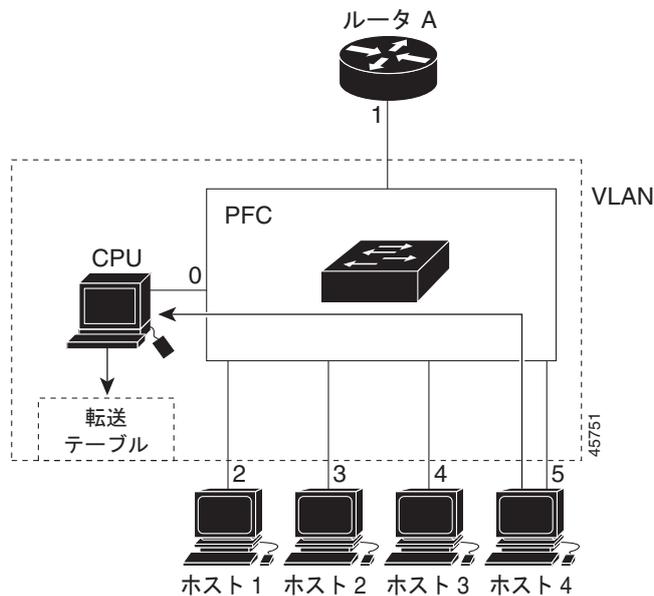


表 28-2 更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2、5

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリーを定期的を送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャストトラフィックを受信しなければならない場合、ルータは VLAN に引き続き、マルチキャストトラフィックを転送します。スイッチは、その IGMP スヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャストグループトラフィックを転送します。

ホストがマルチキャストグループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したスイッチは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャストトラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチからインターフェイスにグループ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマル

マルチキャスト グループのマルチキャスト ツリーからプルーンされます。即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。



(注)

即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。1 つのポートに複数のホストが接続されている VLAN で即時脱退機能をイネーブルにすると、一部のホストが誤って切断される可能性があります。

設定手順については、「[IGMP 即時脱退のイネーブル化](#)」(P.28-11) を参照してください。

IGMP 脱退タイマーの設定

まだ指定のマルチキャスト グループに関心があるかどうかを確認するために、グループ固有のクエリーを送信した後のスイッチの待機時間を設定できます。IGMP 脱退応答時間は、100 ~ 5000 ミリ秒の間で設定できます。タイマーはグローバルにまたは VLAN 単位で設定できますが、VLAN に脱退時間を設定すると、グローバルに設定した脱退時間は上書きされます。

設定手順については、「[IGMP 脱退タイマーの設定](#)」(P.28-11) を参照してください。

IGMP レポート抑制



(注)

IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル (デフォルト) である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、グループのすべてのホストからすべてのマルチキャスト ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。設定手順については、「[IGMP レポート抑制のディセーブル化](#)」(P.28-16) を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。ここでは、次の設定について説明します。

- 「IGMP スヌーピングのデフォルト設定」 (P.28-7)
- 「IGMP スヌーピングのイネーブル化およびディセーブル化」 (P.28-7)
- 「スヌーピング方法の設定」 (P.28-8)
- 「マルチキャスト ルータ ポートの設定」 (P.28-9)
- 「グループに加入するホストの静的な設定」 (P.28-10)
- 「IGMP 即時脱退のイネーブル化」 (P.28-11)
- 「IGMP 脱退タイマーの設定」 (P.28-11)
- 「TCN 関連のコマンドの設定」 (P.28-12)
- 「IGMP スヌーピング クェリアの設定」 (P.28-14)
- 「IGMP レポート抑制のディセーブル化」 (P.28-16)

IGMP スヌーピングのデフォルト設定

表 28-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 28-3 IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	未設定
マルチキャスト ルータの学習 (スヌーピング) 方式	PIM-DVMRP
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN ¹ フラッド クェリー カウント	2
TCN クェリー送信要求	ディセーブル
IGMP スヌーピング クェリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN = Topology Change Notification (トポロジ変更通知)

IGMP スヌーピングのイネーブル化およびディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブルです。グローバルにイネーブルまたはディセーブルに設定されている場合、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルです。デフォルトでは、IGMP スヌーピングはすべての VLAN でイネーブルですが、VLAN 単位で IGMP スヌーピングをイネーブルおよびディセーブルに設定できます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングよりも優先されます。グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチ上で IGMP スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping</code>	既存のすべての VLAN インターフェイスで、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN インターフェイス上で IGMP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i></code>	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan *vlan-id*** グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol Independent Multicast (PIM) パケット、および Distance Vector Multicast Routing Protocol (DVMRP) パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol (CGMP) パケットの待ち受け
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。デフォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングします。CGMP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan *vlan-id* mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、その他の CGMP パケットは待ち受けません。PIM パケットと DVMRP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp** グローバル コンフィギュレーション コマンドを使用します。



(注) 学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャスト ルータがない場合は、**ip cgmp router-only** コマンドを入力し、ルータに動的にアクセスする必要があります。詳細については、[第 50 章「IP マルチキャスト ルーティングの設定」](#)を参照してください。

VLAN インターフェイスがマルチキャスト ルータに動的にアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp pim-dvmrp}	VLAN で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 マルチキャスト ルータの学習方法を指定します。 <ul style="list-style-type: none"> • cgmp : CGMP パケットを待ち受けます。この方法は、制御トラフィックを減らす場合に有用です。 • pim-dvmrp : IGMP クエリーおよび PIM パケットと DVMRP パケットをスヌーピングします。これはデフォルトです。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの学習方式に戻すには、**no ip igmp snooping vlan *vlan-id* mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。

次に、CGMP パケットを学習方式として使用するように IGMP スヌーピングを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加 (マルチキャスト ルータに静的な接続を追加) するには、スイッチ上で **ip igmp snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。



(注) マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

マルチキャスト ルータへの静的な接続をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></code>	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。 <ul style="list-style-type: none"> 指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネルの範囲は 1 ~ 6 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	VLAN インターフェイス上で IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、`no ip igmp snooping vlan vlan-id mrouter interface interface-id` グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# end
```

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i></code>	マルチキャスト グループのメンバとしてレイヤ 2 ポートを静的に設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。 <i>ip-address</i> は、グループの IP アドレスです。 <i>interface-id</i> は、メンバ ポートです。物理インターフェイスまたはポート チャネル (1 ~ 6) に設定できます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip igmp snooping groups</code>	メンバ ポートおよび IP アドレスを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャストグループからレイヤ 2 ポートを削除するには、**no ip igmp snooping vlan *vlan-id* static ip-address interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。

次に、ポート上のホストを静的に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。



(注) 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。

IGMP 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan <i>vlan-id</i> immediate-leave	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping vlan <i>vlan-id</i>	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN 上で IGMP 即時脱退をディセーブルにするには、**no ip igmp snooping vlan *vlan-id* immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP 脱退タイマーの設定

IGMP 脱退タイマーを設定するときには、次の注意事項に従ってください。

- 脱退時間はグローバルまたは VLAN 単位で設定できます。
- VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
- デフォルトの脱退時間は 1000 ミリ秒です。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。
- ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

IGMP 脱退タイマーの設定をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping last-member-query-interval time</code>	グローバルに IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 32768 ミリ秒です。デフォルト値は 1000 秒です。
ステップ 3	<code>ip igmp snooping vlan vlan-id last-member-query-interval time</code>	(任意) VLAN インターフェイス上で、IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 32768 ミリ秒です。 (注) VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp snooping</code>	(任意) 設定された IGMP 脱退タイマーを表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、**no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN から IGMP 脱退タイマーの設定を削除するには、**no ip igmp snooping vlan vlan-id last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

TCN 関連のコマンドの設定

ここでは、TCN イベント中にフラッディングしたマルチキャスト トラフィックを制御する方法を説明します。

- 「TCN イベント後のマルチキャスト フラッディング時間の制御」(P.28-12)
- 「フラッディング モードからの回復」(P.28-13)
- 「TCN イベント中のマルチキャスト フラッディングのディセーブル化」(P.28-14)

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、TCN イベント後にフラッディングするマルチキャスト トラフィックの時間を制御できます。このコマンドは、TCN イベント後にフラッディングするマルチキャスト データのトラフィックに対し、一般クエリー数を設定します。クライアントが場所を変更することで同ポートの受信者がブロックされた後、現在転送中の場合、またはポートが Leave メッセージを送信せずにダウンした場合などが、TCN イベントに該当します。

ip igmp snooping tcn flood query count コマンドを使用して TCN フラッドクエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

TCN フラッディング クエリー カウントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip igmp snooping tcn flood query count count</code>	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ~ 10 です。デフォルトのフラッディング クエリー カウントは 2 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ip igmp snooping</code>	TCN の設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのフラッディング クエリー カウントに戻すには、`no ip igmp snooping tcn flood query count` グローバル コンフィギュレーション コマンドを使用します。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ (グローバル Leave メッセージ) をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、`ip igmp snooping tcn query solicit` グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニングツリーのルートであるかどうかにかかわらず、グローバル Leave メッセージを送信します。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。スイッチがスパニングツリーのルートであれば、このコンフィギュレーション コマンドに関係なく、Leave メッセージが常に送信されます。デフォルトでは、クエリー送信要求はディセーブルに設定されています。

スイッチがスパニングツリー ルートであるかどうかにかかわらず、グローバル Leave メッセージを送信するように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip igmp snooping tcn query solicit</code>	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ (グローバル脱退) を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ip igmp snooping</code>	TCN の設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのクエリー送信要求に戻すには、`no ip igmp snooping tcn query solicit` グローバル コンフィギュレーション コマンドを使用します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチは TCN を受信すると、一般クエリーを 2 つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッディングします。異なるマルチキャストグループのホストに接続しているポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損失が発生する可能性があります。その場合、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用して、この状態を制御できます。

インターフェイス上でマルチキャスト フラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no ip igmp snooping tcn flood	スパンニングツリーの TCN イベント中に発生するマルチキャストトラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。
ステップ 4	exit	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping	TCN の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイス上でマルチキャスト フラッディングを再度イネーブルにするには、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定するときには、次の注意事項に従ってください。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。イネーブルになると、IGMP スヌーピング クエリアはクエリー送信元アドレスとして IP アドレスを使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) IP アドレス (存在する場合) を使用しようとします。SVI IP アドレスが存在しない場合、スイッチはスイッチ上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアはスイッチ上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャストルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブルステートになります。
 - IGMP スヌーピングが VLAN でディセーブルの場合

- PIM が、VLAN に対応する SVI でイネーブルの場合

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip igmp snooping querier	IGMP スヌーピング クエリア機能をイネーブルにします。
ステップ3	ip igmp snooping querier address <i>ip_address</i>	(任意) IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 (注) IGMP スヌーピング クエリアはスイッチ上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
ステップ4	ip igmp snooping querier query-interval <i>interval-count</i>	(任意) IGMP クエリアの間隔を設定します。指定できる範囲は 1 ~ 18000 秒です。
ステップ5	ip igmp snooping querier tcn query [count <i>count</i> <i>interval interval</i>]	(任意) Topology Change Notification (TCN; トポロジ変更通知) クエリーの間隔を設定します。指定できる count の範囲は 1 ~ 10 です。指定できる interval の範囲は 1 ~ 255 秒です。
ステップ6	ip igmp snooping querier timer expiry <i>timeout</i>	(任意) IGMP クエリアが期限切れになるまでの時間を設定します。指定できる範囲は 60 ~ 300 秒です。
ステップ7	ip igmp snooping querier version <i>version</i>	(任意) クエリア機能を使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ8	end	特権 EXEC モードに戻ります。
ステップ9	show ip igmp snooping vlan <i>vlan-id</i>	(任意) VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ステップ10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

IGMP レポート抑制のディセーブル化



(注) IGMP レポート抑制は、マルチキャスト クエリーに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

IGMP レポート抑制はデフォルトでイネーブルです。IGMP レポート抑制がイネーブルの場合、スイッチは、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。

IGMP レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no ip igmp snooping report-suppression</code>	IGMP レポート抑制をディセーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip igmp snooping</code>	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP レポート抑制を再びイネーブルにするには、`ip igmp snooping report-suppression` グローバル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

動的に学習された、あるいは静的に設定されたルータ ポートおよび VLAN インターフェイスに関する IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP アドレス マルチキャスト エントリを表示することもできます。

IGMP スヌーピング情報を表示するには、表 28-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 28-4 IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
<code>show ip igmp snooping [vlan <i>vlan-id</i>]</code>	<p>スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ip igmp snooping groups [count dynamic [count] user [count]]</code>	<p>スイッチまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • dynamic : IGMP スヌーピングによって学習されたエントリを表示します。 • user : ユーザによって設定されたマルチキャスト エントリだけを表示します。
<code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i> count dynamic [count] user[count]]</code>	<p>マルチキャスト VLAN またはその VLAN の特定のパラメータについて、マルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • vlan-id : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • dynamic : IGMP スヌーピングによって学習されたエントリを表示します。 • ip_address : 指定のグループ IP アドレスのマルチキャスト グループについて、特性を表示します。 • user : ユーザによって設定されたマルチキャスト エントリだけを表示します。
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	<p>動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。</p> <p>(注) IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p>
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>]</code>	<p>IP アドレス、および VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p>
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code>	<p>IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。</p>

各コマンドのキーワードおよびオプションの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

MVR の概要

MVR は、イーサネット リング ベースのサービス プロバイダー ネットワークにおいて、マルチキャスト トラフィックを大規模展開する用途（サービス プロバイダー ネットワークによる複数のテレビ チャネルのブロードキャストなど）を想定して開発されました。MVR によってポート上の加入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有できます。MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されます。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退（Join および Leave）を行うことが前提です。これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作します。それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

スイッチの CPU は、MVR IP マルチキャストストリームとそれに対応するスイッチ転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホスト メンバーシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバ ポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアント ポートから転送されます。それ以外のポートからは転送されません。MVR ホストから受信した IGMP レポートも、スイッチのすべての MVR データ ポートから転送されます。したがって、互換モードでスイッチを稼働させた場合と異なり、MVR データ ポートリンクで不要な帯域幅を使用しなくて済みます。

MVR に関与するのはレイヤ 2 ポートだけです。ポートを MVR レシーバ ポートとして設定する必要があります。各スイッチでサポートされる MVR マルチキャスト VLAN は、1 つだけです。

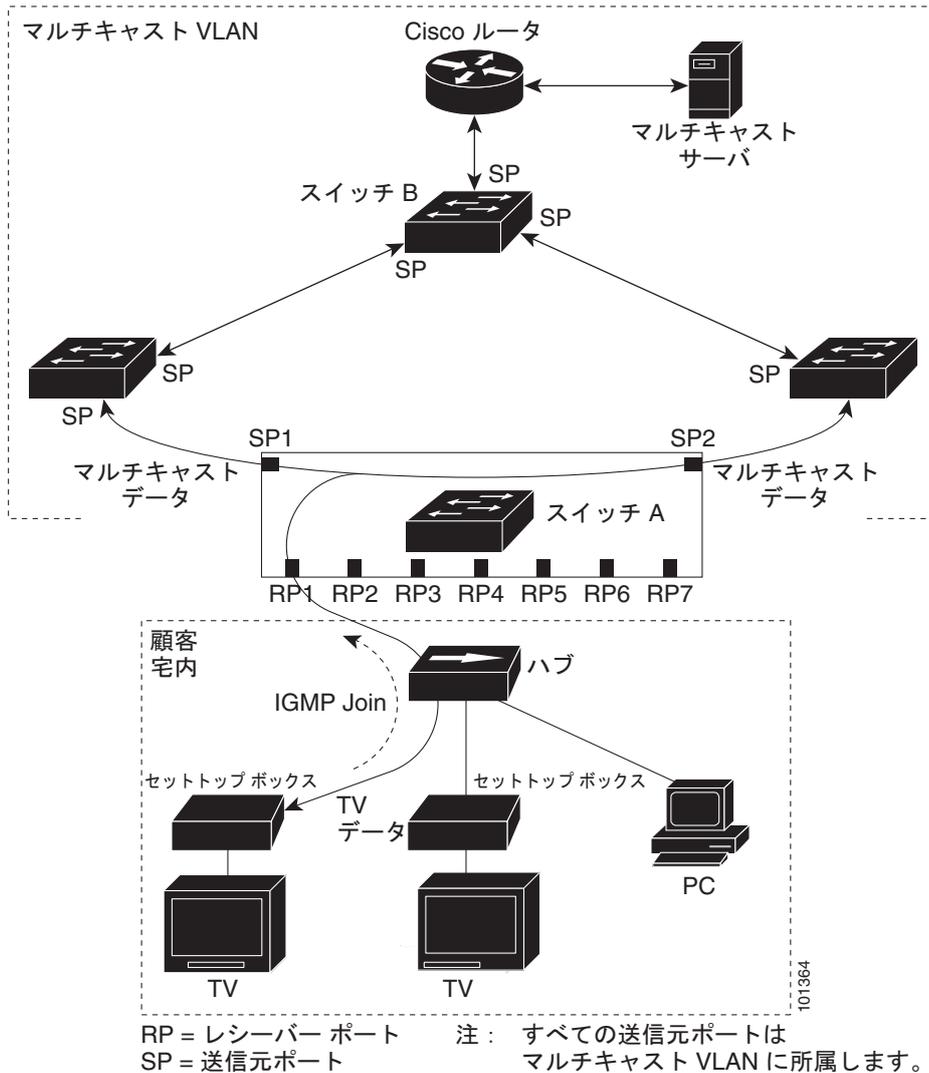
マルチキャスト TV アプリケーションで MVR を使用する場合

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信できます。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR レシーバ ポートとして設定されたスイッチ ポートです。

図 28-3 に構成例を示します。Dynamic Host Configuration Protocol (DHCP) によって、セットトップ ボックスまたは PC に IP アドレスが割り当てられます。加入者がチャンネルを選択すると、適切なマルチキャストに加入するために、セットトップ ボックスまたは PC からスイッチ A に IGMP レポート

が送信されます。IGMP レポートが、設定されている IP マルチキャストグループアドレスの 1 つと一致すると、スイッチの CPU がハードウェア アドレス テーブルを変更して、指定のマルチキャストストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバポートと VLAN を追加します。マルチキャスト VLAN との間でマルチキャストデータを送受信するアップリンクポートを MVR 送信元ポートといいます。

図 28-3 MVR の例



加入者がチャンネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップボックスからマルチキャストストリームに対する IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、このグループに加入している別のセットトップボックスがある場合、そのセットトップボックスはクエリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はそのグループの転送先としてのレシーバポートを除外します。

即時脱退機能を使用しない場合、レシーバポートの加入者から IGMP Leave メッセージを受信したスイッチは、そのポートに IGMP クエリーを送信し、IGMP グループメンバーシップレポートを待ちます。設定された時間内にレポートが届かないと、レシーバポートがマルチキャストグループメンバー

シップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバポートから IGMP クエリーが送信されません。Leave メッセージの受信後ただちに、マルチキャストグループメンバーシップからレシーバポートが削除されるので、脱退のための待ち時間が短縮されます。即時脱退機能をイネーブルにするのは、接続されているレシーバデバイスが 1 つだけのレシーバポートに限定してください。

MVR では、各 VLAN の加入者に TV チャンネルのマルチキャストトラフィックを重複して送信する必要がありません。すべてのチャンネル用のマルチキャストトラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランク全体で 1 回送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN に送られます。これらのメッセージは、レイヤ 3 デバイス上のマルチキャスト VLAN のマルチキャストトラフィックストリームに対して動的に登録されます。スイッチ B アクセス レイヤ スイッチ (スイッチ A) が転送動作を変更し、マルチキャスト VLAN から別個の VLAN 上の加入者ポートへトラフィックを転送できるようにするので、選択されたトラフィックが 2 つの VLAN 間を伝送されます。

IGMP レポートは、マルチキャストデータと同じ IP マルチキャストグループアドレスに送信されません。スイッチ A の CPU は、レシーバポートから送られたすべての IGMP Join および Leave メッセージを取り込み、MVR モードに基づいて、送信元 (アップリンク) ポートのマルチキャスト VLAN に転送しなければなりません。

MVR の設定

ここでは、次の設定について説明します。

- 「MVR のデフォルト設定」 (P.28-20)
- 「MVR 設定時の注意事項および制限事項」 (P.28-21)
- 「MVR グローバルパラメータの設定」 (P.28-21)
- 「MVR インターフェイスの設定」 (P.28-23)

MVR のデフォルト設定

表 28-5 に、MVR のデフォルト設定を示します。

表 28-5 MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	未設定
クエリーの応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	互換
インターフェイスのデフォルト (ポート単位)	レシーバポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

MVR を設定するときには、次の注意事項に従ってください。

- レシーバポートはアクセスポートでなければなりません。トランクポートにすることはできません。スイッチのレシーバポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。
- スイッチ上で設定できるマルチキャスト エントリ (MVR グループ アドレス) の最大数 (受信できるテレビチャンネルの最大数) は 256 です。
- 送信元 VLAN で受信され、レシーバポートから脱退する MVR マルチキャスト データは、スイッチで Time to Live (TTL; 存続可能時間) が 1 だけ少なくなります。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するので、スイッチ上でエイリアスの IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス (224.0.0.xxx 範囲内) を設定する必要はありません。
- プライベート VLAN ポートに MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルの場合、MVR はサポートされません。MVR がイネーブルの場合に、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されます。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとすると、MVR をイネーブルにする操作が取り消され、エラーメッセージが表示されます。
- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR レシーバポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。

MVR グローバル パラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合には (MVR VLAN 以外)、最初に MVR をイネーブルにする必要があります。



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

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mvr</code>	スイッチ上で MVR をイネーブルに設定します。

MVR の設定

	コマンド	目的
ステップ 3	<code>mvr group ip-address [count]</code>	スイッチ上で IP マルチキャストアドレスを設定するか、または <i>count</i> パラメータを使用して、連続する MVR グループアドレスを設定します (<i>count</i> の範囲は 1 ~ 256、デフォルトは 1)。このアドレスに送信されたマルチキャストデータは、スイッチ上のすべての送信元ポートおよびそのマルチキャストアドレスのデータを受信するために選ばれた、すべてのレシーバポートに送信されます。マルチキャストアドレスとテレビチャンネルは 1 対 1 の対応です。
ステップ 4	<code>mvr querytime value</code>	(任意) マルチキャストグループメンバーシップからポートを削除する前に、レシーバポートで IGMP レポートのメンバーシップを待機する最大時間を設定します。この値は 10 分の 1 秒単位で設定します。範囲は 1 ~ 100、デフォルトは 10 分の 5 秒、つまり 0.5 秒です。
ステップ 5	<code>mvr vlan vlan-id</code>	(任意) マルチキャストデータを受信する VLAN を指定します。すべての送信元ポートをこの VLAN に所属させる必要があります。VLAN の範囲は 1 ~ 1001 および 1006 ~ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	<code>mvr mode {dynamic compatible}</code>	(任意) MVR の動作モードを指定します。 <ul style="list-style-type: none"> • dynamic : 送信元ポートでダイナミック MVR メンバーシップを使用できます。 • compatible : Catalyst 3500 XL スイッチおよび Catalyst 2900 XL スイッチとの互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。 デフォルトは compatible モードです。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show mvr</code> または <code>show mvr members</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

スイッチをデフォルトの設定に戻すには、`no mvr [mode | group ip-address | querytime | vlan]` グローバル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにして、MVR グループアドレスを設定し、クエリータイムを 1 秒 (10 分の 10 秒) に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナミックに設定する例を示します。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

`show mvr members` 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャストグループアドレスを確認できます。

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mvr</code>	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	<code>interface interface-id</code>	設定するレイヤ 2 ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>mvr type {source receiver}</code>	<p>MVR ポートを次のいずれかに設定します。</p> <ul style="list-style-type: none"> source : マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。 receiver : 加入者ポートであり、マルチキャスト データを受信するだけの場合、レシーバ ポートとしてポートを設定します。静的に、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバになるまでは、データを受信しません。レシーバ ポートはマルチキャスト VLAN に属することはできません。 <p>デフォルトでは、非 MVR ポートとして設定されます。非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。</p>
ステップ 5	<code>mvr vlan vlan-id group [ip-address]</code>	<p>(任意) マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。グループ メンバとして静的に設定されたポートは、静的に削除されない限り、グループ メンバのままです。</p> <p>(注) 互換モードでは、このコマンドが適用されるのはレシーバ ポートだけです。ダイナミック モードでは、レシーバ ポートおよび送信元ポートに適用されます。</p> <p>レシーバ ポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャスト グループに動的に加入することもできます。</p>
ステップ 6	<code>mvr immediate</code>	<p>(任意) ポート上で MVR の即時脱退機能をイネーブルにします。</p> <p>(注) このコマンドが適用されるのは、レシーバ ポートだけです。また、イネーブルにするのは、単一のレシーバ デバイスが接続されているレシーバ ポートに限定してください。</p>
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show mvr</code> <code>show mvr interface</code> または <code>show mvr members</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの設定に戻すには、`no mvr [type | immediate | vlan vlan-id | group]` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをレシーバポートとして設定し、マルチキャストグループアドレスに送信されたマルチキャストトラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port      Type      Status      Immediate Leave
----      -
G11/2     RECEIVER  ACTIVE/DOWN  ENABLED
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR の設定を表示するには、特権 EXEC モードで表 28-6 のコマンドを使用します。

表 28-6 MVR 情報を表示するためのコマンド

コマンド	目的
<code>show mvr</code>	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまたはディセーブルの判別、マルチキャスト VLAN、マルチキャストグループの最大数 (256) および現在の数 (0 ~ 256)、クエリーの応答時間、および MVR モードです。
<code>show mvr interface [interface-id] [members [vlan vlan-id]]</code>	すべての MVR インターフェイスおよびそれぞれの MVR 設定を表示します。特定のインターフェイスを指定すると、次の情報が表示されます。 <ul style="list-style-type: none"> Type : Receiver または Source Status : 次のいずれか <ul style="list-style-type: none"> ACTIVE は、ポートが VLAN に含まれていることを意味します。 UP/DOWN は、ポートが転送中または転送中ではないことを示します。 INACTIVE は、ポートが VLAN に含まれていないことを意味します。 Immediate Leave : Enabled または Disabled members キーワードを入力すると、そのポート上のすべてのマルチキャストグループメンバが表示されます。VLAN ID を入力した場合は、VLAN 上のすべてのマルチキャストグループメンバが表示されます。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show mvr members [ip-address]</code>	すべての IP マルチキャストグループまたは指定した IP マルチキャストグループ IP アドレスに含まれているレシーバポートおよび送信元ポートがすべて表示されます。

IGMP フィルタリングおよびスロットリングの設定

都市部や Multiple-Dwelling Unit (MDU) などの環境では、スイッチ ポート上のユーザが属する一連のマルチキャスト グループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャスト グループの数を、スイッチ ポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各スイッチ ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャスト グループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。マルチキャスト グループへのアクセスがフィルタリングアクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート (Join および Leave レポートを含む) だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャスト エントリを上書きします。



(注)

IGMP フィルタリングが実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

ここでは、次の設定について説明します。

- 「IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定」(P.28-26)
- 「IGMP プロファイルの設定」(P.28-26) (任意)
- 「IGMP プロファイルの適用」(P.28-27) (任意)
- 「IGMP グループの最大数の設定」(P.28-28) (任意)
- 「IGMP スロットリングアクションの設定」(P.28-29) (任意)

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

表 28-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 28-7 IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用されない
IGMP グループの最大数	最大数は設定されない
IGMP プロファイル	未設定
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

転送テーブルに登録されているグループが最大数に達しているとき、デフォルトの IGMP スロットリング アクションは IGMP レポートを拒否します。設定時の注意事項については、「[IGMP スロットリング アクションの設定](#)」(P.28-29) を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、`ip igmp profile` グローバル コンフィギュレーション コマンドおよびプロファイル番号を使用して、IGMP プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始します。ポートから送信される IGMP Join 要求をフィルタリングするために使用される IGMP プロファイルのパラメータは、このモードから指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny** : 一致するアドレスを拒否します。デフォルトで設定されています。
- **exit** : IGMP プロファイル コンフィギュレーション モードを終了します。
- **no** : コマンドを否定するか、または設定をデフォルトに戻します。
- **permit** : 一致するアドレスを許可します。
- **range** : プロファイルの IP アドレス範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。

デフォルトでは、スイッチには IGMP プロファイルが設定されていません。プロファイルが設定されており、**permit** および **deny** キーワードがいずれも指定されていない場合、デフォルトでは、IP アドレス範囲へのアクセスが拒否されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp profile profile number</code>	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。プロファイル番号の範囲は 1 ~ 4294967295 です。
ステップ 3	<code>permit deny</code>	(任意) IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。

コマンド	目的
ステップ4 range ip multicast address	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 range コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。
ステップ5 end	特権 EXEC モードに戻ります。
ステップ6 show ip igmp profile profile number	プロファイルの設定を確認します。
ステップ7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range ip multicast address** IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否 (デフォルト) である場合は、**show ip igmp profile** の出力には表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して、プロファイルを該当するインターフェイスに適用します。IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。EtherChannel ポート グループに所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 interface interface-id	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ3 ip igmp filter profile number	指定された IGMP プロファイルをインターフェイスに適用します。指定できる範囲は 1 ~ 4294967295 です。
ステップ4 end	特権 EXEC モードに戻ります。

IGMP フィルタリングおよびスロットリングの設定

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

インターフェイスからプロファイルを削除するには、**no ip igmp filter profile number** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの最大数の設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、**ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト設定 (制限なし) に戻すには、このコマンドの **no** 形式を使用します。

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

転送テーブルの IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 3	ip igmp max-groups <i>number</i>	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ~ 4294967294 です。デフォルトでは最大数は設定されません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface <i>interface-id</i>	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

グループの最大数に関する制限を削除し、デフォルト設定 (制限なし) に戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定した後、**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドを使用して受信した IGMP レポートの新しいグループで、既存のグループを上書きします。IGMP Join レポートを廃棄するデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

IGMP スロットリング アクションを設定する場合には、次の注意事項に従ってください。

- この制限事項は、レイヤ 2 ポートにだけ適用されます。このコマンドは、論理 EtherChannel インターフェイスでは使用できませんが、EtherChannel ポート グループに属するポートでは使用できません。
- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action {deny | replace}** コマンドを入力しても効果はありません。
- インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリング アクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。
 - スロットリング アクションを **deny** に設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、スイッチは、インターフェイスで受信した次の IGMP レポートを廃棄します。
 - スロットリング アクションを **replace** に設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、スイッチはランダムに選択したエントリを受信した IGMP レポートで上書きします。

スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、**IGMP スロットリング アクション**を設定します。

転送テーブルに最大数のエントリが登録されているときにスロットリング アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 3	ip igmp max-groups action {deny replace}	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 <ul style="list-style-type: none"> deny : レポートを廃棄します。 replace : 既存のグループを、IGMP レポートを受信した新しいグループで上書きします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

■ IGMP フィルタリングおよび IGMP スロットリング設定の表示

レポートの廃棄というデフォルトのアクションに戻すには、`no ip igmp max-groups action` インターフェイス コンフィギュレーション コマンドを使用します。

IGMP フィルタリングおよび IGMP スロットリング設定の表示

IGMP プロファイルの特性を表示したり、スイッチ上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。また、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 28-8 の特権 EXEC コマンドを使用して、IGMP フィルタリングおよび IGMP スロットリングの設定を表示します。

表 28-8 IGMP フィルタリングおよび IGMP スロットリングの設定を表示するためのコマンド

コマンド	目的
<code>show ip igmp profile [profile number]</code>	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
<code>show running-config [interface interface-id]</code>	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはスイッチ上のすべてのインターフェイスの設定を表示します。



CHAPTER 29

ポート単位のトラフィック制御の設定

この章では、IE 3000 スイッチにポートベースのトラフィック制御機能を設定する手順について説明します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「ストーム制御の設定」 (P.29-1)
- 「保護ポートの設定」 (P.29-6)
- 「ポートブロッキングの設定」 (P.29-7)
- 「ポートセキュリティの設定」 (P.29-9)
- 「プロトコルストームプロテクションの設定」 (P.29-20)
- 「ポート単位のトラフィック制御設定の表示」 (P.29-22)

ストーム制御の設定

ここでは、次の概念と設定情報について説明します。

- 「ストーム制御の概要」 (P.29-1)
- 「ストーム制御のデフォルト設定」 (P.29-3)
- 「ストーム制御およびしきい値レベルの設定」 (P.29-3)
- 「小さいフレームの着信レートの設定」 (P.29-5)

ストーム制御の概要

ストーム制御は、物理インターフェイスの1つで発生したブロードキャスト、マルチキャスト、またはユニキャストストームによってLAN上のトラフィックが混乱することを防ぎます。LANストームは、LANにパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワークパフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされるDoS攻撃もストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のパケット数。
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のビット数。
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

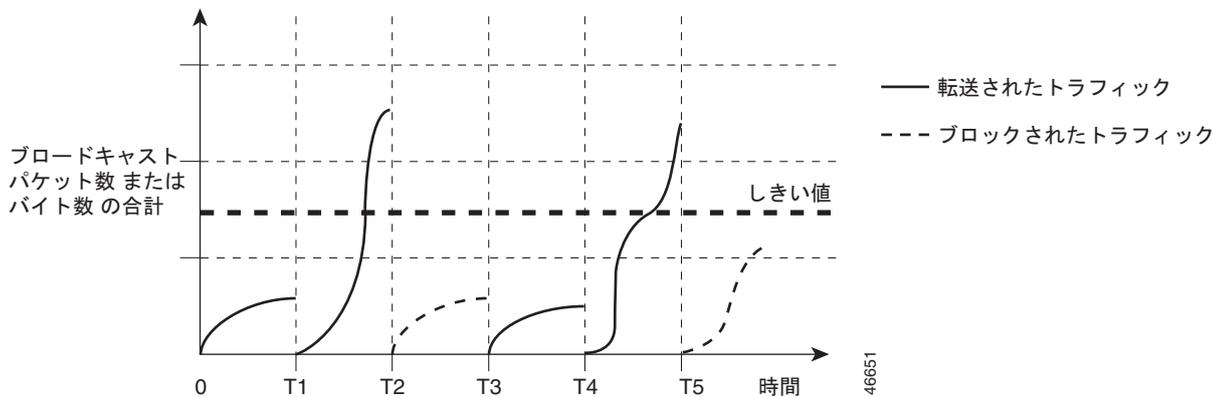


(注)

マルチキャスト トラフィックのストーム制御しきい値に達した場合、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) および Cisco Discovery Protocol (CDP) フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図 29-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも当てはまります。この例では、T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

図 29-1 ブロードキャストストーム制御の例



ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせ、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過するパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。



(注) パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、ユニキャスト、ブロードキャスト、およびマルチキャストストーム制御はスイッチ インターフェイス上でディセーブルになります。したがって、抑制レベルは 100% です。

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。ただし、ハードウェアの制約とともに、さまざまなサイズの packets をどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。



(注) ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>storm-control {broadcast multicast unicast} level {level [level-low] bps bps [bps-low] pps pps [pps-low]}</code>	<p>ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ~ 100.00 です。 • (任意) <i>level-low</i> には、下限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ~ 100.00 です。 <p>しきい値に最大値 (100%) を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。</p> <ul style="list-style-type: none"> • <i>bps bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 • (任意) <i>bps-low</i> には、下限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 • <i>pps pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 • (任意) <i>pps-low</i> には、下限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。</p>

	コマンド	目的
ステップ4	<code>storm-control action {shutdown trap}</code>	ストームが検出された場合に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 <ul style="list-style-type: none"> ストーム中、ポートを <code>errdisable</code> の状態にするには、shutdown キーワードを選択します。 ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、trap キーワードを選択します。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show storm-control [interface-id] [broadcast multicast unicast]</code>	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャストストーム制御の設定が表示されます。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、**no storm-control {broadcast | multicast | unicast} level** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で、上限抑制レベルを 87%、下限抑制レベルを 65% に設定し、ユニキャストストーム制御をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポート上で、ブロードキャストアドレスのストーム制御を 20% のレベルでイネーブルにする例を示します。ブロードキャストトラフィックが、トラフィックストーム制御インターバル内にポートで使用できる総帯域幅のうち、設定された 20% のレベルを超えた場合、トラフィックストーム制御インターバルが終わるまで、スイッチはすべてのブロードキャストトラフィックをドロップします。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control broadcast level 20
```

小さいフレームの着信レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、小さいフレームと見なされます。このパケットはスイッチにより転送されますが、スイッチストーム制御カウンタを増加させません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定されたレート（しきい値）で到着した場合は、ポートがディセーブルになるように設定できます。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを入力すると、指定された時間後にポートが再びイネーブルになります（**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して、リカバリ時間を指定します）。

各インターフェイスのしきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>errdisable detect cause small-frame</code>	スイッチ上の小さいフレームの着信レート機能をイネーブルにします。
ステップ 3	<code>errdisable recovery interval interval</code>	(任意) 指定された <code>errdisable</code> ステートから回復する時間を指定します。
ステップ 4	<code>errdisable recovery cause small-frame</code>	(任意) 小さいフレームの着信によりポートが <code>errdisable</code> になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。
ステップ 5	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	<code>small violation-rate pps</code>	インターフェイスが着信パケットをドロップしてポートを <code>errdisable</code> にするようにしきい値レートを設定します。範囲は、1 ~ 10,000 Packets Per Second (pps; パケット/秒) です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show interfaces interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、小さいフレームの着信レート機能をイネーブルにし、ポートのリカバリ時間を設定し、ポートを `errdisable` にするしきい値を設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

保護ポートの設定

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ 3 デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

ここでは、次の設定について説明します。

- 「保護ポートのデフォルト設定」(P.29-7)
- 「保護ポート設定時の注意事項」(P.29-7)

- 「保護ポートの設定」(P.29-7)

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポート設定時の注意事項

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャンネルで保護ポートをイネーブルにした場合は、そのポート チャンネル グループ内のすべてのポートでイネーブルになります。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport protected</code>	インターフェイスを保護ポートに設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、`no switchport protected` インターフェイス コンフィギュレーション コマンドを使用します。

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト

トラフィックがあるポートから別のポートに転送されないようにするために、(保護または非保護)ポートをブロックし、未知のユニキャストまたはマルチキャストパケットが他のポートにフラッディングされないようにします。



(注)

マルチキャストトラフィックでは、ポートブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。

ここでは、次の設定について説明します。

- 「ポートブロッキングのデフォルト設定」(P.29-8)
- 「インターフェイスでのフラッディングトラフィックのブロッキング」(P.29-8)

ポートブロッキングのデフォルト設定

デフォルトでは、ポートから未知のマルチキャストおよびユニキャストトラフィックのフラッディングがブロックされず、すべてのポートにこのようなパケットがフラッディングされます。

インターフェイスでのフラッディングトラフィックのブロッキング



(注)

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポートチャネルのマルチキャストまたはユニキャストトラフィックをブロックすると、ポートチャネルグループのすべてのポートでブロックされます。

ユニキャストパケットおよびレイヤ 2 マルチキャストパケットのインターフェイスからのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport block multicast</code>	ポートからの未知のマルチキャストの転送をブロックします。 (注) 純粋なレイヤ 2 マルチキャストトラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。
ステップ 4	<code>switchport block unicast</code>	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でトラフィックがブロックされずに、通常の転送が行われるデフォルトの状態にインターフェイスを戻すには、**no switchport block {multicast | unicast}** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のユニキャストおよびレイヤ 2 マルチキャスト フラッドイングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポートセキュリティの設定

ポートセキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたとのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

ここでは、次の概念と設定情報について説明します。

- 「ポートセキュリティの概要」(P.29-9)
- 「ポートセキュリティのデフォルト設定」(P.29-12)
- 「ポートセキュリティの設定時の注意事項」(P.29-12)
- 「ポートセキュリティのイネーブル化および設定」(P.29-14)
- 「ポートセキュリティ エージングのイネーブル化および設定」(P.29-18)
- 「ポートセキュリティおよびプライベート VLAN」(P.29-20)

ポートセキュリティの概要

ここでは、次の概要について説明します。

- 「セキュア MAC アドレス」(P.29-9)
- 「セキュリティ違反」(P.29-10)

セキュア MAC アドレス

ポートで許可されるセキュア アドレスの最大数を設定するには、**switchport port-security maximum value** インターフェイス コンフィギュレーション コマンドを使用します。



(注)

最大値をインターフェイス上ですでに設定されているセキュア アドレスの数より小さい値に設定しようとする、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- **スタティック セキュア MAC アドレス** : `switchport port-security mac-address mac-address` インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- **ダイナミック セキュア MAC アドレス** : 動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- **スティッキセキュア MAC アドレス** : 動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキ ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキ セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。スティッキ ラーニングをイネーブルにするには、`switchport port-security mac-address sticky` インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキ セキュア MAC アドレスに変換します。すべてのスティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキ セキュア MAC アドレスは、コンフィギュレーション ファイル (スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション) に、自動的に反映されません。スティッキ セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。第 10 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合のアクションに基づいて、次の 4 つの違反モードのいずれかにインターフェイスを設定できます。

- **protect** (保護) : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。



(注) トランク ポートに **protect** 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- **restrict** (制限) : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- **shutdown** (シャットダウン) : ポートセキュリティ違反により、インターフェイスが **errdisable** になり、ただちにシャットダウンされます。その後、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが **errdisable** ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。これは、デフォルトのモードです。
- **shutdown vlan** (VLAN シャットダウン) : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が **errdisable** になります。

表 29-1 に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 29-1 セキュリティ違反モードの処置

違反モード	トラフィックの転送 ¹	SNMP トラップの送信	Syslog メッセージの送信	エラーメッセージの表示 ²	違反カウンタの増加	ポートのシャットダウン
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes
shutdown vlan	No	No	Yes	No	Yes	No ³

1. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラーメッセージを返します。
3. 違反が発生した VLAN のみシャットダウンします。

ポートセキュリティのデフォルト設定

表 29-2 に、インターフェイスに対するポートセキュリティのデフォルト設定を示します。

表 29-2 ポートセキュリティのデフォルト設定

機能	デフォルト設定
ポートセキュリティ	ポート上でディセーブル
スティッキアドレスラーニング	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1
違反モード	シャットダウン。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブル エージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポートセキュリティの設定時の注意事項

ポートセキュリティを設定するときには、次の注意事項に従ってください。

- ポートセキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートを Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) の宛先ポートにすることはできません。



(注) 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランク ポートがポートセキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。

- ポートセキュリティを設定する場合は、最初に **switchport port-security maximum** インターフェイス コンフィギュレーション コマンドを使用して許可する MAC アドレスの合計数を指定し、次に許可するアクセス VLAN (**switchport port-security vlan access** インターフェイス コンフィ

ギューレーション コマンド) の数および音声 VLAN (**switchport port-security vlan voice** インターフェイス コンフィギュレーション コマンド) の数を設定します。最初に合計数を指定しなかった場合は、システムによってデフォルト設定 (1 つの MAC アドレス) が返されます。

- インターフェイスの最大セキュア アドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングをサポートしていません。

表 29-3 に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

表 29-3 ポート セキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP ¹ ポート ²	No
トランク ポート	Yes
ダイナミック アクセス ポート ³	No
ルーテッド ポート	No
Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	Yes
トンネリング ポート	Yes
保護ポート	Yes
IEEE 802.1x ポート	Yes
音声 VLAN ポート ⁴	Yes
プライベート VLAN ポート	Yes
IP ソース ガード	Yes
ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) インспекション	Yes
Flex Link	Yes

1. DTP = Dynamic Trunking Protocol

2. **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。

3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol (VQP) ポート。

4. ポートに最大限可能なセキュアなアドレスを設定します (アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数)。

ポートセキュリティのイネーブル化および設定

ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode {access trunk}</code>	インターフェイス スイッチポート モードを <code>access</code> または <code>trunk</code> に設定します。デフォルト モード (<code>dynamic auto</code>) のインターフェイスは、セキュアポートとして設定できません。
ステップ 4	<code>switchport voice vlan vlan-id</code>	ポート上で音声 VLAN をイネーブルにします。 <i>vlan-id</i> : 音声トラフィックに使用する VLAN を指定します。
ステップ 5	<code>switchport port-security</code>	インターフェイス上でポートセキュリティをイネーブルにします。
ステップ 6	<code>switchport port-security [maximum value [vlan {vlan-list {access voice}}]]</code>	<p>(任意) maximum : ポート上のセキュア MAC アドレスの最大数を指定します。デフォルトでは、1 つの MAC アドレスのみ許可されます。</p> <p>スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって決まります。第 10 章「スイッチ SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> vlan-list : トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>

コマンド	目的
ステップ7 <code>switchport port-security [violation {protect restrict shutdown shutdown vlan}]</code>	<p>(任意) 違反モード、つまりセキュリティ違反が検出されたときの対応を、次のいずれかに設定します。</p> <ul style="list-style-type: none"> protect (保護) : ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 <p>(注) トランク ポートに protect モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。</p> <ul style="list-style-type: none"> restrict : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 shutdown : 違反が発生すると、インターフェイスが errdisable になり、ポートの LED が消灯します。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。 shutdown vlan : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 <p>(注) セキュア ポートが errdisable ステートになった場合は、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力して、このステートを解除します。手動で再びイネーブルにするには、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力するか、clear errdisable interface vlan 特権 EXEC コマンドを入力します。</p>

	コマンド	目的
ステップ 8	switchport port-security [mac-address mac-address [vlan { vlan-id { access voice }}]]	<p>(任意) インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。</p> <p>(注) このコマンドの入力後にスティック ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティック セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • vlan-id : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
ステップ 9	switchport port-security mac-address sticky	(任意) インターフェイスでスティック ラーニングをイネーブルにします。
ステップ 10	switchport port-security mac-address sticky [mac-address vlan { vlan-id { access voice }}]	<p>(任意) スティック セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティック セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p>(注) このコマンドの入力前にスティック ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティック セキュア MAC アドレスを入力できません。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> • vlan-id : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。</p>
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show port-security	設定を確認します。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

セキュアポートではないデフォルトの状態にインターフェイスを戻すには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。スティッキ ラーニングがイネーブルの状態でのこのコマンドを入力すると、スティッキ セキュア アドレスが実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。ここですべてのアドレスが動的に学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻すには、**no switchport port-security maximum value** インターフェイス コンフィギュレーション コマンドを使用します。違反モードをデフォルト状態 (shutdown モード) に戻すには、**no switchport port-security violation {protocol | restrict}** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスがスティッキ セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、スティッキ MAC アドレスによる設定を保存した場合、**no switchport port-security mac-address sticky** コマンドの入力後に設定をもう一度保存しないと、スイッチの再起動時にスティッキ アドレスが復元されます。

MAC アドレス テーブルからスイッチまたはインターフェイス上のセキュア アドレスすべてまたは特定 (設定、ダイナミック、スティッキ) のセキュア アドレスすべてを削除するには、**clear port-security {all | configured | dynamic | sticky}** 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイス上のすべてのダイナミック セキュア アドレスをアドレス テーブルから削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドの後に、(インターフェイスでポート セキュリティを再びイネーブルにするために) **switchport port-security** コマンドを入力します。**no switchport port-security** コマンドを使用する前に、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用してスティッキ セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換した場合、手動で設定されたものを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

設定済みのセキュア MAC アドレスをアドレス テーブルから明確に削除する場合、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用する必要があります。

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキ ラーニングはイネーブルです。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポートのスティッキ ポート セキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します (データ VLAN に 10、音声 VLAN に 10 を割り当てます)。

```
Switch(config)# interface FastEthernet1/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
```

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングのイネーブル化および設定

ポート上のすべてのセキュアアドレスにエージングタイムを設定するには、ポートセキュリティエージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- **absolute** : 指定されたエージングタイムの経過後に、ポート上のセキュアアドレスが削除されます。
- **inactivity** : 指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュアアドレスが削除されます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

ポートセキュリティエージングを設定するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ3	<code>switchport port-security aging {static time time type {absolute inactivity}}</code>	<p>セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。</p> <p>(注) スイッチは、スタティックセキュア アドレスのポートセキュリティ エージングをサポートしていません。</p> <p>このポートに、スタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、static を入力します。</p> <p><i>time</i> には、このポートのエージング タイムを指定します。指定できる範囲は、0 ~ 1440 分です。</p> <p>type には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • absolute : エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した時間 (分単位) が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • inactivity : エージング タイプを非アクティブ エージングとして設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show port-security [interface interface-id] [address]</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上のすべてのセキュア アドレスに対してポートセキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** インターフェイス コンフィギュレーション コマンドを使用します。静的に設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスに対して、エージングをイネーブルにし、非アクティブ エージング タイプのエージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

上記のコマンドを確認するには、**show port-security interface interface-id** 特権 EXEC コマンドを入力します。

ポート セキュリティおよびプライベート VLAN

ポート セキュリティにより、管理者はポートで学習する MAC アドレス数を制限したり、ポートで学習する MAC アドレスを定義したりできます。

PVLAN ホストおよび無差別ポートでポート セキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode private-vlan {host promiscuous}</code>	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	<code>switchport port-security</code>	インターフェイス上でポート セキュリティをイネーブルにします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show port-security [interface interface-id] [address]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```



(注)

ポート セキュリティとプライベート VLAN の両方が設定されているポートには、セキュア PVLAN ポートのラベル付けが可能です。セキュア アドレスがセキュア PVLAN ポートで学習される時、同じセキュア アドレスは、同じプライマリ VLAN に属する別のセキュア PVLAN ポートでは学習できません。ただし、非セキュア PVLAN ポートで学習されたアドレスは、同じプライマリ VLAN に属するセキュア PVLAN ポートで学習できます。

ホスト ポートで学習されるセキュア アドレスは、関連プライマリ VLAN で自動的に複製され、また同様に、無差別ポートで学習されるセキュア アドレスは、すべての関連セカンダリ VLAN で自動的に複製されます。静的アドレス (`mac-address-table static` コマンドを使用) は、ユーザがセキュア ポートで設定することはできません。

プロトコルストーム プロテクションの設定

- 「プロトコルストーム プロテクションの概要」 (P.29-21)
- 「デフォルトのプロトコルストーム プロテクションの設定」 (P.29-21)
- 「プロトコルストーム プロテクションのイネーブル化」 (P.29-21)

プロトコル ストーム プロテクションの概要

スイッチが Address Resolution Protocol (ARP; アドレス解決プロトコル) または制御パケットでフラッドされると、CPU の高い使用率により CPU のオーバーロードが発生する可能性があります。これらの問題は、次のように発生します。

- プロトコル制御パケットが受信されず、ネイバーの隣接がドロップされるため、ルーティング プロトコルがフラップする場合があります。
- Spanning Tree Protocol (STP; スパニングツリー プロトコル) Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) が送受信されないため、STP が再収束します。
- CLI が遅くなるか応答しなくなります。

プロトコル ストーム プロテクションを使用すると、パケットのフロー レートの上限しきい値を指定して、制御パケットが送信されるレートを制御できます。サポートされるプロトコルは、ARP、ARP スヌーピング、Dynamic Host Configuration Protocol (DHCP) v4、DHCP スヌーピング、インターネット グループ管理プロトコル (IGMP)、および IGMP スヌーピングです。

パケットのレートが定義されたしきい値を超えると、スイッチは指定されたポートに着信したすべてのトラフィックを 30 秒間ドロップします。パケット レートが再度計測され、必要な場合はプロトコル ストーム プロテクションが再度適用されます。

より強力な保護が必要な場合は、仮想ポートを手動で `errdisable` にし、その仮想ポートのすべての着信トラフィックをブロックできます。また、手動で仮想ポートをイネーブルにしたり、仮想ポートの自動再イネーブル化の時間間隔を設定することもできます。



(注)

超過したパケットは、2 つ以下の仮想ポートにおいてドロップされます。仮想ポートの `errdisable` は、EtherChannel および Flexlink インターフェイスではサポートされません。

デフォルトのプロトコル ストーム プロテクションの設定

プロトコル ストーム プロテクションはデフォルトでディセーブルです。これがイネーブルになると、仮想ポートの自動リカバリがデフォルトでディセーブルになります。

プロトコル ストーム プロテクションのイネーブル化

プロトコル ストーム プロテクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>psp {arp dhcp igmp} pps value</code>	ARP、IGMP、または DHCP に対してプロトコル ストーム プロテクションを設定します。 <i>value</i> には、1 秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム プロテクションが適用されます。範囲は毎秒 5 ~ 50 パケットです。

	コマンド	目的
ステップ 3	errdisable detect cause psp	(任意) プロトコル ストーム プロテクションの errdisable 検出をイネーブルにします。この機能がイネーブルになると、仮想ポートが errdisable になります。この機能がディセーブルになると、そのポートは、ポートを errdisable にせず超過したパケットをドロップします。
ステップ 4	errdisable recovery interval time	(任意) errdisable の仮想ポートの自動リカバリ時間を秒単位で設定します。仮想ポートが errdisable の場合、この時間を過ぎるとスイッチは自動的にリカバリします。指定できる範囲は 30 ~ 86400 秒です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show psp config {arp dhcp igmp}	設定を確認します。

次の例では、DHCP の着信 DHCP トラフィックが毎秒 35 パケットを超えた場合に、トラフィックをドロップするようプロトコル ストーム プロテクションを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# psp dhcp pps 35
```

特定のプロトコルで、プロトコル ストーム プロテクションをディセーブルにするには、**no psp {arp | dhcp | igmp}** 特権 EXEC コマンドを使用します。

プロトコル ストーム プロテクションの **errdisable** 検出をディセーブルにするには、**no errdisable detect cause psp** グローバル コンフィギュレーション コマンドを使用します。

手動で **errdisable** 仮想ポートを再度イネーブルにするには、**errdisable recovery cause psp** グローバル コンフィギュレーション コマンドを使用します。

errdisable ポートの自動リカバリをディセーブルにするには、**no errdisable recovery cause psp** グローバル コンフィギュレーション コマンドを使用します。

プロトコル ストーム プロテクションが設定されている場合、ドロップされたパケットの数がカウンタに記録されます。このカウンタを表示するには、**show psp statistics [arp | igmp | dhcp]** 特権 EXEC コマンドを使用します。あるプロトコルのカウンタをクリアするには、**clear psp counter [arp | igmp | dhcp]** コマンドを使用します。

ポート単位のトラフィック制御設定の表示

show interfaces interface-id switchport 特権 EXEC コマンドを使用すると、(他の特性の中から) インターフェイス トラフィックの抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、ストーム制御およびポート セキュリティの設定が表示されます。

トラフィックの制御情報を表示するには、表 29-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 29-4 トラフィック制御ステータスおよび設定を表示するためのコマンド

コマンド	目的
show interfaces [<i>interface-id</i>] switchport	すべてのスイッチング（非ルーティング）ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポートブロッキングおよびポート保護の設定を含めて表示します。
show storm-control [<i>interface-id</i>] [broadcast multicast unicast]	すべてのインターフェイスまたは指定されたインターフェイスに設定されているストーム制御抑制レベルを、指定されたトラフィックタイプについて、またはブロードキャストトラフィック（トラフィックタイプが入力されていない場合）について表示します。
show port-security [interface <i>interface-id</i>]	スイッチまたは指定されたインターフェイスのポートセキュリティ設定を、各インターフェイスで許容されるセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [interface <i>interface-id</i>] address	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface <i>interface-id</i> vlan	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。

■ ポート単位のトラフィック制御設定の表示



CHAPTER 30

SPAN および RSPAN の設定

この章では、IE 3000 スイッチに スイッチド ポート アナライザ (SPAN) および Remote SPAN (RSPAN; リモート SPAN) を設定する方法について説明します。



(注)

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

この章の内容は、次のとおりです。

- 「SPAN および RSPAN の概要」 (P.30-1)
- 「SPAN および RSPAN の設定」 (P.30-9)
- 「SPAN および RSPAN のステータス表示」 (P.30-23)

SPAN および RSPAN の概要

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー (ミラーリング) して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

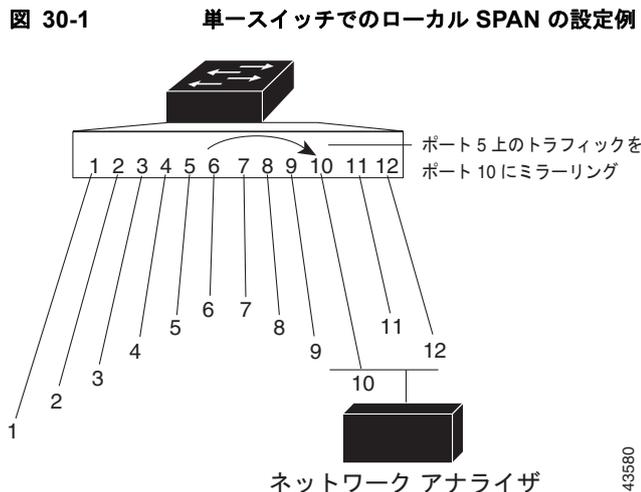
ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム (IDS) センサー装置を宛先ポートに接続すれば、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを閉じることができます。

ここでは、次の概要について説明します。

- 「ローカル SPAN」 (P.30-2)
- 「リモート SPAN」 (P.30-2)
- 「SPAN と RSPAN の概念および用語」 (P.30-3)
- 「SPAN および RSPAN と他の機能の相互作用」 (P.30-8)

ローカル SPAN

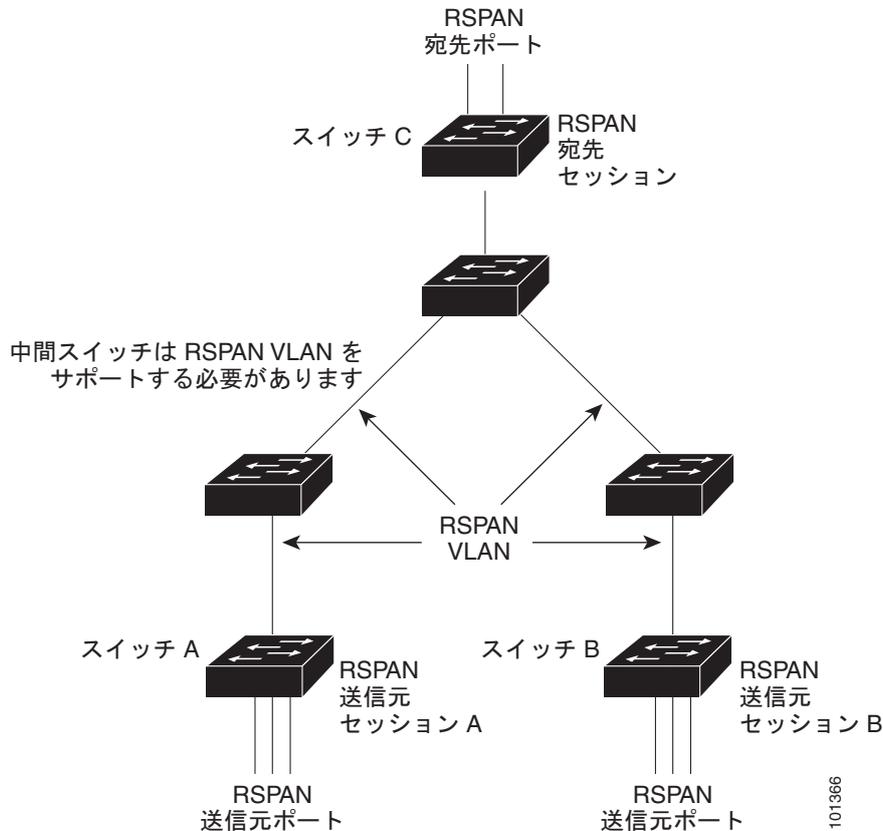
ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。たとえば、[図 30-1](#) の場合、ポート 5 (送信元ポート) 上のすべてのトラフィックがポート 10 (宛先ポート) にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。



リモート SPAN

RSPAN は異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク上にある複数のスイッチのリモート モニタリングを可能にします。[図 30-2](#) に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 30-2 RSPAN の設定例



SPAN と RSPAN の概念および用語

ここでは、SPAN および RSPAN の設定に関連する概念および用語について説明します。

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、送信元セッションおよび宛先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出力の packets セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを通じて宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタグングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、(レイヤ 2 制御パケットを除く) すべての RSPAN VLAN パケットを解析のためにユーザにコピーすることです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要求に応答する必要があります(「RSPAN VLAN」(P.30-8) を参照)。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたは VLAN を送信元にはできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは最大 2 つの送信元セッションをサポートします (ローカル SPAN および RSPAN 送信元セッション)。同じスイッチ内でローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチは合計 66 個の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、設定できる宛先ポート数は最大 64 です。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは 2 回伝送されます (1 回は標準トラフィックとして、もう 1 回はモニタされたパケットとして)。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

監視対象トラフィック

SPAN セッションは、次のトラフィック タイプをモニタできます。

- RX (受信) SPAN : 受信 (または入力) SPAN の役割は、送信元インターフェイスまたは VLAN が受信したすべてのパケットを、スイッチが変更または処理を行う前にできるだけ多くモニタすることです。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Differentiated Services Code Point (DSCP) の変更など、ルーティングや Quality of Service (QoS) が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセス コントロール リスト (ACL)、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- TX (送信) SPAN : 送信 (または出力) SPAN の役割は、スイッチによる変更および処理がすべて完了した後で、送信元インターフェイスが送信したすべてのパケットをできるだけ多くモニタすることです。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

ルーティングが原因で変更されたパケット (Time to Live (TTL; 存続可能時間)、MAC アドレス、QoS 値の変更など) は、宛先ポートで (変更されて) コピーされます。

送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方 : SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol (CDP)、VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル)、Dynamic Trunking Protocol (DTP)、Spanning-Tree Protocol (STP; スパニングツリー プロトコル)、Port Aggregation Protocol (PAgP) などの Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートの場合と同じカプセル化設定 (タグなし、または IEEE 802.1Q) を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクリプトが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スwitchの輻輳が原因でドロップされた出力パケットは、出力 SPAN からドロップされます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向 (RX と TX) SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両方のパケットは同じものになります (レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります)。

送信元ポート

送信元ポート (別名 *監視対象ポート*) は、ネットワーク トラフィック分析のために監視するスイッチドポートまたはルーテッドポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート (スイッチで利用可能なポートの最大数まで) と任意の数の送信

元 VLAN (サポートされている VLAN の最大数まで) をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ (ローカルまたは RSPAN) であるため、単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向 (入力、出力、または両方) を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ (EtherChannel、ファスト イーサネット、ギガビット イーサネットなど) が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、ルーテッド ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN (VSPAN) では、1 つまたは複数の VLAN のネットワーク トラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベース セッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。

- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名 *モニタ側ポート*）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションだけを実行するスイッチには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スwitchの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化について次のとおり動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなしまたは IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなしまたは IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span VLAN** コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VTP に対して可視である VLAN 1 ~ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲 (1006 ~ 4094) 内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックを監視しません。VSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のブルーニングが可能です。
- VLAN およびトランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel：EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバのままですが、*inactive* または *suspended* ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されます。

- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集の packets が 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト packets の送信回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN および RSPAN の設定

ここでは、次の設定について説明します。

- 「SPAN および RSPAN のデフォルト設定」(P.30-9)
- 「ローカル SPAN の設定」(P.30-10)
- 「RSPAN の設定」(P.30-16)

SPAN および RSPAN のデフォルト設定

表 30-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 30-1 SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート (SPAN および RSPAN)	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方 (both)
カプセル化タイプ (宛先ポート)	ネイティブ形式 (タグなしパケット)

表 30-1 SPAN および RSPAN のデフォルト設定 (続き)

機能	デフォルト設定
入力転送 (宛先ポート)	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

ローカル SPAN の設定

ここでは、次の設定について説明します。

- 「SPAN 設定時の注意事項」 (P.30-10)
- 「ローカル SPAN セッションの作成」 (P.30-11)
- 「ローカル SPAN セッションの作成および着信トラフィックの設定」 (P.30-13)
- 「フィルタリングする VLAN の指定」 (P.30-15)

SPAN 設定時の注意事項

SPAN を設定するときには、次の注意事項に従ってください。

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するトラフィックがモニタされるだけです。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー (タグなしまたは IEEE 802.1Q) を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>no monitor session {session_number all local remote}</code>	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ3	<code>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</code>	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートまたは送信元 VLAN を指定します。 <ul style="list-style-type: none"> 送信元 <i>interface-id</i> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel port-channel-number) があります。有効なポートチャネル番号は 1 ~ 6 です。 <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</p> <p>(任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。</p> <ul style="list-style-type: none"> both : 送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 rx : 受信トラフィックをモニタします。 tx : 送信トラフィックをモニタします。 <p>(注) <code>monitor session session_number source</code> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>

	コマンド	目的
ステップ4	monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 (注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 (任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、 encapsulation replicate を入力します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 (注) monitor session <i>session_number</i> destination コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show monitor [session <i>session_number</i>] show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination** **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ~ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサー装置等) 用に着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「[ローカル SPAN セッションの作成](#)」(P.30-11) を参照してください。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。
ステップ3	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx]	SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。

	コマンド	目的
ステップ 4	monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate] [ingress { dot1q vlan <i>vlan-id</i> untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]}	<p>SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。</p> <p><i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。</p> <p><i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</p> <p>(任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、encapsulation replicate を入力します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。</p> <p>宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、ingress をキーワードと一緒に入力します。</p> <ul style="list-style-type: none"> • dot1q vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 • untagged vlan <i>vlan-id</i> または vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show monitor [session <i>session_number</i>] show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination** **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式を使用すると、カプセル化および入力オプションは無視されません。

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>no monitor session {session_number all local remote}</code>	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ3	<code>monitor session session_number source interface interface-id</code>	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ4	<code>monitor session session_number filter vlan vlan-id [, -]</code>	SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ5	<code>monitor session session_number destination {interface interface-id [, -] [encapsulation replicate]}</code>	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 (任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、 encapsulation replicate を入力します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show monitor [session session_number]</code> <code>show running-config</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session session_number filter** グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN の設定

ここでは、次の設定について説明します。

- 「RSPAN 設定時の注意事項」(P.30-16)
- 「RSPAN VLAN としての VLAN の設定」(P.30-17)
- 「RSPAN 送信元セッションの作成」(P.30-18)
- 「RSPAN 宛先セッションの作成」(P.30-19)
- 「RSPAN 宛先セッションの作成および着信トラフィックの設定」(P.30-20)
- 「フィルタリングする VLAN の指定」(P.30-22)

RSPAN 設定時の注意事項

RSPAN を設定するときには、次の注意事項に従ってください。

- 「SPAN 設定時の注意事項」(P.30-10) のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択的にフィルタリングまたはモニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパンニングがサポートされません。

- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
 - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加するすべてのスイッチで RSPAN がサポートされている。
- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがブルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラグディングが防止されます。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッションの RSPAN VLAN となる VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のスイッチ、および中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan vlan-id</code>	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ~ 1001 または 1006 ~ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ~ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 3	<code>remote-span</code>	VLAN を RSPAN VLAN として設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、`no remote-span` VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {<i>session_number</i> all local remote}</code>	セッションに対する既存の RSPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3	<code>monitor session <i>session_number</i> source {interface <i>interface-id</i> vlan <i>vlan-id</i>} [, -] [both rx tx]</code>	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 <ul style="list-style-type: none"> <i>interface-id</i> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel <i>port-channel-number</i>) があります。有効なポートチャネル番号は 1 ~ 48 です。 <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。</p> <ul style="list-style-type: none"> both : 送信トラフィックと受信トラフィックの両方をモニタします。 rx : 受信トラフィックをモニタします。 tx : 送信トラフィックをモニタします。
ステップ 4	<code>monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i></code>	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 <i>session_number</i> には、ステップ 3 で指定した番号を入力します。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。

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

SPAN セッションを削除するには、`no monitor session session_number` グローバル コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、`no monitor session session_number source {interface interface-id | vlan vlan-id}` グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、`no monitor session session_number destination remote vlan vlan-id` コマンドを使用します。

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/2 rx

Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチ（送信元セッションが設定されていないスイッチ）に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>vlan vlan-id</code>	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ~ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ~ 4 は不要です。
ステップ3	<code>remote-span</code>	VLAN を RSPAN VLAN として識別します。
ステップ4	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ5	<code>no monitor session {session_number all local remote}</code>	セッションに対する既存の RSPAN 設定を削除します。 <code>session_number</code> の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除する場合は <code>all</code> 、すべてのローカルセッションを削除する場合は <code>local</code> 、すべてのリモート SPAN セッションを削除する場合は <code>remote</code> をそれぞれ指定します。

	コマンド	目的
ステップ 6	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	monitor session <i>session_number</i> destination interface <i>interface-id</i>	RSPAN セッションおよび宛先インターフェイスを指定します。 <i>session_number</i> には、ステップ 6 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 encapsulation replicate はコマンドラインのヘルプ スtring に表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show monitor [session <i>session_number</i>] show running-config	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session** *session_number* **source remote vlan** *vlan-id* コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet1/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサー装置等) 用に着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「[RSPAN 宛先セッションの作成 \(P.30-19\)](#)」を参照してください。この手順は、RSPAN VLAN がすでに設定されていることを前提にしています。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。

コマンド	目的
ステップ3 monitor session session_number source remote vlan vlan-id	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ4 monitor session session_number destination {interface interface-id [, -] [ingress {dot1q vlan vlan-id untagged vlan vlan-id vlan vlan-id}]}	SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。 <i>session_number</i> には、ステップ 4 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 encapsulation replicate はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、 ingress を追加のキーワードと一緒に入力します。 <ul style="list-style-type: none"> dot1q vlan vlan-id : VLAN をデフォルトの VLAN として指定し、IEEE 802.1Q カプセル化を使用して着信パケットを転送します。 untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ5 end	特権 EXEC モードに戻ります。
ステップ6 show monitor [session session_number] show running-config	設定を確認します。
ステップ7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションを削除するには、**no monitor session session_number** グローバル コンフィギュレーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、**no monitor session session_number destination interface interface-id** グローバル コンフィギュレーション コマンドを使用します。入力オプションは、**no** 形式では無視されます。

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/2 ingress vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3	monitor session <i>session_number</i> source interface <i>interface-id</i>	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 4	monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i>	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show monitor [<i>session session_number</i>] show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session *session_number* filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
(config)# monitor session 2 source interface gigabitethernet1/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination remote vlan 902
```

```
Switch(config)# end
```

SPAN および RSPAN のステータス表示

現在の SPAN または RSPAN 設定を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。また、設定された SPAN および RSPAN セッションを表示するには、**show running-config** 特権 EXEC コマンドを使用できます。



CHAPTER 31

LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定

この章では、IE 3000 スイッチ上でリンク層検出プロトコル (LLDP)、LLDP Media Endpoint Discovery (LLDP-MED)、および有線のロケーション サービスを設定する手順について説明します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

- 「LLDP、LLDP-MED、およびワイヤードロケーションサービスの概要」(P.31-1)
- 「LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定」(P.31-4)
- 「LLDP、LLDP-MED、ワイヤードロケーションサービスのモニタリングとメンテナンス」(P.31-10)

LLDP、LLDP-MED、およびワイヤードロケーションサービスの概要

Cisco Discovery Protocol (CDP) は、すべてのシスコ デバイス (ルータ、ブリッジ、アクセス サーバ、およびスイッチ) のレイヤ 2 (データ リンク層) 上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、ネットワーク接続されている他のシスコ デバイスを自動的に検出し、識別できます。

スイッチでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB リンク層検出プロトコル (LLDP) をサポートしています。LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。このプロトコルはデータ リンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は一連の属性をサポートし、これらを使用してネイバー デバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイス機能、およびデバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV

- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアダバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV (IEEE 802.1 に固有の TLV)
- MAC/PHY コンフィギュレーション/ステータス TLV (IEEE 802.3 に固有の TLV)



(注)

スイッチ スタックは、ネットワーク内で 1 つのスイッチと見なされます。したがって、LLDP は個々のスタック メンバではなく、スイッチ スタックを検出します。

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) は LLDP の拡張版で、IP 電話などのエンドポイント デバイスとスイッチなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet (PoE)、コンポーネント管理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイネーブルです。

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能を識別できます。

- ネットワーク ポリシー TLV

ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 属性をポート上の特定アプリケーションにアダバタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のスイッチに接続し、VLAN 番号を取得してから、コール制御の通信を開始できます。

ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、サービス クラス (CoS)、Differentiated Services Code Point (DSCP)、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。その後、これらのプロファイル属性は、スイッチで中央集約的に保守され、IP 電話に伝播されます。

- 電源管理 TLV

LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。スイッチおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの電源情報を通知することができます。

- コンポーネント管理 TLV

エンドポイントは、スイッチにエンドポイントの詳細なコンポーネント情報を送信することが可能です。コンポーネント情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。

- ロケーション TLV

スイッチからのロケーション情報をエンドポイント デバイスに提供します。ロケーション TLV はこの情報を送信することができます。

- 都市ロケーション情報

都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

– ELIN ロケーション情報

発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号 (ELIN) によって決定されます。これは、緊急通報を **Public Safety Answering Point (PSAP)** にルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

ワイヤード ロケーション サービス

スイッチはワイヤード ロケーション サービス機能を使用して、接続されたデバイスのロケーションおよび接続のトラッキング情報を **Cisco Mobility Services Engine (MSE; モビリティ サービス エンジン)** に送信します。トラッキングされたデバイスは、ワイヤレス エンドポイント、ワイヤード エンドポイント、またはワイヤード スイッチやワイヤード コントローラになります。スイッチは、MSE に **Network Mobility Services Protocol (NMSP; ネットワーク モビリティ サービス プロトコル)** のロケーション通知および接続通知を介して、デバイスのリンク アップ イベントおよびリンク ダウン イベントを通知します。

MSE がスイッチに対して NMSP 接続を開始すると、サーバ ポートが開きます。MSE がスイッチに接続する場合は、バージョンの互換性を確保する 1 組のメッセージ交換およびサービス交換情報があり、その後にロケーション情報の同期が続きます。接続後、スイッチは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンク アップ イベントまたはリンク ダウン イベントは、集約されてインターバルの最後に送信されます。

スイッチがリンク アップ イベントまたはリンク ダウン イベントでデバイスの有無を確認した場合は、スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固有情報を取得します。クライアントが LLDP-MED または CDP に対応している場合は、スイッチは LLDP-MED ロケーション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク アップ時に取得します。

- ポート接続で指定されたスロットおよびポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名 (該当する場合)。
- デバイス カテゴリは、*wired station* として指定されます。
- ステータスは *new* として指定されます。
- シリアル番号、UDI。
- モデル番号
- スイッチによる関連付け検出後の時間 (秒)。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク ダウン時に取得します。

- 切断されたスロットおよびポート。
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名 (該当する場合)。
- デバイス カテゴリは、*wired station* として指定されます。
- ステータスは *delete* として指定されます。

- シリアル番号、UDI。
- スイッチによる関連付け解除の検出後の時間（秒）。

スイッチがシャットダウンする場合は、スイッチは、MSE との NMSP 接続を終了する前に、ステート *delete* および IP アドレスとともに接続情報通知を送信します。MSE は、この通知を、スイッチに関連付けられているすべてのワイヤード クライアントに対する関連付け解除として解釈します。

スイッチ上のロケーションアドレスを変更すると、スイッチは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定

- 「デフォルトの LLDP 設定」(P.31-4)
- 「設定時の注意事項」(P.31-4)
- 「LLDP のイネーブル化」(P.31-5)
- 「LLDP 特性の設定」(P.31-6)
- 「LLDP-MED TLV の設定」(P.31-6)
- 「Network-Policy TLV の設定」(P.31-7)
- 「ロケーション TLV およびワイヤード ロケーション サービスの設定」(P.31-9)

デフォルトの LLDP 設定

表 31-1 デフォルトの LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル（すべての TLV との送受信）
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 送信	ディセーブル
LLDP med-tlv-select	ディセーブル（すべての LLDP-MED TLV への送信）。LLDP がグローバルにイネーブルにされると、LLDP-MED-TLV もイネーブルになります。

設定時の注意事項

- インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。

- 最初にインターフェイス上にネットワークポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。**switchport voice vlan vlan-id** がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシー プロファイルを持つインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。
- プライベート VLAN ポート上では、ネットワーク ポリシー プロファイルを設定できません。
- ワイヤード ロケーションが機能するためには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

LLDP のイネーブル化

LLDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	lldp run	スイッチ上で LLDP をイネーブルに設定します。
ステップ3	interface interface-id	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	lldp transmit	LLDP パケットを送信するようにインターフェイスをイネーブルにします。
ステップ5	lldp receive	LLDP パケットを受信するようにインターフェイスをイネーブルにします。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show lldp	設定を確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LLDP をディセーブルにするには、**no lldp run** グローバル コンフィギュレーション コマンドを使用します。インターフェイス上の LLDP をディセーブルにするには、**no lldp transmit** および **no lldp receive** インターフェイス コンフィギュレーション コマンドを使用します。

次に、LLDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

LLDP 特性を設定するには、特権 EXEC モードで次の手順を実行します。



(注) ステップ 2 ~ 5 は任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>lldp holdtime seconds</code>	(任意) デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ~ 65535 秒です。デフォルトは 120 秒です。
ステップ 3	<code>lldp reinit delay</code>	(任意) 任意のインターフェイス上で LLDP の初期化の遅延時間 (秒) を指定します。 指定できる範囲は 2 ~ 5 秒です。デフォルトは 2 秒です。
ステップ 4	<code>lldp timer rate</code>	(任意) インターフェイス上で LLDP の更新の遅延時間 (秒) を指定します。 指定できる範囲は 5 ~ 65534 秒です。デフォルトは 30 秒です。
ステップ 5	<code>lldp tlv-select</code>	(任意) 送受信する LLDP TLV を指定します。
ステップ 6	<code>lldp med-tnv-select</code>	(任意) 送受信する LLDP-MED TLV を指定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show lldp</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各 LLDP コマンドの **no** 形式を使用します。

次に、LLDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

LLDP-MED TLV の設定

デフォルトでは、スイッチはエンドデバイスから LLDP-MED パケットを受信するまで、LLDP パケットだけを送信します。スイッチは、MED TLV を持つ LLDP も送信します。LLDP-MED エントリが期限切れになった場合は、スイッチは再び LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用することで、表 31-2 に示された TLV を送信しないようにインターフェイスを設定できます。

表 31-2 LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイス上で TLV をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	lldp med-tlv-select tlv	イネーブルにする TLV を指定します。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

Network-Policy TLV の設定

ネットワーク ポリシー プロファイルを作成し、ポリシー属性を設定して、インターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	network-policy profile profile number	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポリシー コンフィギュレーション モードを開始します。指定できる範囲は 1 ~ 4294967295 です。

コマンド	目的
ステップ 3 {voice voice-signaling} vlan [vlan-id {cos cvalue dscp dvalue}] [[dot1p {cos cvalue dscp dvalue}] none untagged]	<p>ポリシー属性を設定します。</p> <p>voice : 音声アプリケーション タイプを指定します。</p> <p>voice-signaling : 音声シグナリング アプリケーション タイプを指定します。</p> <p>vlan : 音声トラフィックのネイティブ VLAN を指定します。</p> <p>vlan-id : (任意) 音声トラフィックの VLAN を指定します。指定できる範囲は 1 ~ 4094 です。</p> <p>cos cvalue : (任意) 設定された VLAN のレイヤ 2 プライオリティ サービス クラス (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルトは 0 です。</p> <p>dscp dvalue : (任意) 設定された VLAN の Differentiated Services Code Point (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルトは 0 です。</p> <p>dot1p : (任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように IP 電話を設定します。</p> <p>none : (任意) 音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。</p> <p>untagged : (任意) タグなしの音声トラフィックを送信するように IP 電話を設定します。これが IP Phone のデフォルト設定になります。</p>
ステップ 4 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5 interface interface-id	ネットワーク ポリシー プロファイルを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6 network-policy profile number	ネットワークポリシー プロファイルの番号を指定します。
ステップ 7 lldp med-tlv-select network-policy	ネットワーク ポリシー TLV を指定します。
ステップ 8 end	特権 EXEC モードに戻ります。
ステップ 9 show network-policy profile	設定を確認します。
ステップ 10 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワーク ポリシー プロファイルおよびネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
Switch(config-network-policy)# voice vlan dot1p dscp 34
```

ロケーション TLV およびワイヤード ロケーション サービスの設定

エンドポイントのロケーション情報を設定し、その設定をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	location { admin-tag <i>string</i> civic-location identifier <i>id</i> elin-location <i>string identifier id</i> }	エンドポイントにロケーション情報を設定します。 <ul style="list-style-type: none"> admin-tag : 管理タグまたはサイト情報を指定します。 civic-location : 都市ロケーション情報を指定します。 elin-location : 緊急ロケーション情報 (ELIN) を指定します。 identifier id : 都市ロケーションの ID を指定します。 <i>string</i> : サイト情報またはロケーション情報を英数字形式で指定します。
ステップ 3	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	interface <i>interface-id</i>	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	location { additional-location-information <i>word</i> civic-location-id <i>id</i> elin-location-id <i>id</i> }	インターフェイスにロケーション情報を入力します。 <p>additional-location-information : ロケーションまたは場所の追加情報を指定します。</p> <p>civic-location-id : インターフェイスのグローバル都市ロケーション情報を指定します。</p> <p>elin-location-id : インターフェイスの緊急ロケーション情報を指定します。</p> <p><i>id</i> : 都市ロケーションまたは ELIN ロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。</p> <p><i>word</i> : 追加のロケーション情報を指定する語またはフレーズを指定します。</p>
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show location admin-tag <i>string</i> または show location civic-location identifier <i>id</i> または show location elin-location identifier <i>id</i>	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの **no** 形式を使用します。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
```

```
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

スイッチ上でワイヤード ロケーション サービスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。



(注) スイッチは暗号化されたソフトウェア イメージを実行して、**nmosp** グローバル コンフィギュレーション コマンドをイネーブルにする必要があります。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	nmosp enable	NMSP 機能をスイッチ上でイネーブルにします。
ステップ 3	nmosp notification interval {attachment location} interval-seconds	NMSP 通知間隔を指定します。 attachment : 接続通知間隔を指定します。 location : 位置通知間隔を指定します。 interval-seconds : スイッチから MSE にロケーション更新または接続更新が送信されるまでの期間 (秒)。指定できる範囲は 1 ~ 30 です。デフォルト値は 30 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show network-policy profile	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチ上で NMSP をイネーブルにして、位置通知間隔を 10 秒に設定する方法を示します。

```
Switch(config)# nmosp enable
Switch(config)# nmosp notification interval location 10
```

LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス

デバイス上の LLDP、LLDP-MED、およびワイヤード ロケーション サービスをモニタリングおよびメンテナンスするには、特権 EXEC モードで次の作業を 1 回以上実行します。

コマンド	説明
clear lldp counters	トラフィック カウンタをゼロにリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmosp statistics	NMSP 統計情報カウンタを消去します。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間のよ うな、インターフェイス上のグローバル情報を表示します。

コマンド	説明
show lldp entry <i>entry-name</i>	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [<i>interface-id</i>]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [<i>interface-id</i>] [detail]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタ類を表示します。
show location admin-tag <i>string</i>	指定した管理タグまたはサイトのロケーション情報を表示します。
show location civic-location identifier <i>id</i>	特定のグローバル都市ロケーションのロケーション情報を表示します。
show location elin-location identifier <i>id</i>	緊急ロケーションのロケーション情報を表示します。
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。
show nmosp	NMSP 情報を表示します。



CHAPTER 32

CDP の設定



(注)

この章では、IE 3000 スイッチに Cisco Discovery Protocol (CDP) を設定する手順について説明します。この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

- 「CDP の概要」 (P.32-1)
- 「CDP の設定」 (P.32-2)
- 「CDP のモニタおよびメンテナンス」 (P.32-5)

CDP の概要

CDP はすべてのシスコ デバイス (ルータ、ブリッジ、アクセス サーバ、およびスイッチ) のレイヤ 2 (データリンク層) で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコ デバイスを検出できます。また、下位レイヤのトランスペアレント プロトコル稼働しているネイバー デバイスのデバイス タイプや、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) エージェント アドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンド スイッチから最大 3 台 (デフォルト) 離れたクラスタ対応の他のデバイスについての情報を維持します。

スイッチおよび Cisco Medianet が稼働している接続されたエンドポイント デバイスの場合は、次のようになります。

- CDP は、スイッチと直接通信する接続されたエンドポイントを識別します。
- ネイバー デバイスのレポートが重複しないように、1 つの有線スイッチだけがロケーション情報をレポートします。
- 有線スイッチとエンドポイントは、ロケーションの送信と受信の両方を行います。

詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html

スイッチは CDP バージョン 2 をサポートします。

CDP の設定

ここでは、次の設定について説明します。

- 「[CDP のデフォルト設定](#)」 (P.32-2)
- 「[CDP の特性の設定](#)」 (P.32-3)
- 「[CDP のディセーブル化およびイネーブル化](#)」 (P.32-3)
- 「[インターフェイス上での CDP のディセーブル化およびイネーブル化](#)」 (P.32-4)

CDP のデフォルト設定

表 32-1 に、CDP のデフォルト設定を示します。

表 32-1 CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー (パケット更新頻度)	60 秒
CDP ホールドタイム (廃棄までの時間)	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の特性の設定

CDP 更新の頻度、廃棄するまで情報を保持する期間、およびバージョン 2 アドバタイズを送信するかどうかを設定できます。

CDP タイマー、ホールドタイム、およびアドバタイズ タイプを設定するには、特権 EXEC モードで次の手順を実行します。



(注) ステップ 2 ~ 4 はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>cdp timer seconds</code>	(任意) CDP 更新の送信頻度 (秒) を設定します。 指定できる範囲は 5 ~ 254 です。デフォルトは 60 秒です。
ステップ3	<code>cdp holdtime seconds</code>	(任意) デバイスから送信された情報を受信側デバイスが廃棄するまで保持する期間を指定します。 指定できる範囲は 10 ~ 255 秒です。デフォルトは 180 秒です。
ステップ4	<code>cdp advertise-v2</code>	(任意) バージョン 2 アドバタイズを送信するように CDP を設定します。 これがデフォルトの状態になります。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show cdp</code>	設定値を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

次に、CDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

その他の CDP `show` コマンドについては、「[CDP のモニタおよびメンテナンス](#)」(P.32-5) を参照してください。

CDP のディセーブル化およびイネーブル化

CDP はデフォルトでイネーブルです。



(注) スイッチ クラスタと他のシスコ デバイス (Cisco IP Phone など) は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。詳細については、[第 6 章「スイッチのクラスタ化」](#)を参照してください。

CDP デバイス検出機能をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	CDP をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

次に、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

インターフェイス上での CDP のディセーブル化およびイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

ポート上で CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no cdp enable	インターフェイス上で CDP をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定のポート上で、ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>cdp enable</code>	インターフェイス上で、ディセーブル化されている CDP をイネーブルにします。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、特定のポート上で、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```



(注) CDP がスイッチ インターフェイスでディセーブルの場合は、音声 VLAN がポート セキュリティにカウントされません。

CDP のモニタおよびメンテナンス

デバイス上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
<code>clear cdp counters</code>	トラフィック カウンタをゼロにリセットします。
<code>clear cdp table</code>	ネイバーに関する情報を格納する CDP テーブルを削除します。
<code>show cdp</code>	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を表示します。
<code>show cdp entry entry-name [protocol version]</code>	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
<code>show cdp interface [interface-id]</code>	CDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 必要なインターフェイスの情報だけを表示できます。

コマンド	説明
<code>show cdp neighbors [interface-id]</code> <code>[detail]</code>	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
<code>show cdp traffic</code>	CDP カウンタ（送受信されたパケット数、チェックサム エラーなど）を表示します。



CHAPTER 33

UDLD の設定

この章では、IE 3000 スイッチに単一方向リンク検出 (UDLD) プロトコルを設定する方法について説明します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「UDLD の概要」 (P.33-1)
- 「UDLD の設定」 (P.33-3)
- 「UDLD ステータスの表示」 (P.33-7)

UDLD の概要

UDLD は、光ファイバまたはツイストペアイーサネットケーブルを通して接続されたデバイスからケーブルの物理設定をモニタしたり、単一方向リンクの存在を検出したりできるようにするためのレイヤ 2 プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパンニングツリートポロジープをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、ノーマル (デフォルト) とアグレッシブの 2 つの動作モードをサポートしています。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブモードの UDLD は、光ファイバリンクおよびツイストペアリンク上の片方向トラフィックと、光ファイバリンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モードの UDLD は、光ファイバポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされません。

アグレッシブモードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブモードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバリンクまたはツイストペアリンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバリンクまたはツイストペアリンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイントリンクでは、UDLD hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブモードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で hello パケット（別名アドバタイズまたはプローブ）を定期的送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

スイッチが hello メッセージを受信すると、エージングタイム（ホールドタイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュエントリの期限が切れる前に、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

UDLD の稼働中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはスイッチをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュエントリをすべて消去します。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

- イベントドリブン検出およびエコー

UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコーメッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

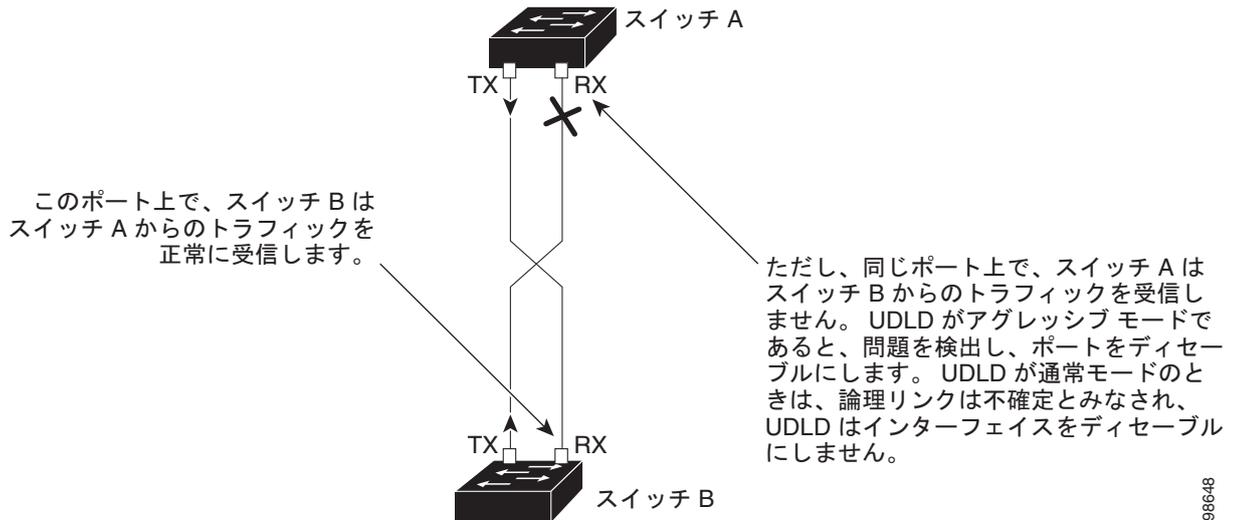
検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされません。UDLD がアグレッシブモードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュエントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブモードをイネーブルにしている、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンクステータスが不確定のままの場合、UDLD はポートをシャットダウンします。

図 33-1 に、単一方向リンク条件の例を示します。

図 33-1 UDLD による単一方向リンクの検出



98648

UDLD の設定

ここでは、次の設定について説明します。

- 「UDLD のデフォルト設定」 (P.33-4)
- 「設定時の注意事項」 (P.33-4)
- 「UDLD のグローバルなイネーブル化」 (P.33-5)
- 「インターフェイス上での UDLD のイネーブル化」 (P.33-5)
- 「UDLD によってディセーブル化されたインターフェイスのリセット」 (P.33-6)

UDLD のデフォルト設定

表 33-1 に、UDLD のデフォルト設定を示します。

表 33-1 UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート (光ファイバ メディア用)	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート (ツイストペア (銅製) メディア用)	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

設定時の注意事項

UDLD 設定時の注意事項を次に示します。

- UDLD は Asynchronous Transfer Mode (ATM; 非同期転送モード) ポート上ではサポートされていません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。
- モード (通常またはアグレッシブ) を設定する場合、リンクの両側に同じモードを設定します。



注意

ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは標準モードで UDLD をイネーブルにし、スイッチのすべての光ファイバポートに設定可能なメッセージ タイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>udld {aggressive enable message time message-timer-interval}</code>	UDLD の動作モードを指定します。 <ul style="list-style-type: none"> • aggressive : すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • enable : スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、udld enable グローバル コンフィギュレーション コマンドの設定を上書きします。 アグレッシブおよび通常モードの詳細については、「動作モード (P.33-1)」を参照してください。 • message time message-timer-interval : アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プローブ メッセージ間の間隔を設定します。指定できる範囲は 1 ~ 90 秒です。 <p>(注) このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、udld インターフェイス コンフィギュレーション コマンドを使用します。詳細については、「インターフェイス上での UDLD のイネーブル化 (P.33-5)」を参照してください。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show udld</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD をグローバルにディセーブルにするには、**no udld enable** グローバル コンフィギュレーション コマンドを使用して、すべての光ファイバ ポート上で標準モードの UDLD をディセーブルにします。すべての光ファイバ ポート上でアグレッシブ モードの UDLD をディセーブルにする場合は、**no udld aggressive** グローバル コンフィギュレーション コマンドを使用します。

インターフェイス上での UDLD のイネーブル化

ポート上で、UDLD をアグレッシブ モードまたは通常モードでイネーブルにするか、または UDLD をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	UDLD のためにイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	<code>udld port [aggressive]</code>	UDLD はデフォルトでディセーブルです。 <ul style="list-style-type: none"> • udld port : 指定されたポート上で、UDLD を通常モードでイネーブルにします。 • udld port aggressive : 指定されたポート上で、UDLD をアグレッシブ モードでイネーブルにします。 <p>(注) 特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、no udld port インターフェイス コンフィギュレーション コマンドを使用します。</p> <p>アグレッシブおよび通常モードの詳細については、「動作モード」(P.33-1) を参照してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show udld interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD によってディセーブル化されたインターフェイスのリセット

UDLD によってディセーブルにされたすべてのポートをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>udld reset</code>	UDLD によってディセーブルにされたすべてのポートをリセットします。
ステップ 2	<code>show udld</code>	設定を確認します。

次のコマンドを使用して、ポートを起動することもできます。

- **shutdown** インターフェイス コンフィギュレーション コマンドに続けて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブルのポートを再起動できます。
- **no udld { aggressive | enable}** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port [aggressive]** インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバ ポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の **errdisable** ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを入力すると、UDLD の **errdisable** ステートから回復する時間を指定できます。

UDLD ステータスの表示

指定されたポートまたはすべてのポートの UDLD ステータスを表示するには、**show udld** [*interface-id*] 特権 EXEC コマンドを使用します。

コマンド出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 34

RMON の設定

この章では、IE 3000 スイッチにリモート ネットワーク モニタリング (RMON) を設定する手順について説明します。

RMON は、RMON 準拠のコンソール システムとネットワーク プローブ間で交換可能な一連の統計情報と機能を定義した標準モニタリング仕様です。RMON によって、総合的なネットワーク障害診断、プランニング、パフォーマンス チューニングに関する情報が得られます。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』(Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) の「System Management Commands」の項を参照してください。

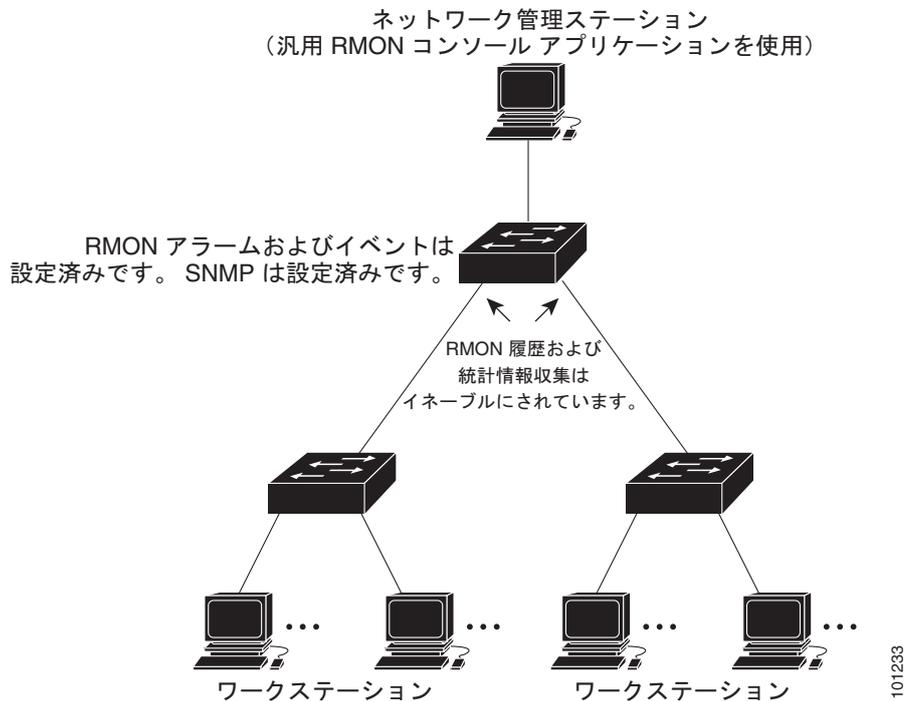
この章の内容は、次のとおりです。

- 「RMON の概要」(P.34-1)
- 「RMON の設定」(P.34-3)
- 「RMON ステータスの表示」(P.34-6)

RMON の概要

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) 標準モニタリング仕様です。図 34-1 のように、RMON 機能をスイッチの Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) エージェントと組み合わせて使用することによって、接続されているすべての LAN セグメント上のスイッチ間で流れるすべてのトラフィックをモニタリングできます。

図 34-1 リモート モニタリングの例



スイッチは次の RMON グループ (RFC 1757 で規定) をサポートしています。

- 統計情報 (RMON グループ 1) : インターフェイス上のイーサネットの統計情報 (スイッチ タイプとサポートされているインターフェイスに応じた、ファストイーサネットやギガビットイーサネット統計情報など) を収集します。
- 履歴 (RMON グループ 2) : 指定されたポーリング間隔で、イーサネットポート上 (スイッチタイプおよびサポートされるインターフェイスに応じた、ファストイーサネットおよびギガビットイーサネット統計情報を含む) の統計情報グループの履歴を収集します。
- アラーム (RMON グループ 3) : 指定された期間、特定の MIB (管理情報ベース) オブジェクトをモニタリングし、指定された値 (上限しきい値) でアラームを発生し、別の値 (下限しきい値) でアラームをリセットします。アラームはイベントと組み合わせて使用できます。アラームがイベントを発生させ、イベントによってログ エントリまたは SNMP トラップが生成されるようになります。
- イベント (RMON グループ 9) : アラームによってイベントが発生したときのアクションを指定します。アクションは、ログ エントリまたは SNMP トラップを生成できます。

このソフトウェア リリースがサポートするスイッチは、RMON データの処理にハードウェア カウンタを使用するので、モニタが効率的になり、処理能力はほとんど必要ありません。



(注)

64 ビット カウンタは、RMON アラームではサポートされていません。

RMON の設定

ここでは、次の設定について説明します。

- 「RMON のデフォルト設定」(P.34-3)
- 「RMON アラームおよびイベントの設定」(P.34-3) (必須)
- 「インターフェイス上でのグループ履歴統計情報の収集」(P.34-5) (任意)
- 「インターフェイス上でのイーサネット グループ統計情報の収集」(P.34-6) (任意)

RMON のデフォルト設定

RMON はデフォルトでディセーブルです。アラームまたはイベントは設定されていません。

RMON アラームおよびイベントの設定

スイッチを RMON 対応として設定するには、コマンドライン インターフェイス (CLI) または SNMP 準拠の Network Management Station (NMS; ネットワーク管理ステーション) を使用します。NMS 上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用することを推奨します。RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。詳細については、第 36 章「SNMP の設定」を参照してください。



(注) 64 ビット カウンタは、RMON アラームではサポートされていません。

RMON アラームおよびイベントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>rmon alarm number variable interval {absolute delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	MIB オブジェクトにアラームを設定します。 <ul style="list-style-type: none"> <code>number</code> には、アラーム番号を指定します。指定できる範囲は 1 ~ 65535 です。 <code>variable</code> には、モニタ対象の MIB オブジェクトを指定します。 <code>interval</code> には、アラームが MIB 変数をモニタリングする時間を秒数で指定します。指定できる範囲は 1 ~ 4294967295 秒です。 各 MIB 変数を直接テストする場合は、absolute キーワードを指定します。MIB 変数のサンプル間の変動をテストする場合は、delta キーワードを指定します。 <code>value</code> には、アラームを発生させる値およびアラームがリセットされる値を指定します。上限および下限しきい値に指定できる範囲は -2147483648 ~ 2147483647 です。 (任意) <code>event-number</code> には、上限および下限しきい値が限度を超えた場合に発生させるイベントの番号を指定します。 (任意) <code>owner string</code> には、アラームの所有者を指定します。
ステップ 3	<code>rmon event number [description string] [log] [owner string] [trap community]</code>	RMON イベント番号に対応付けられた RMON イベント テーブルにイベントを追加します。 <ul style="list-style-type: none"> <code>number</code> には、イベント番号を割り当てます。指定できる範囲は 1 ~ 65535 です。 (任意) <code>description string</code> には、イベントの説明を指定します。 (任意) イベント発生時に RMON ログ エントリを生成する場合は、log キーワードを使用します。 (任意) <code>owner string</code> には、イベントの所有者を指定します。 (任意) <code>trap community</code> には、このトラップ用の SNMP コミュニティ スtring を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アラームをディセーブルにするには、設定した各アラームに対して、**no rmon alarm number** グローバル コンフィギュレーション コマンドを使用します。設定したすべてのアラームを一度にディセーブルにすることはできません。イベントをディセーブルにするには、**no rmon event number** グローバル コンフィギュレーション コマンドを使用します。アラームおよびイベントの詳細および相互作用については、RFC 1757 を参照してください。

任意の MIB オブジェクトにアラームを設定できます。次の例では、**rmon alarm** コマンドを使用して、RMON アラーム番号 10 を設定します。このアラームは、ディセーブルにされない限り、20 秒ごとに 1 度の間隔で MIB 変数 *ifEntry.20.1* をモニタリングし、変数の上下の変動をチェックします。*ifEntry.20.1* 値で MIB カウンタが 100000 から 100015 になるなど、15 以上増加すると、アラームが発生します。そのアラームによってさらにイベント番号 1 が発生します。イベント番号 1 は、**rmon event** コマンドで設定されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。*ifEntry.20.1* 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

次に、**rmon event** コマンドを使用して RMON イベント番号 1 を作成する例を示します。このイベントは *High ifOutErrors* と定義され、アラームによってイベントが発生したときに、ログ エントリが生成されます。ユーザ *jjones* が、このコマンドによってイベント テーブルに作成される行を所有します。次の例の場合も、イベント発生時に SNMP トラップが生成されます。

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

インターフェイス上でのグループ履歴統計情報の収集

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

インターフェイス上でグループ履歴統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	履歴を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	rmon collection history index [buckets bucket-number] [interval seconds] [owner ownername]	指定されたバケット数および時間で、履歴収集をイネーブルにします。 <ul style="list-style-type: none"> <i>index</i> には、RMON 統計グループを指定します。指定できる範囲は 1 ~ 65535 です。 (任意) buckets bucket-number には、RMON 統計グループ履歴収集に必要な最大バケット数を指定します。指定できる範囲は 1 ~ 65535 です。デフォルトのバケット数は 50 です。 (任意) interval seconds には、ポーリング サイクルを秒数で指定します。指定できる範囲は 1 ~ 3600 です。デフォルトは 1800 秒です。 (任意) owner ownername には、RMON 統計グループの所有者名を入力します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。

	コマンド	目的
ステップ 6	<code>show rmon history</code>	スイッチ履歴テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

履歴収集をディセーブルにするには、`no rmon collection history index` インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイス上でのイーサネット グループ統計情報の収集

インターフェイス上でイーサネット統計グループを収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	統計情報を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>rmon collection stats index [owner ownername]</code>	インターフェイス上で RMON 統計情報収集をイネーブルにします。 <ul style="list-style-type: none"> <code>index</code> には、RMON 統計グループを指定します。有効な範囲は 1 ~ 65535 です。 (任意) <code>owner ownername</code> には、RMON 統計グループの所有者名を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>show rmon statistics</code>	スイッチ統計テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

イーサネット統計グループの収集をディセーブルにするには、`no rmon collection stats index` インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、所有者 `root` の RMON 統計情報を収集する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rmon collection stats 2 owner root
```

RMON ステータスの表示

RMON ステータスを表示するには、表 34-1 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 34-1 RMON ステータスを表示するコマンド

コマンド	目的
<code>show rmon</code>	汎用 RMON 統計情報を表示します。
<code>show rmon alarms</code>	RMON アラーム テーブルを表示します。
<code>show rmon events</code>	RMON イベント テーブルを表示します。

表 34-1 RMON ステータスを表示するコマンド (続き)

コマンド	目的
<code>show rmon history</code>	RMON 履歴テーブルを表示します。
<code>show rmon statistics</code>	RMON 統計情報テーブルを表示します。

これらの表示のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』(Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) の「System Management Commands」の項を参照してください。



CHAPTER 35

システム メッセージ ログिंगの設定

この章では、IE 3000 スイッチにシステム メッセージ ログिंगを設定する方法について説明します。



(注) この章で使用されるコマンドの構文と使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。このドキュメントは、Cisco.com の次の場所にあります。[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]

この章の内容は、次のとおりです。

- 「システム メッセージ ログिंगの概要」 (P.35-1)
- 「システム メッセージ ログिंगの設定」 (P.35-2)
- 「ログिंग設定の表示」 (P.35-14)



注意

高レートでコンソールへのメッセージを記録すると、CPU の使用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ログिंगの概要

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をログング プロセスに送信します。ログング プロセスはログ メッセージを各宛先（設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ログング プロセスは、コンソールにもメッセージを送信します。



(注) Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

ログング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

ログングされたシステム メッセージにアクセスするには、スイッチのコマンドライン インターフェイス (CLI) を使用するか、または適切に設定された Syslog サーバにこれらのシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージを内部バッファに保存します。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポート経由でスイッチにアクセスします。

システム メッセージ ログングの設定

ここでは、次の設定について説明します。

- 「システム ログ メッセージのフォーマット」 (P.35-2)
- 「システム メッセージ ログングのデフォルト設定」 (P.35-3)
- 「メッセージ ログングのディセーブル化」 (P.35-4) (任意)
- 「メッセージ表示宛先デバイスの設定」 (P.35-5) (任意)
- 「ログ メッセージの同期化」 (P.35-6) (任意)
- 「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」 (P.35-8) (任意)
- 「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」 (P.35-8) (任意)
- 「メッセージ重大度の定義」 (P.35-9) (任意)
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」 (P.35-10) (任意)
- 「設定変更ロガーのイネーブル化」 (P.35-11) (任意)
- 「UNIX Syslog サーバの設定」 (P.35-12) (任意)

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号 (%)、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報 (設定されている場合) で構成されています。メッセージは、次のフォーマットで表示されます。

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime [localtime] [msec] [show-timezone]**、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 35-1 に、Syslog メッセージの要素を示します。

表 35-1 システム ログ メッセージの要素

要素	説明
<i>seq no:</i>	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「 ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 (P.35-8) を参照してください。
<i>timestamp</i> のフォーマット： <i>mm/dd hh:mm:ss</i> または <i>hh:mm:ss</i> (短時間) または <i>d h</i> (長時間)	メッセージまたはイベントの日時です。 service timestamps log [datetime log] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。 詳細については、「 ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 (P.35-8) を参照してください。
<i>facility</i>	メッセージが参照する機能 (SNMP、SYS など) です。サポートされる機能の一覧については、 表 35-4 (P.35-14) を参照してください。
<i>severity</i>	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。重大度の詳細については、 表 35-3 (P.35-10) を参照してください。
<i>MNEMONIC</i>	メッセージを一意に示すテキスト ストリングです。
<i>description</i>	レポートされているイベントの詳細を示すテキスト ストリングです。

次に、スイッチ システム メッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

システム メッセージ ログイングのデフォルト設定

表 35-2 に、システム メッセージ ログイングのデフォルト設定を示します。

表 35-2 システム メッセージ ログイングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ログイング	イネーブル。
コンソールの重大度	debugging (および数値的により低いレベル。 表 35-3 (P.35-10) を参照)
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ

表 35-2 システム メッセージ ログイングのデフォルト設定 (続き)

機能	デフォルト設定
タイム スタンプ	ディセーブル
同期ログイング	ディセーブル
ログイング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
設定変更ロガー	ディセーブル
サーバ機能	Local7 (表 35-4 (P.35-14) を参照)
サーバの重大度	informational (および数値的により低いレベル。 表 35-3 (P.35-10) を参照)

メッセージ ログイングのディセーブル化

メッセージ ログイングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ログイングをイネーブルにする必要があります。メッセージ ログイングがイネーブルの場合、ログ メッセージはログイング プロセスに送信されます。ログイング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

メッセージ ログイングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no logging console	メッセージ ログイングをディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config または show logging	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ログイング プロセスがディセーブルの場合、メッセージは生成後すぐに (通常はコマンド出力に割り込む形で) コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、**Return** を押さなければメッセージが表示されません。詳細については、「[ログ メッセージの同期化](#)」(P.35-6) を参照してください。

メッセージ ログイングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先デバイスの設定

メッセージ ログイングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。メッセージの受信場所を指定するには、特権 EXEC モードで次のコマンドを 1 つまたは複数使用します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>logging buffered [size]</code>	<p>スイッチの内部バッファへのメッセージを記録します。指定できる範囲は 4096 ~ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。</p> <p>スイッチに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。ステップ 4 を参照してください。</p> <p>(注) バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、show memory 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。</p>
ステップ 3	<code>logging host</code>	<p>UNIX Syslog サーバ ホストにメッセージを記録します。</p> <p><i>host</i> には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。</p> <p>ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。</p> <p>Syslog サーバの設定手順については、「UNIX Syslog サーバの設定 (P.35-12)」を参照してください。</p>
ステップ 4	<code>logging file flash:filename</code> [<i>max-file-size</i> [<i>min-file-size</i>]] [<i>severity-level-number</i> <i>type</i>]	<p>フラッシュ メモリ内のファイルにログ メッセージを保存します。</p> <ul style="list-style-type: none"> <i>filename</i> には、ログ メッセージのファイル名を入力します。 (任意) <i>max-file-size</i> には、ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ~ 2147483647 です。デフォルトは 4096 バイトです。 (任意) <i>min-file-size</i> には、ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ~ 2147483647 です。デフォルトは 2048 バイトです。 (任意) <i>severity-level-number</i> <i>type</i> には、ログイングの重大度またはログイング タイプを指定します。重大度に指定できる範囲は 0 ~ 7 です。ログイング タイプ キーワードの一覧については、表 35-3 (P.35-10) を参照してください。デフォルトでは、デバッグ メッセージ、および数値的により低いレベルのメッセージがログ ファイルに送信されます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>terminal monitor</code>	<p>現在のセッション中に、コンソール以外の端末にメッセージを記録します。</p> <p>端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。</p>

	コマンド	目的
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ログ メッセージが内部バッファにコピーされます。循環バッファなので、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。バッファ内の最も古いメッセージが最初に表示されます。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

特定の PoE に対応したポートで Power over Ethernet (PoE) イベントのログिंगをイネーブルにしたリディセーブルにしたリするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。これらのポートへのログिंगは、デフォルトでイネーブルです。

コンソールへのログिंगをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。ファイルへのログिंगをディセーブルにするには、**no logging file [severity-level-number | type]** グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ログिंगがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザ プロンプトを再表示します。

同期ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	line [console vty] line-number [ending-line-number]	<p>メッセージの同期ログイングを行うように、回線を設定します。</p> <ul style="list-style-type: none"> • スイッチのコンソール ポートを介して行われる設定には、console キーワードを使用します。 • 同期ログイングをイネーブルにする vty 回線を指定するには、line vty line-number コマンドを使用します。Telnet セッションを介して行われる設定には、vtty 接続を使用します。回線番号に指定できる範囲は 0 ~ 15 です。 <p>16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。</p> <p>line vty 0 15</p> <p>また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。</p> <p>line vty 2</p> <p>このコマンドを入力すると、ライン コンフィギュレーション モードになります。</p>
ステップ3	logging synchronous [level [severity-level all] limit number-of-buffers]	<p>メッセージの同期ログイングをイネーブルにします。</p> <ul style="list-style-type: none"> • (任意) level severity-level には、メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 • (任意) level all を指定すると、重大度に関係なく、すべてのメッセージが非同期に出力されます。 • (任意) limit number-of-buffers には、キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 20 です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show running-config	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、**no logging synchronous [level severity-level | all] [limit number-of-buffers]** ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

ログ メッセージのタイム スタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service timestamps log uptime または service timestamps log datetime [msec] [localtime] [show-timezone]	ログのタイム スタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動した後の経過時間が表示されます。 2 番目のコマンドを実行すると、ログ メッセージのタイム スタンプがイネーブルになります。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間 (ミリ秒)、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デバッグ メッセージとログ メッセージの両方のタイム スタンプをディセーブルにするには、**no service timestamps** グローバル コンフィギュレーション コマンドを使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service sequence-numbers	シーケンス番号をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

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

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のログイング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します (表 35-3 を参照)。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>logging console level</code>	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 35-3 (P.35-10) を参照)。
ステップ3	<code>logging monitor level</code>	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 35-3 (P.35-10) を参照)。
ステップ4	<code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します (表 35-3 (P.35-10) を参照)。 Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.35-12) を参照してください。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show running-config</code> または <code>show logging</code>	設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) *level* を指定すると、このレベルのメッセージ、および数値的により低いレベルのメッセージが宛先に表示されます。

コンソールへのログをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのログをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのログをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 35-3 に *level* キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 35-3 メッセージ ログ level キーワード

level キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ~ **emergencies** の重大度で表示されます。このタイプのメッセージは、スイッチの機能に影響があることを示します。この誤動作からの回復手順については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- debug** コマンドの出力：**debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center (TAC) でのみ使用されます。
- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP Network Management Station (NMS; ネットワーク管理ステーション) に送信されるように Syslog メッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ (表 35-3 (P.35-10) を参照) が、履歴テーブルに 1 つ格納されます。

重大度および履歴テーブル サイズのデフォルト値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>logging history level¹</code>	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。 <i>level</i> キーワードのリストについては、表 35-3 (P.35-10) を参照してください。 デフォルトでは、 warnings 、 errors 、 critical 、 alerts 、および emergencies のメッセージが送信されます。
ステップ3	<code>logging history size number</code>	履歴テーブルに格納できる Syslog メッセージ数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ~ 500 です。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

1. 表 35-3 に、*level* キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合 (`logging history size` グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合) は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのログイングをデフォルトの重大度に戻すには、`no logging history` グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、`no logging history size` グローバル コンフィギュレーション コマンドを使用します。

設定変更ロガーのイネーブル化

コマンドライン インターフェイス (CLI) で行った設定変更をトラッキングするために設定ロガーをイネーブルにすることができます。`logging enable` 設定変更ロガー コンフィギュレーション コマンドを入力すると、設定変更用に入力されたセッション、ユーザおよびコマンドがログに記録されます。設定ログのサイズは 1 ~ 1000 エントリの間で設定することができます (デフォルトは 100)。`no logging enable` コマンドの後に `logging enable` コマンドを入力してログイングをディセーブルにして再びイネーブルにすることで、いつでもログをクリアすることができます。

`show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning]` 特権 EXEC コマンドを使用して、設定ログ全体または指定したパラメータのログを表示します。

デフォルトで設定ログイングはディセーブルになっています。

コマンドの詳細については、次の URL にアクセスして『Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T』を参照してください。

設定ログをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ3	log config	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ4	logging enable	設定変更ログをイネーブルにします。
ステップ5	logging size entries	(任意) 設定ログで取得するエントリ数を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 100 です。 (注) 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show archive log config	設定ログを表示することでエントリを確認します。

次に、設定変更ロガーをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

設定ログの出力例は次のとおりです。

```
Switch# show archive log config all
idx  sess      user@line      Logged command
 38   11   unknown user@vty3 |no aaa authorization config-commands
 39   12   unknown user@vty3 |no aaa authorization network default group radius
 40   12   unknown user@vty3 |no aaa accounting dot1x default start-stop group
radius
 41   13   unknown user@vty3 |no aaa accounting system default
 42   14           temi@vty4      |interface GigabitEthernet4/0/1
 43   14           temi@vty4      | switchport mode trunk
 44   14           temi@vty4      | exit
 45   16           temi@vty5      |interface FastEthernet5/0/1
 46   16           temi@vty5      | switchport mode trunk
 47   16           temi@vty5      | exit
```

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ログング機能を定義する手順について説明します。

UNIX Syslog デーモンへのログ メッセージ

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。この手順は任意です。

root としてログインし、次のステップを実行します。



(注) 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ログイングをイネーブルにするには、Syslog コマンドラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

ステップ 1 /etc/syslog.conf ファイルに次のような行を 1 行追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

local7 キーワードは、使用するログイング機能を指定します。機能の詳細については、表 35-4 (P.35-14) を参照してください。**debug** キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 35-3 (P.35-10) を参照してください。Syslog デーモンは、これ以上の重大度の場合に、次のフィールドで指定されたファイルにメッセージを送信します。このファイルは、Syslog デーモンに書き込み権限がある既存ファイルでなければなりません。

ステップ 2 UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3 Syslog デーモンに新しい設定を認識させます。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

UNIX システム ログイング機能の設定

システム ログ メッセージを外部デバイスに送信する場合は、メッセージを UNIX Syslog 機能から送信されたメッセージとして特定するようにシステムを設定できます。

UNIX システム機能メッセージ ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	logging host	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを記録します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

	コマンド	目的
ステップ 3	<code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれより下のレベルのメッセージを受信します。 <i>level</i> キーワードについては、表 35-3 (P.35-10) を参照してください。
ステップ 4	<code>logging facility facility-type</code>	Syslog 機能を設定します。 <i>facility-type</i> キーワードについては、表 35-4 (P.35-14) を参照してください。 デフォルトは <code>local7</code> です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、`no logging host` グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのログイングをディセーブルにするには、`no logging trap` グローバル コンフィギュレーション コマンドを入力します。

表 35-4 に、ソフトウェアでサポートされている UNIX システム機能を示します。これらの機能の詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 35-4 ログイング facility-type キーワード

facility-type キーワード	説明
<code>auth</code>	許可システム
<code>cron</code>	cron 機能
<code>daemon</code>	システム デーモン
<code>kern</code>	カーネル
<code>local0 ~ local7</code>	ローカルに定義されたメッセージ
<code>lpr</code>	ライン プリンタ システム
<code>mail</code>	メール システム
<code>news</code>	USENET ニュース
<code>sys9 ~ sys14</code>	システムで使用
<code>syslog</code>	システム ログ
<code>user</code>	ユーザ プロセス
<code>uucp</code>	UNIX から UNIX へのコピー システム

ログイング設定の表示

ログイング設定およびログ バッファの内容を表示するには、`show logging` 特権 EXEC コマンドを使用します。この場合に表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Configuration Fundamentals Command Reference, Release 12.2』を参照してください。



CHAPTER 36

SNMP の設定

この章では、IE 3000 スイッチに簡易ネットワーク管理プロトコル (SNMP) を設定する方法について説明します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスおよび『*Cisco IOS Network Management Command Reference, Release 12.4*』を参照してください。

- 「SNMP の概要」 (P.36-1)
- 「SNMP の設定」 (P.36-6)
- 「SNMP ステータスの表示」 (P.36-19)

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージフォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB (管理情報ベース) で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System (NMS; ネットワーク管理システム) に統合できます。エージェントおよび MIB は、スイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワークデータの保存場所である MIB から値を収集します。また、エージェントはマネージャからのデータ取得要求または設定要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンクステータス (アップまたはダウン)、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

ここでは、次の概要について説明します。

- 「SNMP バージョン」 (P.36-2)
- 「SNMP マネージャ機能」 (P.36-3)
- 「SNMP エージェント機能」 (P.36-4)
- 「SNMP コミュニティストリング」 (P.36-4)
- 「SNMP を使用して MIB 変数にアクセスする方法」 (P.36-4)

- 「SNMP 通知」 (P.36-5)
- 「SNMP ifIndex MIB オブジェクト値」 (P.36-6)

SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1 : RFC1157 に規定された SNMP (完全インターネット標準)。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティベースの管理およびセキュリティフレームワークをコミュニティストリングベースの管理フレームワークに置き換えたものです。次の機能があります。
 - SNMPv2 : RFC 1902 ~ 1907 に規定された SNMP バージョン 2 (ドラフト版インターネット標準)
 - SNMPv2C : RFC 1901 に規定された SNMPv2 のコミュニティストリングベースの管理フレームワーク (試験版インターネットプロトコル)
- SNMPv3 : SNMP のバージョン 3 は、RFC 2273 ~ 2275 に規定されている相互運用可能な標準ベースプロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
 - メッセージの完全性 : パケットが伝送中に改ざんされないようにします。
 - 認証 : メッセージの送信元が有効かどうかを判別します。
 - 暗号化 : パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。



(注) 暗号化を選択するには、**priv** キーワードを入力します。このキーワードは、暗号化ソフトウェアイメージがインストールされている場合のみ使用可能です。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラーメッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラーコードが使用されています。これらのエラーは、SNMPv1 では単一のエラーコードで報告されます。SNMPv2 では、エラーリターンコードでエラータイプが報告されるようになりました。

SNMPv3 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティモデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。セキュリティレベルとセキュリティモデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティメカニズムが決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

表 36-1 に、セキュリティ モデルとセキュリティ レベルのさまざまな組み合わせについて、その特性を示します。

表 36-1 SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	Username	No	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	No	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv authPriv (暗号化ソフトウェアイメージが必要)	MD5 または SHA	Data Encryption Standard (DES; データ暗号化規格) または Advanced Encryption Standard (AES; 高度暗号化規格)	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。次の暗号化アルゴリズムで、User-based Security Model (USM) を指定できます。 <ul style="list-style-type: none"> CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化 3DES 168 ビット暗号化 AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 36-2 に示す動作を実行します。

表 36-2 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 ¹
get-bulk-request ²	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

- この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
- get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップメッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパンニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ スtring

SNMP コミュニティ スtring は、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ スtring 定義が、スイッチ上の 3 つのコミュニティ スtring 定義の少なくとも 1 つと一致していなければなりません。

コミュニティ スtring の属性は、次の 3 つのいずれかです。

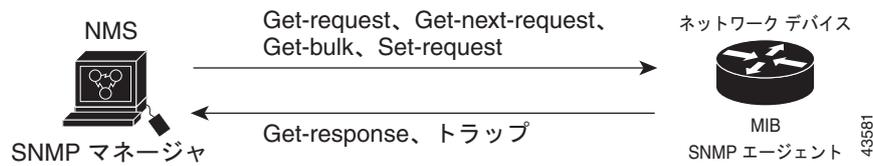
- Read-Only (RO)：許可された管理ステーションに、コミュニティ スtring を除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write (RW)：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ スtring に対するアクセスは許可しません。
- クラスタを作成すると、コマンドスイッチがメンバスイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に設定された RW および RO コミュニティ スtring にメンバスイッチ番号 (@esN、N はスイッチ番号) を追加し、これらのスString をメンバスイッチに伝播します。詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 36-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリーに応答します。

図 36-1 SNMP ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード *traps* はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。



(注) SNMPv1 は *informs* をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうか送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなる原因になります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチ メモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である **interface index** (ifIndex) オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチのソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、表 36-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 36-3 ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI	1 ~ 4999
EtherChannel	5001 ~ 5048
種類とポート番号に基づく物理 (ギガビット イーサネットまたは SFP モジュール インターフェイスなど)	10000 ~ 14500
ヌル	10501
ループバックおよびトンネル	24567 +



(注)

スイッチは、範囲内の連続した値を使用しない場合があります。

SNMP の設定

- 「SNMP のデフォルト設定」 (P.36-7)
- 「SNMP 設定時の注意事項」 (P.36-7)
- 「SNMP エージェントのディセーブル化」 (P.36-8)
- 「コミュニティ スtring の設定」 (P.36-8)
- 「SNMP グループおよびユーザの設定」 (P.36-10)
- 「SNMP 通知の設定」 (P.36-13)
- 「CPU しきい値通知のタイプと値の設定」 (P.36-17)
- 「エージェント コンタクトおよびロケーションの設定」 (P.36-17)
- 「SNMP を通して使用する TFTP サーバの制限」 (P.36-18)
- 「SNMP の例」 (P.36-18)

SNMP のデフォルト設定

表 36-4 に、SNMP のデフォルト設定を示します。

表 36-4 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル ¹
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ (tty) 以外は、イネーブルではありません。
SNMP バージョン	version キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで noauth (noAuthNoPriv) になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

- これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン ID は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合は、以下の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザに対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。通知ビューの設定が必要な状況については、『*Cisco IOS Network Management Command Reference*』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth** (**authNoPriv**) および **priv** (**authPriv**) の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。(コマンドラインで入力された) ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に

従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、`snmp-server user username` グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ スtring も再設定する必要があります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no snmp-server</code>	SNMP エージェントの動作をディセーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`no snmp-server` グローバル コンフィギュレーション コマンドを使用すると、デバイスで稼働中のすべてのバージョン (バージョン 1、バージョン 2C、バージョン 3) がディセーブルになります。SNMP をイネーブルにする特定の Cisco IOS コマンドは存在しません。最初に入力する `snmp-server` グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

コミュニティ スtring の設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ スtring を使用します。コミュニティ スtring は、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。スString に対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ スString を使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server community string [view view-name] [ro rw] [access-list-number]</code>	<p>コミュニティ ストリングを設定します。</p> <p>(注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。</p> <ul style="list-style-type: none"> <code>string</code> には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 (任意) <code>view</code> には、コミュニティがアクセスできるビュー レコードを指定します。 (任意) 許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用 (<code>ro</code>)、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き (<code>rw</code>) を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 (任意) <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>(任意) ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します (コミュニティ ストリングに値を入力しないでください)。

特定のコミュニティ ストリングを削除するには、`no snmp-server community string` グローバル コンフィギュレーション コマンドを使用します。

次に、ストリング *comaccess* を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト 4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名 (エンジン ID) を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上で SNMP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server engineID {local <i>engineid-string</i> remote <i>ip-address</i> [<i>udp-port port-number</i>] <i>engineid-string</i>}</code>	<p>SNMP のローカル コピーまたはリモート コピーの名前を設定します。</p> <ul style="list-style-type: none"> <i>engineid-string</i> は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。たとえば、123400000000000000000000 というエンジン ID を設定する場合、<code>snmp-server engineID local 1234</code> のように入力できます。 <code>remote</code> を指定した場合、SNMP のリモート コピーが置かれているデバイスの <i>ip-address</i> を指定し、任意でリモート デバイスの UDP ポートを指定します。デフォルト値は 162 です。

コマンド	目的
ステップ 3 snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	<p>リモート デバイスに新規 SNMP グループを設定します。</p> <ul style="list-style-type: none"> • <i>groupname</i> には、グループを指定します。 • セキュリティ モデルを指定します。 <ul style="list-style-type: none"> – v1 は、最も安全性の低いセキュリティ モデルです。 – v2c は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を送送できます。 – 最も安全な v3 の場合、認証レベルを選択する必要があります。 <p>auth : MD5 および SHA によるパケット認証が可能です。</p> <p>noauth : noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、これがデフォルトです。</p> <p>priv : DES によるパケット暗号化をイネーブルにします (<i>privacy</i> と呼ばれます)。</p> <p>(注) priv キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。</p> <ul style="list-style-type: none"> • (任意) read <i>readview</i> とともに、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) write <i>writeview</i> とともに、データを入力し、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) notify <i>notifyview</i> とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) access <i>access-list</i> とともに、アクセス リスト名のストリング (64 文字以下) を入力します。

	コマンド	目的
ステップ4	<pre>snmp-server user username groupname {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]} [priv {des 3des aes {128 192 256}} priv-password]</pre>	<p>SNMP グループに対して新規ユーザを追加します。</p> <ul style="list-style-type: none"> • <i>username</i> は、エージェントに接続するホスト上のユーザ名です。 • <i>groupname</i> は、ユーザが対応付けられるグループの名前です。 • remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルト値は 162 です。 • SNMP バージョン番号 (v1、v2c、または v3) を入力します。v3 を入力する場合は、次のオプションを追加します。 <ul style="list-style-type: none"> – encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードが指定されている場合のみ使用可能です。 – auth は認証レベル設定セッションで、HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。パスワードストリング <i>auth-password</i> (64 文字以下) が必要です。 • v3 を入力してスイッチが暗号化ソフトウェアイメージを実行中の場合は、プライベート (priv) 暗号化およびパスワードストリング <i>priv-password</i> (64 文字以下) の設定もできます。 <ul style="list-style-type: none"> – priv は、User-based Security Model (USM) を指定します。 – des は、56 ビット DES アルゴリズムの使用を指定します。 – 3des は、168 ビット DES アルゴリズムの使用を指定します。 – aes は、DES アルゴリズムの使用を指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 • (任意) access access-list とともに、アクセスリスト名のストリング (64 文字以下) を入力します。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	<p>設定を確認します。</p> <p>(注) auth noauth priv モード設定に関する SNMPv3 情報を表示するには、show snmp user 特権 EXEC コマンドを入力する必要があります。</p>
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているスイッチでは、トラップ マネージャを無制限に設定できます。



(注)

コマンド構文で *traps* というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

表 36-5 に、サポートされているスイッチ トラップ (通知タイプ) を示します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host host-addr informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

表 36-5 スwitchの通知タイプ

通知タイプのキーワード	説明
bgp	ボーダー ゲートウェイ プロトコル (BGP) 状態変化トラップを生成します。このオプションは、拡張マルチレイヤ イメージがインストールされている場合だけ使用できます。
bridge	Spanning-Tree Protocol (STP; スパニングツリー プロトコル) ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
cpu threshold	CPU に関連したトラップをイネーブルにします。
envmon	環境モニタ トラップを生成します。ファン (fan)、シャットダウン (shutdown)、ステータス (status)、電源 (supply)、温度 (temperature) の環境トラップのいずれかまたはすべてをイネーブルにできます。
errdisable	ポート VLAN が errdisable ステートになった場合に、トラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 10000 です。デフォルトは 0 で、レート制限がないという意味です。
flash	SNMP FLASH 通知を生成します。
hsrp	Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol (MSDP) が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First (OSPF) が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。

表 36-5 スイッチの通知タイプ (続き)

通知タイプのキーワード	説明
pim	Protocol-Independent Multicast (PIM) が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント (RP) マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 (注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 <ul style="list-style-type: none"> • snmp-server enable traps port-security • snmp-server enable traps port-security trap-rate rate
rtr	SNMP Response Time Reporter (RTR) のトラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 に設定されています (制限なしの状態では、発生ごとにトラップが送信されます)。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) が変更された場合に、トラップを生成します。



(注) **fru-ctrl**、**insertion**、および **removal** キーワードは、コマンドラインのヘルプ スtring に表示されますが、サポートされていません。

表 36-5 に示す通知タイプを受信するには、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID remote ip-address engineid-string	リモート ホスト用のエンジン ID を指定します。

コマンド	目的
ステップ3 snmp-server user <i>username</i> <i>groupname</i> { remote <i>host</i> [udp-port <i>port</i>]} { v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted [access <i>access-list</i>] [auth { md5 sha } <i>auth-password</i>]}]}	ステップ 2 で設定したリモート ホストと対応付ける SNMP ユーザを設定します。 (注) アドレスに対応するリモート ユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラー メッセージが表示され、コマンドが実行されません。
ステップ4 snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	SNMP グループを設定します。
ステップ5 snmp-server host <i>host-addr</i> [informs traps] [version { 1 2c 3 { auth noauth priv }}] <i>community-string</i> [<i>notification-type</i>]	SNMP トラップ動作の受信側を指定します。 <ul style="list-style-type: none"> • <i>host-addr</i> には、ホスト (対象となる受信側) の名前またはインターネット アドレスを指定します。 • (任意) SNMP 情報をホストに送信するには、informs を指定します。 • (任意) SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。 • (任意) SNMP version (1、2c、または 3) を指定します。SNMPv1 は informs をサポートしていません。 • (任意) バージョン 3 の場合、認証レベルとして auth、noauth、または priv を選択します。 (注) priv キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。 <ul style="list-style-type: none"> • <i>community-string</i> には、version 1 または version 2c が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティ スtring を入力します。version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。 (注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ スtring の一部として @ 記号を使用しないでください。 <ul style="list-style-type: none"> • (任意) <i>notification-type</i> には、表 36-5 (P.36-13) に記載されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。

コマンド	目的
ステップ 6 snmp-server enable traps <i>notification-types</i>	<p>スイッチがトラップまたは情報を送信できるようにし、送信する通知のタイプを指定します。通知タイプの一覧については、表 36-5 (P.36-13) を参照するか、snmp-server enable traps ? と入力してください。</p> <p>複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに snmp-server enable traps コマンドを個別に入力する必要があります。</p> <p>(注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。</p> <ul style="list-style-type: none"> • snmp-server enable traps port-security • snmp-server enable traps port-security trap-rate rate
ステップ 7 snmp-server trap-source <i>interface-id</i>	(任意) 送信元インターフェイスを指定します。そこからトラップ メッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 8 snmp-server queue-length <i>length</i>	(任意) 各トラップ ホストのメッセージ キュー長を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 10 です。
ステップ 9 snmp-server trap-timeout <i>seconds</i>	(任意) トラップ メッセージを再送信する間隔を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。
ステップ 10 end	特権 EXEC モードに戻ります。
ステップ 11 show running-config	設定を確認します。
ステップ 12 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

snmp-server host コマンドでは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドによって、指定された通知メカニズム (トラップおよび情報) がグローバルでイネーブルになります。ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host host** グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用してください。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps notification-types** グローバル コンフィギュレーション コマンドを使用します。

CPU しきい値通知のタイプと値の設定

CPU しきい値通知のタイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>process cpu threshold type {total process interrupt} rising percentage interval seconds [falling fall-percentage interval seconds]</code>	<p>CPU しきい値通知のタイプと値を設定します。</p> <ul style="list-style-type: none"> total : 通知タイプを CPU 使用率の合計に設定します。 process : 通知タイプを CPU プロセス使用率に設定します。 interrupt : 通知タイプを CPU 割り込み使用率に設定します。 rising percentage : CPU リソースのパーセンテージ (1 ~ 100)。設定された間隔を過ぎると CPU しきい値通知を送信します。 interval seconds : CPU しきい値超過の秒単位の持続時間 (5 ~ 86400)。この条件が満たされると CPU しきい値通知を送信します。 falling fall-percentage : CPU リソースのパーセンテージ (1 ~ 100)。設定された間隔の間、使用率がこのレベルより低下すると、CPU しきい値通知を送信します。 <p>この値は、rising percentage の値以下である必要があります。この値を指定しないと、falling fall-percentage の値は rising percentage の値と同じになります。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>snmp-server contact text</code>	<p>システムに関する問い合わせ先を表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server contact Dial System Operator at beeper 21555.</pre>
ステップ3	<code>snmp-server location text</code>	<p>システムのロケーションを表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server location Building 3/Room 222</pre>
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP を通して使用する TFTP サーバの制限

SNMP を通してコンフィギュレーション ファイルを保存およびロードするために使用する TFTP（簡易ファイル転送プロトコル）サーバを、アクセス リストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server tftp-server-list access-list-number</code>	SNMP を通してコンフィギュレーション ファイルをコピーするために使用する TFTP サーバを、アクセス リスト内のサーバに限定します。 <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP の例

次に、SNMP の全バージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング `public` を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

```
Switch(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング `public` を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33（SNMPv1 を使用）や、ホスト 192.180.1.27（SNMPv2C を使用）へ VTP トラップを送信します。コミュニティ ストリング `public` は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の *snmp-server host* コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードのときに **auth** (**authNoPriv**) 認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、表 36-6 に記載されたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。この場合に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

表 36-6 SNMP 情報を表示するためのコマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID [local remote]	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。

表 36-6 SNMP 情報を表示するためのコマンド (続き)

機能	デフォルト設定
<code>show snmp sessions</code>	現在の SNMP セッションの情報を表示します。
<code>show snmp user</code>	SNMP ユーザテーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドは、 auth noauth priv モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、 show running-config の出力には表示されません。



CHAPTER 37

組み込みイベント マネージャの設定

Embedded Event Manager (EEM; 組み込みイベント マネージャ) は、Cisco IOS デバイス内でイベント検出および回復のために配布されカスタマイズされたアプローチです。EEM はイベントを監視する機能を提供します。また、監視されたイベントが発生するかしきい値に達した場合に情報を得たり、是正措置を行ったり、または他の EEM 処理を実行したりする機能も提供します。EEM ポリシーは、イベントおよびイベントが発生した場合に行う処理を定義します。

この章では、EEM の使用方法と IE3000 スイッチで EEM を設定する方法について説明します。この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチのコマンド リファレンスおよび『Cisco IOS Network Management Command Reference』を参照してください。EEM の完全なマニュアルセットについては、『Cisco IOS Network Management Configuration Guide』の以下のマニュアルを参照してください。

- *Embedded Event Manager Overview*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- *Writing Embedded Event Manager Policies Using the Cisco IOS CLI*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html
- *Writing Embedded Event Manager Policies Using Tcl*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html



(注)

この機能は、IP サービス イメージが稼働しているスイッチでだけサポートされます。

この章で説明する内容は、次のとおりです。

- 「組み込みイベント マネージャの概要」(P.37-1)
- 「組み込みイベント マネージャの設定」(P.37-5)
- 「組み込みイベント マネージャ情報の表示」(P.37-7)

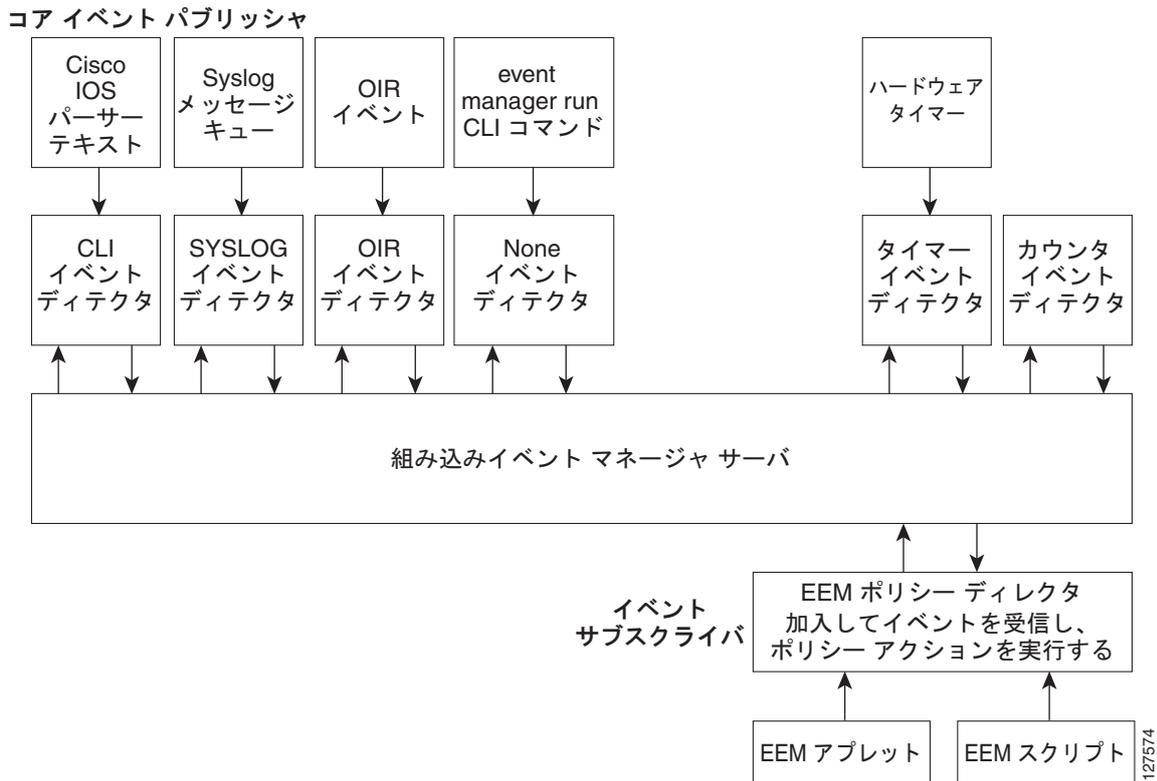
組み込みイベント マネージャの概要

EEM はキー システムのイベントを監視し、セット ポリシーを通してイベントに作用します。このポリシーはプログラムされたスクリプトで、これを使用して、発生した特定の一連のイベントに基づいて処理を呼び出すように、スクリプトをカスタマイズできます。このスクリプトは、カスタム Syslog または Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップの生成、CLI (コマンドライン インターフェイス) コマンドの呼び出し、フェールオーバーの強制などの処理を生成します。スイッチからすべてのイベント管理を管理できるわけではなく、何らかの問題によつ

て、スイッチと外部ネットワーク管理デバイス間の通信に障害が発生することがあるため、EEM のイベント管理機能は役立ちます。スイッチをリブートすることなく自動回復処理が行われる場合、ネットワークの可用性は向上します。

図 37-1 に、EEM サーバ、コア イベント パブリッシャ (イベント検出器)、およびイベント サブスクリバ (ポリシー) の関係を示します。イベントパブリッシャはイベントを選別し、イベント サブスクリバによって提供されたイベント仕様と一致するときに、それらをパブリッシュします。イベントが発生すると、イベント検出器が EEM サーバに通知します。次に、システムの現在の状態と特定のイベントに対してポリシーで指定された処理に基づいて、EEM ポリシーが回復を実行します。

図 37-1 組み込みイベントマネージャ コア イベント検出器



EEM の導入例については、『[EEM Configuration for Cisco Integrated Services Router Platforms Guide](#)』を参照してください。

- 「イベント検出器」 (P.37-2)
- 「組み込みイベントマネージャの処理」 (P.37-4)
- 「組み込みイベントマネージャポリシー」 (P.37-4)
- 「組み込みイベントマネージャの環境変数」 (P.37-4)

イベント検出器

イベント検出器として知られる EEM ソフトウェアは、EEM イベントがいつ発生するかを決定します。イベント検出器は、SNMP などのモニタ対象のエージェントとアクションを実装可能な EEM ポリシー間のインターフェイスを提供する個別のシステムです。

- アプリケーション特有のイベント検出器：任意の EEM ポリシーがイベントをパブリッシュできます。
- IOS CLI イベント検出器：CLI によって入力されたコマンドに基づいてポリシーを生成します。
- カウンタ イベント検出器：ネームド カウンタが指定されたしきい値を超えたとき、イベントをパブリッシュします。
- インターフェイス カウンタ イベント検出器：指定したインターフェイスの汎用 Cisco IOS インターフェイス カウンタが定義したしきい値を超えると、イベントをパブリッシュします。しきい値は絶対値か増分値で指定できます。たとえば、増分値を 50 に設定した場合、インターフェイス カウンタが 50 増えると、イベントがパブリッシュされます。

この検出器は、エントリ値と終了値の変化率に基づいて、インターフェイスに関するイベントをパブリッシュします。
- None イベント検出器：**event manager run CLI** コマンドが EEM ポリシーを実行するとき、イベントをパブリッシュします。EEM は、ポリシー内のイベント仕様に基づいて、ポリシーをスケジューリングして実行します。EEM ポリシーは、**event manager run** コマンドが実行される前に、手動で識別して登録する必要があります。
- Online Insertion and Removal (OIR; 活性挿抜) イベント検出器：ハードウェアの挿入または取り外し (OIR) イベントが発生したときに、イベントをパブリッシュします。
- リソースしきい値イベント検出器：グローバル プラットフォームの値およびしきい値に基づいて、ポリシーを生成します。CPU の利用率および残りのバッファ容量などのリソースを含みます。
- Remote procedure call (RPC; リモート プロシージャ コール)：Secure Shell (SSH; セキュア シェル) を使用した暗号化接続を介してスイッチの外側から EEM ポリシーを起動し、XML ベースのメッセージ交換に、Simple Object Access Protocol (SOAP) データ符号化を使用します。さらに、EEM ポリシーを実行してから、SOAP XML フォーマットの応答内の出力を取得します。
- SNMP イベント検出器：次の場合に、標準 SNMP MIB オブジェクトをモニタし、イベントを生成できます。
 - オブジェクトが指定した値と一致するか指定したしきい値を超える。
 - 期間の開始時における監視対象の Object Identifier (OID; オブジェクト ID) 値と、イベントがパブリッシュされたときの実際の OID 値の違いである SNMP デルタ値が、指定された値と一致する。
- SNMP 通知イベント検出器：スイッチが受信した SNMP トラップおよび通知メッセージを代行受信します。着信メッセージが指定された値と一致するか、定義されたしきい値を超えたとき、イベントがパブリッシュされます。
- Syslog イベント検出器：正規表現パターンマッチを持つ Syslog メッセージを選別できます。選別されたメッセージをさらに限定し、指定された時間内に特定の回数の発生を記録するように要求できます。指定されたイベント基準での一致により、設定されたポリシー処理がトリガーされます。
- タイマー イベント検出器：次のイベントをパブリッシュします。
 - absolute-time-of-day タイマーは、指定された絶対的な日時が発生したとき、イベントをパブリッシュします。
 - カウントダウン タイマーは、タイマーがゼロにカウントダウンされたとき、イベントをパブリッシュします。
 - ウォッチドッグ タイマーは、タイマーがゼロにカウントダウンされたとき、イベントをパブリッシュします。タイマーは初期値に自動リセットされ、再びカウントダウンを開始します。
 - CRON タイマーは、UNIX 標準 CRON 仕様を使用して、イベントをパブリッシュする時期を定義することによって、イベントをパブリッシュします。CRON タイマーは、1 分間にイベントを複数回パブリッシュすることはありません。

- ウォッチドック イベント検出器 (IOSWDSysMon) : 次の場合に、イベントをパブリッシュします。
 - Cisco IOS プロセスでの CPU の利用率がしきい値を超えたとき
 - Cisco IOS プロセスでのメモリの利用率がしきい値を超えたとき
- 同時に 2 つのイベントを監視でき、イベントがパブリッシュされる基準は、いずれかまたは両方のイベントが指定されたしきい値を超えた場合です。

組み込みイベント マネージャの処理

イベントに反応して次の処理が発生します。

- ネームドカウンタの修正
- アプリケーション特有のイベントのパブリッシュ
- SNMP トラップの生成
- 優先される Syslog メッセージの生成
- Cisco IOS ソフトウェアのリロード

組み込みイベント マネージャ ポリシー

EEM はイベントを監視して情報を提供するか、または監視されたイベントが発生するかしきい値に達した場合には是正措置を行うことができます。EEM ポリシーは、イベントおよびイベントが発生した場合に行う処理を定義するエンティティです。

EEM ポリシーにはアプレットとスクリプトの 2 つのタイプがあります。アプレットは、CLI 設定内で定義される簡易なポリシーです。イベントの選択基準とイベントが発生した場合に行う処理を定義する簡易な方法です。スクリプトは、ASCII エディタを使用して、ネットワーク デバイス上で定義されます。スクリプト (バイトコード (.tbc) とテキスト (.tcl) スクリプトで作成できます) は、次に、ネットワーク デバイスにコピーされ、EEM によって登録されます。さらに、1 つの .tcl ファイルに複数のイベントを登録できます。

EEM を使用して、EEM ポリシー Tool Command Language (TCL; ツール コマンド言語) スクリプトを使用する独自のポリシーを記述して実行します。

キーワード拡張という形のシスコの TCL 機能拡張は、EEM ポリシーの開発を容易にします。これらのキーワードは、検出されたイベント、その後の処理、ユーティリティ情報、カウンタ値、およびシステム情報を識別します。

EEM ポリシーおよびスクリプトの設定の詳細については、『Cisco IOS Network Management Configuration Guide, Release 12.4T』を参照してください。

組み込みイベント マネージャの環境変数

EEM は EEM ポリシーで環境変数を使用します。これらの変数は、CLI コマンドと **event manager environment** コマンドを実行することにより、EEM ポリシー TCL スクリプトで定義されます。

- ユーザ定義の変数
 - ユーザ定義のポリシーに対して、ユーザにより定義されます。
- シスコ定義の変数
 - 特定のサンプル ポリシーに対して、シスコにより定義されます。

- シスコ組み込み変数 (EEM アプレットで使用可能)

シスコにより定義され、読み取り専用または読み取りと書き込みに設定できます。読み取り専用変数は、アプレットが実行を開始する前に、システムによって設定されます。1 つの読み取りと書き込み変数 `_exit_status` により、同期イベントからトリガーされるポリシーの終了ステータスを設定できます。

シスコ定義の環境変数とシスコ システム定義環境変数は、特定の 1 つのイベント検出器またはすべてのイベント検出器に適用されます。ユーザ定義の環境変数またはサンプル ポリシーでシスコにより定義される環境変数は、**event manager environment** グローバル コンフィギュレーション コマンドを使用して設定されます。ポリシーを登録する前に、変数を EEM ポリシーに定義する必要があります。

EEM がサポートする環境変数の詳細については、『Cisco IOS Network Management Configuration Guide, Release 12.4T』を参照してください。

組み込みイベント マネージャの設定

- 「組み込みイベント マネージャ アプレットの登録と定義」 (P.37-5)
- 「組み込みイベント マネージャ TCL スクリプトの登録と定義」 (P.37-6)

組み込みイベント マネージャの設定の詳細については、『Cisco IOS Network Management Configuration Guide, Release 12.4T』を参照してください。

組み込みイベント マネージャ アプレットの登録と定義

EEM でアプレットを登録し、**event applet** および **action applet** コンフィギュレーション コマンドを使用して EEM アプレットを定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>event manager applet <i>applet-name</i></code>	EEM でアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ3	<code>event snmp oid oid-value get-type {exact next} entry-op {gt ge eq ne lt le} entry-val entry-val [exit-comb {or and}] [exit-op {gt ge eq ne lt le}] [exit-val exit-val] [exit-time exit-time-val] poll-interval poll-int-val</code>	EEM アプレットを稼働させるイベント基準を指定します。 (任意) 終了基準。終了基準を指定しない場合、イベント モニタリングがすぐに再イネーブル化されます。
ステップ4	<code>action label syslog [priority priority-level] msg msg-text</code>	EEM アプレットがトリガーされたときの処理を指定します。この処理を繰り返して、アプレットに他の CLI コマンドを追加します。 <ul style="list-style-type: none"> (任意) プライオリティ キーワードは、Syslog メッセージのプライオリティ レベルを指定します。選択した場合、プライオリティ レベル引数を定義する必要があります。 <code>msg-text</code> の場合、引数は文字テキスト、環境変数、またはこの 2 つを組み合わせたものになります。
ステップ5	<code>end</code>	アプレット コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、SNMP オブジェクト ID によって指定されたフィールドの 1 つが定義されたしきい値を超えた場合の EEM での出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

次に、EEM イベントに反応して行われる処理の例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"
Switch (config-applet)# action 2.0 force-switchover
```

組み込みイベント マネージャ TCL スクリプトの登録と定義

EEM で TCL スクリプトを登録し、TCL スクリプトとポリシー コマンドを定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	show event manager environment [all variable-name]	(任意) show event manager environment コマンドは、EEM 環境変数の名前と値を表示します。 (任意) all キーワードは、EEM 環境変数を表示します。 (任意) variable-name 引数は、指定された環境変数に関する情報を表示します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	event manager environment variable-name string	指定された EEM 環境変数の値を設定します。要求されたすべての環境変数でこのステップを繰り返します。
ステップ 5	event manager policy policy-file-name [type system] [trap]	EEM ポリシーを登録し、ポリシー内で定義された特定のイベントが発生した場合に実行されるようにします。
ステップ 6	exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、`show event manager environment` コマンドの出力例を示します。

```
Switch# show event manager environment all
No. Name Value
1 _cron_entry 0-59/2 0-23/1 * * 0-6
2 _show_cmd show ver
3 _syslog_pattern .*UPDOWN.*Ethernet1/0.*
4 _config_cmd1 interface Ethernet1/0
5 _config_cmd2 no shut
```

次に、ソフトウェアによって割り当てられた CRON タイマー環境変数を毎日の毎時間、毎分、毎秒に設定する方法を示します。

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

次に、システム ポリシーとして登録された `tm_cli_cmd.tcl` という名前の EEM ポリシーの例を示します。システム ポリシーは Cisco IOS イメージの一部です。ユーザ定義の TCL スクリプトは、最初にフラッシュ メモリにコピーする必要があります。

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

組み込みイベント マネージャ情報の表示

EEE に関する情報 (EEM の登録されたポリシーや EEM の履歴データを含む) を表示するには、『*Cisco IOS Network Management Command Reference*』を参照してください。



CHAPTER 38

ACL によるネットワーク セキュリティの設定

この章では、アクセス コントロール リスト (ACL) (アクセス リストとも呼ばれる) を使用して、IE 3000 スイッチにネットワーク セキュリティを設定する手順について説明します。この章では、IP ACL の参考資料は IP Version 4 (IPv4) の ACL を対象としています。IPv6 ACL の詳細については、[第 45 章「IPv6 ACL の設定」](#)を参照してください。

この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

- [「ACL の概要」 \(P.38-1\)](#)
- [「IPv4 ACL の設定」 \(P.38-6\)](#)
- [「名前付き MAC 拡張 ACL の作成」 \(P.38-28\)](#)
- [「VLAN マップの設定」 \(P.38-31\)](#)
- [「ルータ ACL を VLAN マップと組み合わせて使用する方法」 \(P.38-38\)](#)
- [「IPv4 ACL の設定の表示」 \(P.38-43\)](#)

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィック

の種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

ACL には、Access Control Entry (ACE; アクセス コントロール エントリ) の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

スイッチは、IP ACL とイーサネット (MAC) ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル (UDP)、インターネット グループ管理プロトコル (IGMP)、およびインターネット制御メッセージ プロトコル (ICMP) などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service (QoS) 分類 ACL もサポートしています。詳細については、「[QoS ACL に基づく分類](#)」(P.39-8) を参照してください。

ここでは、次の概要について説明します。

- 「[サポートされる ACL](#)」(P.38-2)
- 「[フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理](#)」(P.38-5)

サポートされる ACL



(注)

ルータ ACL および VLAN マップは、IP サービス イメージが稼働しているスイッチ上でだけサポートされます。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。スイッチでは、発信方向のポート ACL はサポートしません。1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。詳細については、「[ポート ACL](#)」(P.38-3) を参照してください。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向 (着信または発信) に適用されます。詳細については、「[ルータ ACL](#)」(P.38-4) を参照してください。
- VLAN ACL または VLAN マップは、すべてのパケット (ブリッジドパケットおよびルーテッドパケット) のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット (ルーテッドパケットまたはブリッジドパケット) が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。詳細については、「[VLAN マップ](#)」(P.38-5) を参照してください。

同じスイッチ上で入力ポート ACL、ルータ ACL、VLAN マップを併用できます。ただし、ポート ACL はルータ ACL または VLAN マップよりも優先されます。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。

- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

インターフェイスで IEEE 802.1Q トンネリングを設定している場合、トンネルポートで受信した IEEE 802.1Q カプセル化 IP パケットは、MAC ACL によってフィルタリングされますが、IP ACL ではフィルタリングされません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。ルータ ACL、ポート ACL、および VLAN マップに、この制限が適用されます。IEEE 802.1Q トンネリングの詳細については、第 20 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

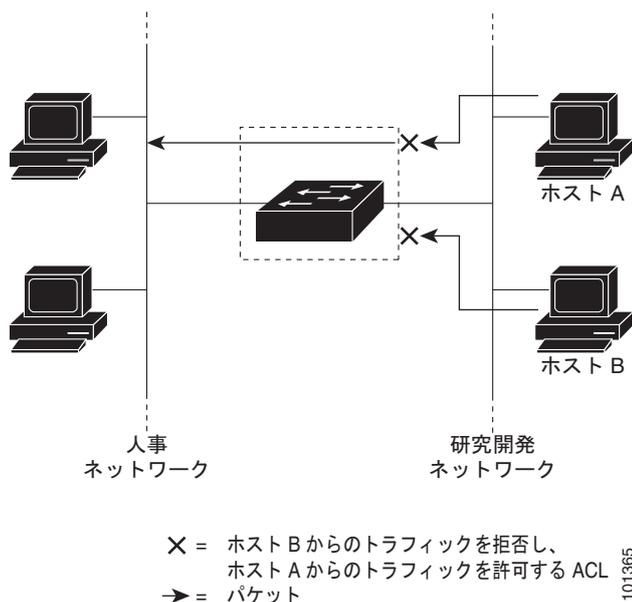
ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL がサポートされるのは物理インターフェイスだけで、EtherChannel インターフェイスではサポートされず、着信方向のインターフェイスだけに適用されます。次のアクセスリストがサポートされています。

- 送信元アドレスを使用する IP アクセスリスト
- 送信元および宛先のアドレスと任意でプロトコルタイプ情報を使用できる拡張 IP アクセスリスト
- 送信元および宛先の MAC アドレスと任意でプロトコルタイプ情報を使用できる MAC 拡張アクセスリスト

スイッチは、インターフェイスに設定されたすべての着信機能に関連付けられた ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。図 38-1 に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 入力に適用される ACL は、ホスト A に Human Resources ネットワークへのアクセスを許可しますが、ホスト B には同じネットワークへのアクセスを禁止しません。ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 38-1 ACL によるネットワークへのトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。



(注)

レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに新しい IP アクセス リストまたは MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスである SVI、物理レイヤ 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

1 つの ACL をある特定インターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回、照合されます。

IPv4 トラフィックでサポートされるアクセス リストは次のとおりです。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。ただし、ルータ ACL は両方向でサポートされますが、適用できるのは着信ポート ACL だけです。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクスト ホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセスを制御できます。図 38-1 では、ルータへの入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は拒否されます。

VLAN マップ

VLAN ACL または VLAN マップを使用して、すべてのトラフィックをアクセス コントロールできます。VLAN との間でルーティングされる、またはスイッチの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

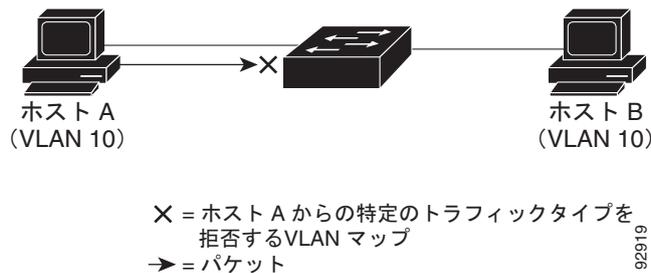
VLAN マップはセキュリティ パケット フィルタリングに使用してください。VLAN マップで方向（着信または発信）は定義されません。

VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックには、MAC VLAN マップによるアクセス コントロールができません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。図 38-2 に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 38-2 VLAN マップによるトラフィックの制御



フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

ACE には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報 (TCP や UDP などのプロトコル タイプを含む) をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```



(注)

最初の 2 つの ACE には宛先アドレスの後に `eq` キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれ Simple Mail Transfer Protocol (SMTP; シンプル メール転送プロトコル) および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE (`permit`) と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE (`deny`) と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE (`permit`) と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート `ftp` に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE (`deny`) と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の `permit` ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

IPv4 ACL の設定

このスイッチで IP v4ACL を設定する手順は、他の Cisco スイッチやルータで IP v4ACL を設定する手順と同じです。ここでは、その設定手順を簡単に説明します。ACL の設定に関する詳細は、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。コマンドの詳細については、『Cisco IOS IP Command Reference,

『Volume 1 of 3: Addressing and Services, Release 12.2』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

このスイッチは、Cisco IOS ルータの ACL に関連する次の機能をサポートしていません。

- 非 IP プロトコル ACL (表 38-1 (P.38-8) を参照) またはブリッジ グループ ACL
- IP アカウンティング
- 着信および発信レート制限 (QoS ACL によるレート制限を除く)
- リフレクシブ ACL またはダイナミック ACL (スイッチ クラスタリング機能で使用される専用のダイナミック ACL を除く)
- ポート ACL および VLAN マップに関する ACL ロギング

このスイッチで IP ACL を使用する手順は次のとおりです。

-
- ステップ 1** アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。
- ステップ 2** その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。
-

ここでは、次の設定について説明します。

- 「標準 IPv4 ACL および拡張 IPv4 ACL の作成」 (P.38-7)
- 「端末回線への IPv4 ACL の適用」 (P.38-20)
- 「インターフェイスへの IPv4 ACL の適用」 (P.38-20)
- 「ハードウェアおよびソフトウェアによる IP ACL の処理」 (P.38-22)
- 「ACL のトラブルシューティング」 (P.38-22)
- 「IPv4 ACL の設定例」 (P.38-24)

標準 IPv4 ACL および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL (アクセス リスト) をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさが高めることもできます。

ここでは、アクセス リストとその作成方法について説明します。

- 「アクセス リスト番号」 (P.38-8)
- 「ACL のロギング」 (P.38-8)
- 「番号制標準 ACL の作成」 (P.38-9)
- 「番号付き拡張 ACL の作成」 (P.38-10)

- 「ACL 内の ACE の並べ替え」(P.38-15)
- 「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.38-15)
- 「ACL での時間範囲の使用」(P.38-17)
- 「ACL へのコメントの挿入」(P.38-19)

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。表 38-1 に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト (1 ~ 199 および 1300 ~ 2699) をサポートします。

表 38-1 アクセス リスト番号

アクセス リスト番号	タイプ	サポートされる
1 ~ 99	IP 標準アクセス リスト	Yes
100 ~ 199	IP 拡張アクセス リスト	Yes
200 ~ 299	プロトコル タイプコード アクセス リスト	No
300 ~ 399	DECnet アクセス リスト	No
400 ~ 499	XNS 標準アクセス リスト	No
500 ~ 599	XNS 拡張アクセス リスト	No
600 ~ 699	AppleTalk アクセス リスト	No
700 ~ 799	48 ビット MAC アドレス アクセス リスト	No
800 ~ 899	IPX 標準アクセス リスト	No
900 ~ 999	IPX 拡張アクセス リスト	No
1000 ~ 1099	IPX SAP アクセス リスト	No
1100 ~ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	No
1200 ~ 1299	IPX サマリー アドレス アクセス リスト	No
1300 ~ 1999	IP 標準アクセス リスト (拡張範囲)	Yes
2000 ~ 2699	IP 拡張アクセス リスト (拡張範囲)	Yes



(注)

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

ACL のロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。



(注) ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可 (*permit*) または拒否 (*deny*) ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

番号制標準 ACL の作成

番号付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard] [log]</code>	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 <i>access-list-number</i> には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は deny 、許可する場合は permit を指定します。 <i>source</i> には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビット長の値。 <i>source</i> および <i>source-wildcard</i> の 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。 <i>source-wildcard</i> を入力する必要はありません。 <i>source</i> および <i>source-wildcard</i> の値 <i>source</i> 0.0.0.0 の省略形を意味するキーワード host。 (任意) <i>source-wildcard</i> は、ワイルドカード ビットを送信元アドレスに適用します。 (任意) log を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no access-list access-list-number** グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストから個々の ACE は削除できません。



(注)

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、他のすべてのホストへのアクセスを許可し、結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny    171.69.198.102
    20 permit any
```

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号制標準 IPv4 ACL は、端末回線（「[端末回線への IPv4 ACL の適用](#)」(P.38-20) を参照）、インターフェイス（「[インターフェイスへの IPv4 ACL の適用](#)」(P.38-20) を参照）、または VLAN（「[VLAN マップの設定](#)」(P.38-31) を参照）に適用できます。

番号付き拡張 ACL の作成

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさが高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

次の IP プロトコルがサポートされます（プロトコル キーワードはカッコ内に太字で示してあります）。

認証ヘッダー プロトコル (**ahp**)、Enhanced IGRP (**eigrp**)、Encapsulating Security Payload (**esp**)、Generic Routing Encapsulation (**gre**)、インターネット制御メッセージ プロトコル (**icmp**)、インターネット グループ管理プロトコル (**igmp**)、任意の内部プロトコル (**ip**)、IP-in-IP トンネリング (**ipinip**)、KA9Q NOS 互換 IP over IP トンネリング (**nos**)、Open Shortest Path First ルーティング (**ospf**)、Payload Compression Protocol (**pcp**)、Protocol Independent Multicast (**pim**)、伝送制御プロトコル (**tcp**)、ユーザ データグラム プロトコル (**udp**)

各プロトコルのキーワードの詳細については、次のコマンド リファレンスを参照してください。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2』
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2』

これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] から入手できます。

**(注)**

このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、タイプ オブ サービス (ToS) の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

サポートされているパラメータのカテゴリは、TCP、UDP、ICMP、IGMP、その他の IP です。
拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2a access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] (注) dscp 値を入力した場合、 tos または precedence は入力できません。 dscp を入力しない場合は、 tos と precedence 値の両方を入力できます。	<p>拡張 IPv4 アクセス リストおよびアクセス条件を定義します。</p> <p><i>access-list-number</i> には、100 ~ 199 または 2000 ~ 2699 の 10 進数を指定します。</p> <p>条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。</p> <p>プロトコルについては、IP プロトコルの名前または番号を入力します。名前または番号は、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、tcp、udp、あるいは IP プロトコル番号を表す 0 ~ 255 の範囲の整数です。一致条件としてインターネット プロトコル (ICMP、TCP、UDP など) を指定するには、キーワード ip を使用します。</p> <p>(注) この手順には、ほとんどの IP プロトコルのオプションが含まれていません。TCP、UDP、ICMP、および IGMP の追加のパラメータについては、ステップ 2b ~ 2e を参照してください。</p> <p><i>source</i> には、パラメータの送信元であるネットワークまたはホストの番号を指定します。</p> <p><i>source-wildcard</i> は、ワイルドカード ビットを送信元アドレスに適用します。</p> <p><i>destination</i> には、パラメータの宛先であるネットワークまたはホストの番号を指定します。</p> <p><i>destination-wildcard</i> は、ワイルドカード ビットを宛先アドレスに適用します。</p> <p><i>source</i>、<i>source-wildcard</i>、<i>destination</i>、および <i>destination-wildcard</i> の値は、次の形式で指定します。</p> <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビット長の値。 0.0.0.0 255.255.255.255 (任意のホスト) を表すキーワード any。 単一のホスト 0.0.0.0 を表すキーワード host。 <p>その他のキーワードはオプションであり、次の意味を持ちます。</p> <ul style="list-style-type: none"> precedence : パケットを 0 ~ 7 の番号または名前前で指定する優先度と一致させる場合に入力します。指定できる値は、routine (0)、priority (1)、immediate (2)、flash (3)、flash-override (4)、critical (5)、internet (6)、network (7) です。 fragments : 2 つめ以降のフラグメントをチェックする場合に入力します。 tos : パケットを 0 ~ 15 の番号または名前前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、normal (0)、max-reliability (2)、max-throughput (4)、min-delay (8) です。 log : エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。 time-range : このキーワードの詳細については、「ACL での時間範囲の使用」(P.38-17) を参照してください。 dscp : パケットを 0 ~ 63 の番号で指定する DSCP 値と一致させる場合に入力します。また、指定できる値のリストを表示するには、疑問符 (?) を使用します。

コマンド	目的
または <code>access-list access-list-number {deny permit} protocol any any [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</code>	アクセス リスト コンフィギュレーション モードで、source および source wildcard の値 0.0.0.0 255.255.255.255 の省略形と destination および destination wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよびワイルドカードの代わりに any キーワードを使用できます。
または <code>access-list access-list-number {deny permit} protocol host source host destination [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</code>	source および source wildcard の値 source 0.0.0.0 の省略形と destination および destination wildcard の値 destination 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに host キーワードを使用できます。
ステップ 2b <code>access-list access-list-number {deny permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] [flag]</code>	(任意) 拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。 次の例外を除き、ステップ 2a の説明にあるパラメータと同じパラメータを使用します。 (任意) <i>operator</i> および <i>port</i> を入力すると、送信元ポート (<i>source source-wildcard</i> の後に入力した場合) または宛先ポート (<i>destination destination-wildcard</i> の後に入力した場合) が比較されます。使用可能な演算子は、 eq (等しい)、 gt (より大きい)、 lt (より小さい)、 neq (等しくない)、 range (包含範囲) などです。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。 <i>port</i> には、10 進数 (0 ~ 65535) のポート番号または TCP ポート名を入力します。TCP ポート名を確認するには、? を使用するか、あるいは、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none">• established : 確立された接続と照合する場合に入力します。このキーワードは、ack または rst フラグでの照合と同じ機能を果たします。• flag : 指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、ack (確認応答)、fin (終了)、psh (プッシュ)、rst (リセット)、syn (同期)、または urg (緊急) です。
ステップ 2c <code>access-list access-list-number {deny permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</code>	(任意) 拡張 UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、 udp を入力します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、 <i>[operator [port]]</i> ポート番号またはポート名は、UDP ポートの番号または名前であればなりません。また、UDP では、 flag および established パラメータは無効です。

	コマンド	目的
ステップ 2d	access-list <i>access-list-number</i> {deny permit} icmp <i>source source-wildcard destination destination-wildcard</i> [<i>icmp-type</i> [[<i>icmp-type icmp-code</i>] [<i>icmp-message</i>]]] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	(任意) 拡張 ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、 icmp を入力します。 ICMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <i>icmp-type</i> : ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 <i>icmp-code</i> : ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 <i>icmp-message</i> : ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージタイプ名およびコード名のリストを参照する場合は、? を使用するか、『Cisco IOS IP Configuration Guide, Release 12.2』の「Configuring IP Services」を参照してください。
ステップ 2e	access-list <i>access-list-number</i> {deny permit} igmp <i>source source-wildcard destination destination-wildcard</i> [<i>igmp-type</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	(任意) 拡張 IGMP アクセス リストおよびアクセス条件を定義します。 インターネットグループ管理プロトコルの場合は、 igmp を入力します。 IGMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 <i>igmp-type</i> : IGMP メッセージタイプと照合するには、0 ~ 15 の番号またはメッセージ名 (dvmrp 、 host-query 、 host-report 、 pim 、または trace) を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists [<i>number</i> <i>name</i>]	アクセス リストの設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

アクセス リスト全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストから個々の ACE は削除できません。

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを拒否し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します (**eq** キーワードを宛先アドレスの後に指定すると、Telnet に対応する TCP 宛先ポート番号がチェックされます)。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
 10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
 20 permit tcp any any
```

ACL の作成後に（端末からの入力などによって）追加したエントリは、リストの末尾に追加されます。番号付きアクセス リストの特定の場所にはアクセス リスト エントリを追加または削除できません。



(注)

ACL を作成するときには、アクセス リストの末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号制拡張 ACL は、端末回線（「[端末回線への IPv4 ACL の適用](#)」(P.38-20) を参照）、インターフェイス（「[インターフェイスへの IPv4 ACL の適用](#)」(P.38-20) を参照）、または VLAN（「[VLAN マップの設定](#)」(P.38-31) を参照）に適用できます。

ACL 内の ACE の並べ替え

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時に自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、ACL のシーケンス番号を編集したり、ACE の適用順序を変更したりできます。たとえば、ACL に新しい ACE を追加すると、その ACE はリストの末尾に配置されます。この場合、シーケンス番号を変更することで、ACE を ACL 内の別の位置に移動できます。

名前付き標準 ACL および名前付き拡張 ACL の作成

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。



(注)

標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項および制限事項に留意してください。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できません。また、VLAN マップでも名前を指定できません。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- 「[標準 IPv4 ACL および拡張 IPv4 ACL の作成](#)」(P.38-7) で説明したとおり、番号付き ACL も使用できます。
- VLAN マップには、標準 ACL および拡張 ACL（名前付きまたは番号制）を使用できます。

名前を使用して標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list standard name</code>	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ~ 99 の番号を使用できます。
ステップ 3	<code>deny {source [source-wildcard] host source any} [log]</code> または <code>permit {source [source-wildcard] host source any} [log]</code>	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかがドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。 <ul style="list-style-type: none"> host source : source および source wildcard の値 <code>source 0.0.0.0</code> any : source および source wildcard の値 <code>0.0.0.0 255.255.255.255</code>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

名前付き標準 ACL を削除するには、`no ip access-list standard name` グローバル コンフィギュレーション コマンドを使用します。

名前を使用して拡張範囲 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list extended name</code>	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ~ 199 の番号を使用できます。
ステップ 3	<code>{deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host destination any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</code>	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。 <code>log</code> キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 プロトコルおよび他のキーワードの定義については、「番号付き拡張 ACL の作成」(P.38-10) を参照してください。 <ul style="list-style-type: none"> host source : source および source wildcard の値 <code>source 0.0.0.0</code> host destination : destination および destination wildcard の値 <code>destination 0.0.0.0</code> any : source および source wildcard の値または destination および destination wildcard の値である <code>0.0.0.0 255.255.255.255</code>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

名前付き標準 ACL を削除するには、**no ip access-list extended name** グローバル コンフィギュレーション コマンドを使用します。

標準 ACL または拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホストアドレス アクセス リストの指定からマスクを省略すると、**0.0.0.0** がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

作成した名前付き ACL は、インターフェイス（「[インターフェイスへの IPv4 ACL の適用](#)」(P.38-20) を参照）または VLAN（「[VLAN マップの設定](#)」(P.38-31) を参照）に適用できます。

ACL での時間範囲の使用

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、「[標準 IPv4 ACL および拡張 IPv4 ACL の作成](#)」(P.38-7) および「[名前付き標準 ACL および名前付き拡張 ACL の作成](#)」(P.38-15) にある名前付きおよび番号付き拡張 ACL の作成に関する表を参照してください。

時間範囲を使用する利点の一部を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新しい設定を他の機能や TCAM にロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセス リストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。



(注)

時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロック ソースが必要です。Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用してスイッチ クロックを同期させることを推奨します。詳細については、「[システム日時の管理](#)」(P.7-1) を参照してください。

ACL の時間範囲パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	time-range <i>time-range-name</i>	作成する時間範囲には意味のある名前 (<i>workhours</i> など) を割り当て、時間範囲 コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 3	absolute [start time date] [end time date] または periodic <i>day-of-the-week hh:mm to [day-of-the-week] hh:mm</i> または periodic {weekdays weekend daily} <i>hh:mm to hh:mm</i>	適用対象の機能がいつ動作可能になるかを指定します。 <ul style="list-style-type: none">時間範囲には、absolute ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。複数の periodic ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show time-range	時間範囲の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

設定した時間範囲の制限を削除するには、**no time-range *time-range-name*** グローバル コンフィギュレーション コマンドを使用します。

次に、*workhours* (営業時間) の時間範囲および会社の休日 (2006 年 1 月 1 日) を設定し、設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
    10 deny tcp any any time-range new_year_day_2006 (inactive)
    20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
  10 permit ip any any
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。コメントがどの **permit** ステートメントまたは **deny** ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する **permit** または **deny** ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list access-list number remark remark** グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

ACL をインターフェイスに適用する手順については、「[インターフェイスへの IPv4 ACL の適用](#)」(P.38-20) を参照してください。VLAN への ACL の適用については、「[VLAN マップの設定](#)」(P.38-31) を参照してください。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>line [console vty] line-number</code>	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • console : コンソール端末回線を指定します。コンソール ポートは DCE です。 • vty : リモート コンソール アクセス用の仮想端末を指定します。 <i>line-number</i> は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ~ 16 です。
ステップ 3	<code>access-class access-list-number {in out}</code>	(デバイスへの) 特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

端末回線から ACL を削除するには、`no access-class access-list-number {in | out}` ライン コンフィギュレーション コマンドを使用します。

インターフェイスへの IPv4 ACL の適用

次の注意事項に留意してください。

- ACL は着信レイヤ 2 ポートだけに適用してください。
- レイヤ 3 インターフェイスには、発信側または着信側のいずれかに ACL を適用してください。
- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN のメンバであるポートに ACL を適用すると、そのポートの ACL は VLAN インターフェイスに適用された ACL よりも優先されます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。ポートの ACL は常にレイヤ 2 ポートで受信した着信パケットをフィルタリングします。

- レイヤ 3 インターフェイスに ACL が適用され、ルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。



(注)

パケットがアクセス グループによって拒否された場合、デフォルトでは、ルータは ICMP 到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。ポート ACL は例外です。ポート ACL は ICMP 到達不能メッセージを生成しません。

ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachable**s インターフェイス コマンドを使用してディセーブルにできます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス (ポート ACL) またはレイヤ 3 インターフェイス (ルータ ACL) を指定できます。
ステップ 3	ip access-group {access-list-number name} {in out}	指定されたインターフェイスへのアクセスを制御します。 out キーワードはレイヤ 2 インターフェイス (ポート ACL) ではサポートされません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	アクセス リストの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定したアクセス グループを削除するには、**no ip access-group {access-list-number | name} {in | out}** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートにアクセス リスト 2 を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```



(注)

ip access-group インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス (SVI、レイヤ 3 EtherChannel、またはルーテッド ポート) に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、スイッチはパケットの受信後に ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、スイッチは、制御されたインターフェイスとの間でパケットを送受信した後に ACL とパケットを照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には CPU に転送してソフトウェア処理を行う必要があるものもあります。ハードウェアで ACL の設定を保存する領域が不足すると、パケットは転送のために CPU に送られます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックより大幅に低くなります。



(注)

スイッチのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受ける（ソフトウェアで転送される）のは、スイッチに着信した該当 VLAN 内のトラフィックだけです。パケットのソフトウェア転送が発生すると、消費される CPU サイクル数に応じて、スイッチのパフォーマンスが低下することがあります。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー（許可フローと拒否フロー）の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

ルータ ACL の設定をハードウェアに適用できない場合、VLAN に着信したルーティング対象パケットはソフトウェアでルーティングされますが、ブリッジングはハードウェアで行われます。ACL により多数のパケットが CPU に送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチドパケットおよびルーテッドパケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

ACL のトラブルシューティング

次の ACL マネージャ メッセージが表示されて [chars] がアクセス リスト名である場合は、

```
ACL MGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

スイッチには、ACL のハードウェア表現を作成するのに使用可能なリソースが不足しています。このリソースには、ハードウェア メモリおよびラベル スペースが含まれますが、CPU メモリは含まれません。この問題の原因は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足です。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外 (**ne**、**gt**、**lt**、**range**) のテストが必要です。

次のいずれかの回避策を使用します。

- ACL 設定を変更して使用するリソースを減らします。
- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

専用のハードウェア リソースを識別するには、**show platform layer4 acl map** 特権 EXEC コマンドを入力します。スイッチに使用可能なリソースがない場合は、出力に **index 0 ~ index 15** が使用できないことが示されます。

十分なリソースがない ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

たとえば、次の ACL をインターフェイスに適用します。

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

なおかつ次のメッセージが表示される場合は次のようにします。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子は使用できません。この問題を回避するには、

- **ip access-list resequence** グローバル コンフィギュレーション コマンドを使用することによって、4 つめの ACE を 1 つめの ACE の前に移動させます。

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

または

- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します (たとえば、ACL 79 を ACL 1 に変更します)。

これで、ACL 内の 1 つめの ACE をインターフェイスに適用できます。スイッチは ACE を **Opselect index** 内の使用可能なマッピング ビットに割り当てた後、フラグ関連の演算子を割り当てて TCAM 内の同じビットを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL (入力および出力) の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- **ip unreachable** がディセーブルの場合、**log** を指定しないと、セキュリティ ACL の拒否ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

IPv4 ACL の設定例

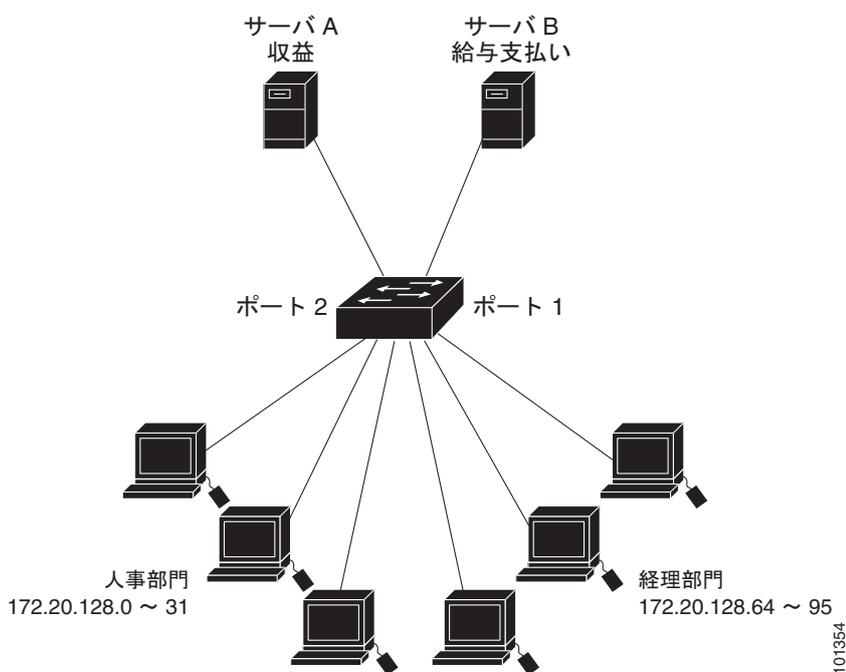
ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『Cisco IOS Security Configuration Guide, Release 12.2』、および『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。

図 38-3 に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

図 38-3 ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ~ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ~ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッドポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
  permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 106 in
```

番号制 ACL

次の例のネットワーク 36.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番目のオクテットは、特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番目の行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番目の行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できません。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。ギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ~ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間に IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group strict in
```

コメント付きの IP ACL エントリ

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL のロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged
```

Log Buffer (4096 bytes):

```
00:00:48: NTP: authentication delay calculation problems
```

<output truncated>

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセスリスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOGDP で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1
0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1
packet
```

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。



(注)

レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

mac access-list extended コマンドでサポートされている非 IP プロトコルの詳細については、このリリースのコマンド リファレンスを参照してください。



(注)

appletalk は、コマンドラインのヘルプ スtring に表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

名前付き MAC 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mac access-list extended name</code>	名前を使用して拡張 MAC アクセス リストを定義します。
ステップ3	<code>{deny permit} {any host source MAC address source MAC address mask} {any host destination MAC address destination MAC address mask} [type mask lsap lsap mask aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos cos]</code>	<p>拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての (any) 送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト (host) 送信元 MAC アドレス、およびすべての (any) 宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、permit または deny を指定します。</p> <p>(任意) 次のオプションを入力することもできます。</p> <ul style="list-style-type: none"> type mask : Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる <i>don't care</i> ビットのマスクが EtherType に適用されます。 lsap lsap mask : IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で <i>don't care</i> ビットのマスクを指定できます。 aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp : 非 IP プロトコル。 cos cos : プライオリティを設定する 0 ~ 7 の IEEE 802.1Q CoS 番号。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、`no mac access-list extended name` グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、他のすべてのタイプのトラフィックを許可するアクセス リスト `mac1` を作成および表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny any any decnet-iv
    20 permit any any
```

レイヤ 2 インターフェイスへの MAC ACL の適用

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

レイヤ 2 インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ 2 インターフェイス (ポート ACL) でなければなりません。
ステップ 3	<code>mac access-group {name} {in}</code>	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は、着信方向に限りサポートされます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mac access-group [interface interface-id]</code>	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定したアクセス グループを削除するには、`no mac access-group {name}` インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス リスト `mac1` をポートに適用してポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mac access-group mac1 in
```



(注) `mac access-group` インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用された場合に限り有効となります。このコマンドは、EtherChannel ポート チャンネルには使用できません。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

VLAN マップの設定

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケットタイプ (IP または MAC) に対する **match** 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケットタイプに対する **match** コマンドがない場合、デフォルトでは、パケットが転送されます。

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

ステップ 1 VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。「標準 IPv4 ACL および拡張 IPv4 ACL の作成」(P.38-7) および「VLAN マップの作成」(P.38-33) を参照してください。

ステップ 2 VLAN ACL マップ エントリを作成するには、**vlan access-map** グローバル コンフィギュレーション コマンドを入力します。

ステップ 3 アクセス マップ コンフィギュレーション モードでは、**action** として、**forward** (デフォルト) または **drop** を入力することもできます。また、**match** コマンドを入力して、既知の MAC アドレスだけが格納された IP パケットまたは非 IP パケットを指定したり、1 つまたは複数の ACL (標準または拡張) とパケットを照合したりすることもできます。



(注) パケットタイプ (IP または MAC) に対する **match** 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。**match** 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。

ステップ 4 VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用します。

ここでは、次の設定について説明します。

- 「VLAN マップの設定時の注意事項」(P.38-32)
- 「VLAN マップの作成」(P.38-33)
- 「VLAN への VLAN マップの適用」(P.38-35)
- 「ネットワークでの VLAN マップの使用法」(P.38-36)

VLAN マップの設定時の注意事項

VLAN マップを設定するときには、次の注意事項に従ってください。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケットタイプ (IP または MAC) に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケットタイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまたは MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットをソフトウェアでブリッジングおよびルーティングする必要があります。
- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できます。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
 - ホスト ポートから無差別ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
 - 無差別ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

設定例については、「ネットワークでの VLAN マップの使用法」(P.38-36) を参照してください。

ルータ ACL および VLAN マップを組み合わせて使用方法については、「VLAN マップとルータ ACL の設定時の注意事項」(P.38-38) を参照してください。

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	vlan access-map name [number]	VLAN マップを作成し、名前および番号（任意）を指定します。番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ3	action {drop forward}	(任意) マップ エントリに対するアクションを設定します。デフォルトは転送 (forward) です。
ステップ4	match {ip mac} address {name number} [name number]	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します (IP または MAC アドレスを使用)。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。
ステップ5	end	グローバル コンフィギュレーション モードに戻ります。
ステップ6	show running-config	アクセス リストの設定を表示します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マップを削除するには、**no vlan access-map name** グローバル コンフィギュレーション コマンドを使用します。マップ内のシーケンス エントリを 1 つ削除するには、**no vlan access-map name number** グローバル コンフィギュレーション コマンドを使用します。

デフォルトのアクションである転送を行うには、**no action** アクセス マップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の **permit** または **deny** キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の **permit** は、一致するという意味です。ACL 内の **deny** は、一致しないという意味です。

ACL および VLAN マップの例

次に、特定の目的のための ACL および VLAN マップを作成する例を示します。

例 1

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、**ip1** ACL (TCP パケット) に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する **ip1ACL** を作成します。VLAN マップには IP パケットに対する **match** 句が存在するため、デフォルトのアクションでは、どの **match** 句とも一致しない IP パケットがすべてドロップされます。

```
Switch(config)# ip access-list extended ip1
```

```
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット (TCP でも UDP でもないパケット) がドロップされます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

例 2

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例 3

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-nacl)# permit host 000.0c00.0111 any
Switch(config-ext-nacl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-nacl)# permit any any decnet-ip
Switch(config-ext-nacl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例 4

次の例の VLAN マップでは、デフォルトですべての packets (IP および非 IP) がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP packets が転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC packets が転送されます。
- その他のすべての IP packets がドロップされます。
- その他のすべての MAC packets がドロップされます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan filter mapname vlan-list list	VLAN マップを 1 つまたは複数の VLAN ID に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12, 22, 30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 3	show running-config	アクセス リストの設定を表示します。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN マップを削除するには、**no vlan filter mapname vlan-list list** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN マップ 1 を VLAN 20 ~ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

ネットワークでの VLAN マップの使用法

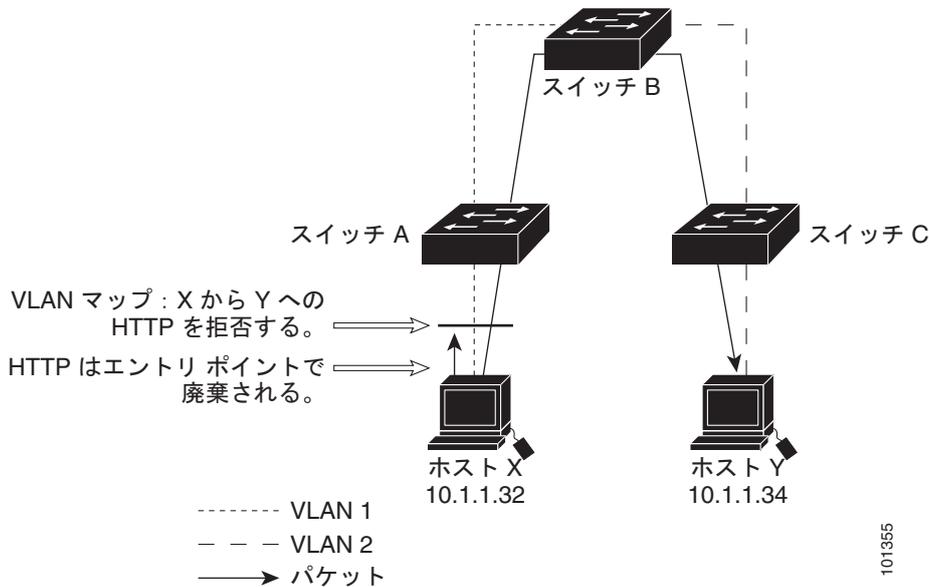
ここでは、一般的な VLAN マップの使用法について一部説明します。

- 「ワイヤリング クローゼットの設定」(P.38-36)
- 「別の VLAN にあるサーバへのアクセスの拒否」(P.38-37)

ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上でイネーブルにされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。
 図 38-4 では、ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定しています。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。

図 38-4 ワイヤリング クローゼットの設定



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可 (一致) する IP アクセス リスト `http` を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

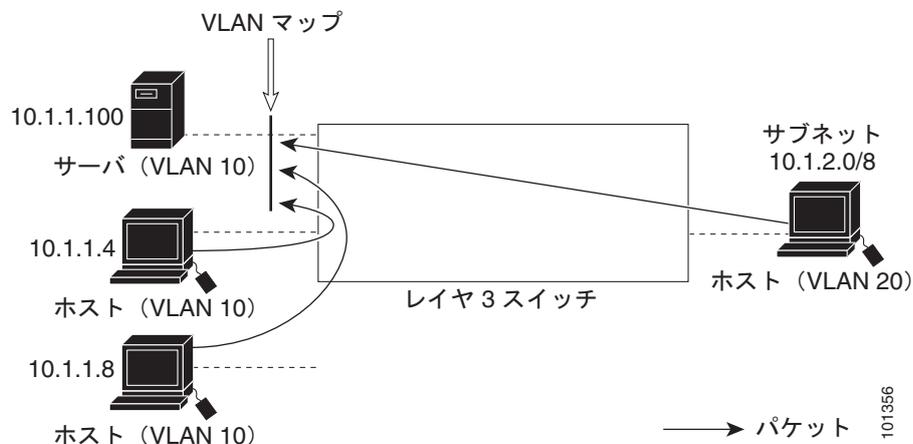
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセスの拒否

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります (図 38-5 を参照)。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 38-5 他 VLAN 上のサーバへのアクセス拒否



次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ *SERVER1-ACL* を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップ *SERVER1* を VLAN 10 に適用します。

ステップ 1 正しいパケットと一致する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

- ステップ 2** SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

- ステップ 3** VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

ルータ ACL を VLAN マップと組み合わせて使用する方法

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケット フローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケット フローは拒否されます。



(注) ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケット タイプ (IP または MAC) に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

ここでは、ルータ ACL を VLAN マップと組み合わせて使用する方法について説明します。

- 「VLAN マップとルータ ACL の設定時の注意事項」 (P.38-38)
- 「VLAN に適用されるルータ ACL と VLAN マップの例」 (P.38-39)

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

スイッチ ハードウェアは、方向 (入力および出力) ごとにセキュリティ ACL を 1 回検索します。したがって、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL と VLAN マップを統合すると、ACE の数が膨大になる場合があります。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルト アクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

```
permit...
permit...
permit...
deny ip any any
```

または

```
deny...
deny...
deny...
permit ip any any
```

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

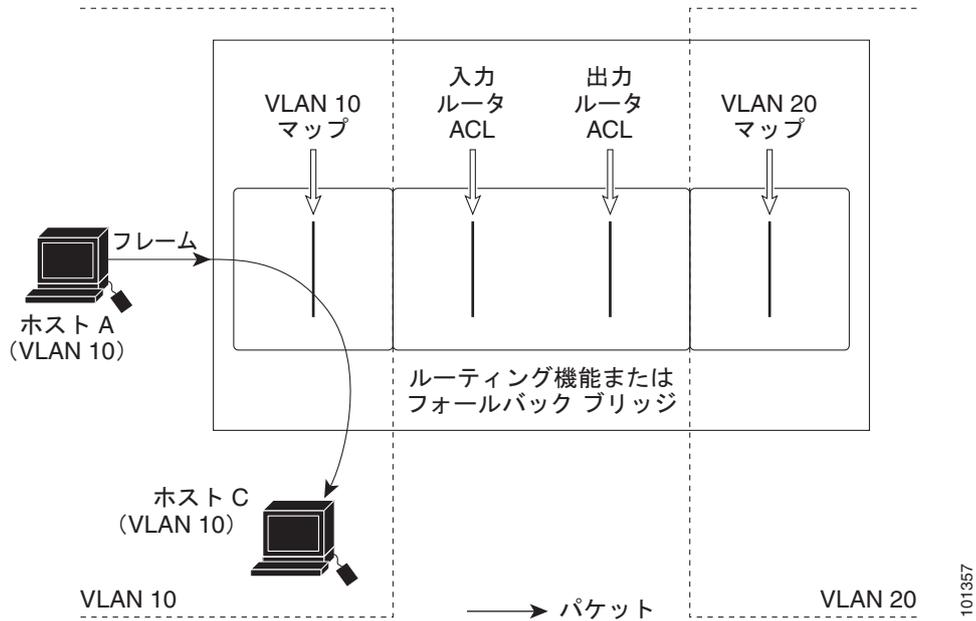
VLAN に適用されるルータ ACL と VLAN マップの例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

ACL およびスイッチド パケット

図 38-6 に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップだけが適用されます。

図 38-6 スイッチド パケットへの ACL の適用

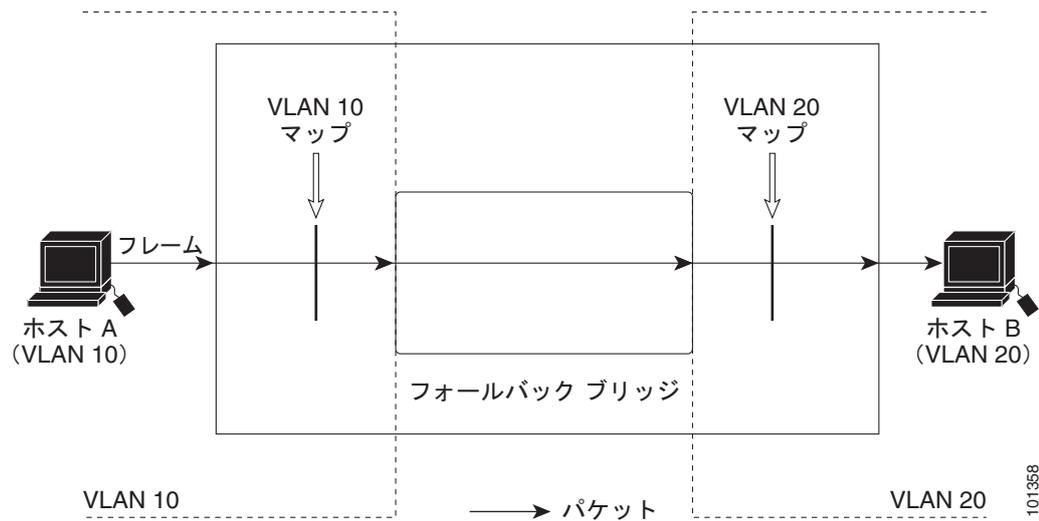


101357

ACL およびブリッジド パケット

図 38-7 に、フォールバックブリッジドパケットに ACL を適用する方法を示します。ブリッジドパケットの場合は、入力 VLAN にレイヤ 2 ACL だけが適用されます。また、非 IP および非 ARP パケットだけがフォールバックブリッジドパケットとなります。

図 38-7 ブリッジドパケットへの ACL の適用



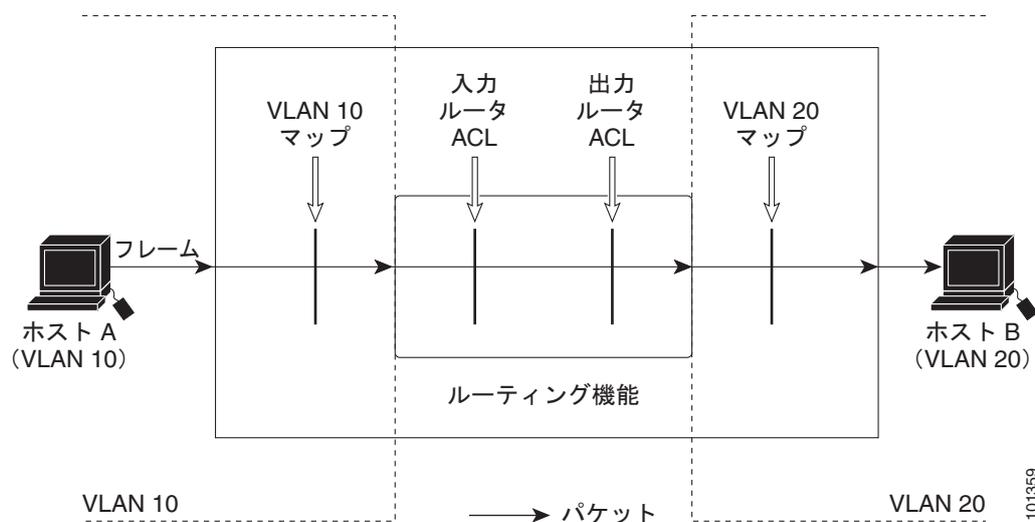
101358

ACL およびルーテッド パケット

図 38-8 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

図 38-8 ルーテッド パケットへの ACL の適用

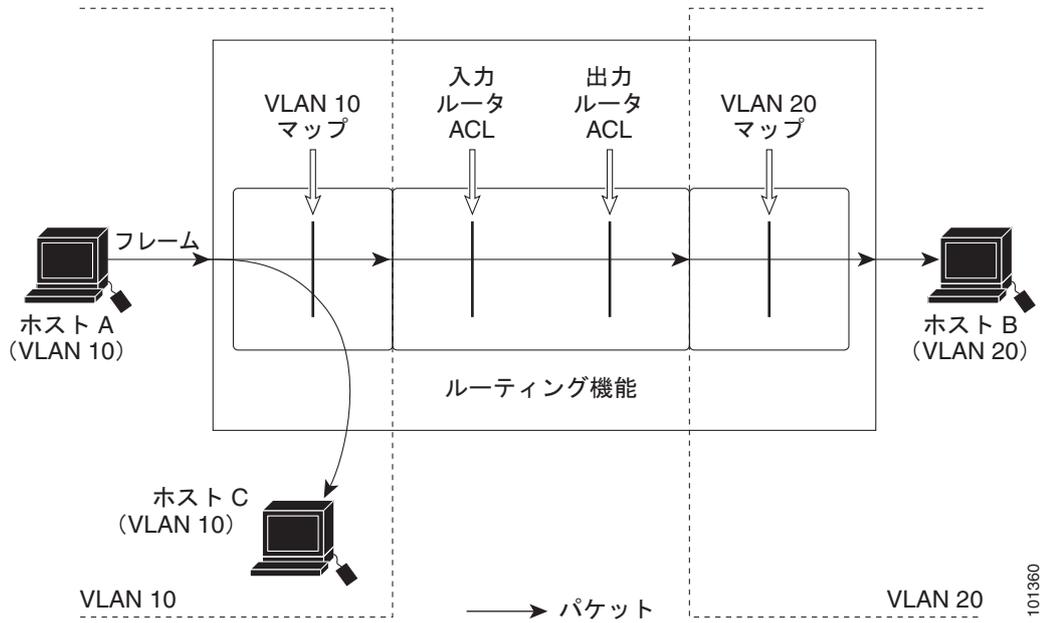


ACL およびマルチキャスト パケット

図 38-9 に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。

最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップ (図 38-9 の VLAN 10 マップ) によってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。

図 38-9 マルチキャスト パケットへの ACL の適用



IPv4 ACL の設定の表示

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示できます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、表 38-2 に記載された特権 EXEC コマンドを使用します。

表 38-2 アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
<code>show access-lists [number name]</code>	現在の 1 つまたはすべての IP および MAC アドレス アクセス リストの内容、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
<code>show ip access-lists [number name]</code>	現在のすべての IP アクセス リスト、または特定の IP アクセス リスト（番号付きまたは名前付き）の内容を表示します。
<code>show ip interface interface-id</code>	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、 ip access-group インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
<code>show running-config [interface interface-id]</code>	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
<code>show mac access-group [interface interface-id]</code>	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

VLAN アクセス マップまたは VLAN フィルタに関する情報を表示できます。VLAN マップ情報を表示するには、表 38-3 に記載された特権 EXEC コマンドを使用します。

表 38-3 VLAN マップ情報を表示するコマンド

コマンド	目的
<code>show vlan access-map [mapname]</code>	すべての VLAN アクセス マップまたは指定されたアクセス マップに関する情報を表示します。
<code>show vlan filter [access-map name vlan vlan-id]</code>	すべての VLAN フィルタに関する情報、または指定された VLAN や VLAN アクセス マップに関する情報を表示します。



CHAPTER 39

QoS の設定

この章では、IE 3000 スイッチで Automatic QoS (auto-QoS) コマンドを使用して、または標準 QoS コマンドを使用して Quality of Service (QoS) を設定する手順について説明します。QoS を使用すると、特定のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。

QoS は物理ポートおよび Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に設定できます。ポリシー マップを適用する他に、分類、キューイング、およびスケジューリングなどの QoS を同じ方法で物理ポートおよび SVI に設定します。物理ポートに QoS を設定した場合は、非階層型のポリシー マップをポートに適用します。SVI に QoS を設定すると、非階層型、または階層型のポリシー マップが適用されます。



(注)

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

この章で説明する内容は、次のとおりです。

- 「QoS の概要」 (P.39-2)
- 「自動 QoS の設定」 (P.39-21)
- 「自動 QoS 情報の表示」 (P.39-30)
- 「標準 QoS の設定」 (P.39-31)
- 「標準 QoS 情報の表示」 (P.39-80)

スイッチは、Modular QoS Command Line Interface (MQC; モジュラ QoS コマンドライン インターフェイス) コマンドの一部をサポートします。MQC コマンドの詳細については、『Cisco IOS Quality of Service Solutions Guide, Release 12.2』の「Modular Quality of Service Command-Line Interface Overview」の章を参照してください。

QoS の概要

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生した場合に、廃棄される可能性についても、すべてのトラフィックで同じです。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の新しい規格である Differentiated Services (DiffServ) アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP タイプ オブ サービス (ToS) フィールドの 6 ビットを使用して、分類 (クラス) 情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します (図 39-1 を参照)。

- レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット (ユーザ プライオリティ ビット) で CoS 値が伝達されます。レイヤ 2 IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除くすべてのトラフィックが IEEE 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ) です。

- レイヤ 3 パケットのプライオリティ ビット

レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point (DSCP) 値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ~ 7 です。

DSCP 値の範囲は 0 ~ 63 です。



(注)

Cisco IOS Release 12.2(52)SE 以降では、デュアル IPv4/IPv6 Switch Database Management (SDM) テンプレートを持つ IPv6 ポート ベースのトラストをサポートしています。IPv6 が動作しているスイッチのデュアル IPv4/IPv6 テンプレートを持つスイッチをリロードする必要があります。詳細については、第 10 章「SDM テンプレートの設定」を参照してください。



(注)

IPv6 QoS はこのリリースでサポートされていません。

図 39-1 フレームおよびパケットにおける QoS 分類レイヤ

カプセル化されたパケット

レイヤ 2 ヘッダー	IP ヘッダー	データ
---------------	---------	-----

レイヤ 2 ISL フレーム

ISL ヘッダー (26 バイト)	カプセル化されたフレーム 1... (24.5 KB)	FCS (4 バイト)
----------------------	--------------------------------	----------------

↑ 3 ビットを CoS に使用

レイヤ 2 802.1Q および 802.1p フレーム

プリアンブル	開始フレーム 区切り文字	DA	SA	タグ	PT	データ	FCS
--------	-----------------	----	----	----	----	-----	-----

↑ 3 ビット (ユーザプライオリティ ビット) を CoS に使用

レイヤ 3 IPv4 パケット

バージョン 長	ToS (1 バイト)	長さ	ID	オフセット	TTL	プロトコル	FCS	IP-SA	IP-DA	データ
------------	----------------	----	----	-------	-----	-------	-----	-------	-------	-----

↑ IP precedence または DSCP

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てられるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コアスイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィッククラスに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィックタイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

QoS の基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し (分類)、パケットがスイッチを通過するとき所定の QoS を指定するラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ (ポリシングおよびマーキング)、リソース競合が発生する状況に応じて異なる処理 (キューイングおよびスケジューリング) を行う必要があります。また、スイッチから送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります (シェーピング)。

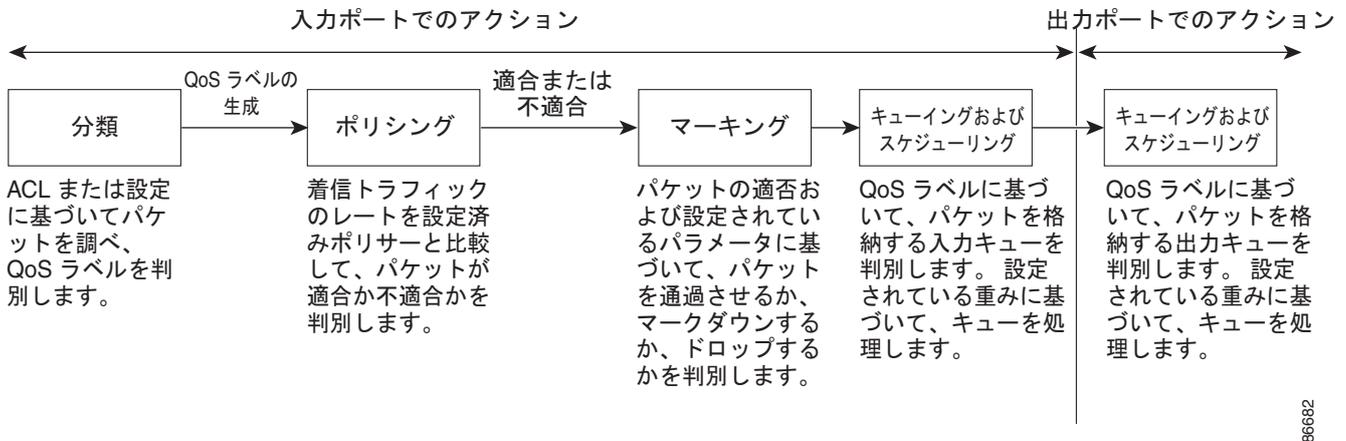
図 39-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。詳細については、「[分類](#)」(P.39-5) を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。詳細については、「[ポリシングおよびマーキング](#)」(P.39-9) を参照してください。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。詳細については、「[ポリシングおよびマーキング](#)」(P.39-9) を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを 2 つの入力キューのどちらに格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail-Drop (WTD) アルゴリズムによって拡張されます。しきい値を超過している場合、パケットはドロップされます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.39-14) を参照してください。
- スケジューリングでは、設定されている Shaped Round Robin (SRR; シェイプド ラウンド ロビン) の重みに基づいて、キューを処理します。入力キューの 1 つがプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから他のキューを処理します。詳細については、「[SRR のシェーピングおよび共有](#)」(P.39-15) を参照してください。

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.39-14) を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

図 39-2 QoS の基本モデル



分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを決定します。QoS ラベルは信頼設定およびパケットタイプに従ってマッピングされます（図 39-3 (P.39-7) を参照）。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。非 IP トラフィックには、次の分類オプションを使用できます（図 39-3 を参照）。

- 着信フレームの CoS 値を信頼します（ポートが CoS を信頼するように設定します）。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ 2 の ISL フレームヘッダーは、1 バイトのユーザフィールドの下位 3 ビットで CoS 値を伝達します。レイヤ 2 IEEE 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0（ロープライオリティ）～ 7（ハイプライオリティ）です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
- 設定されたレイヤ 2 の MAC アクセスコントロールリスト (ACL) に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

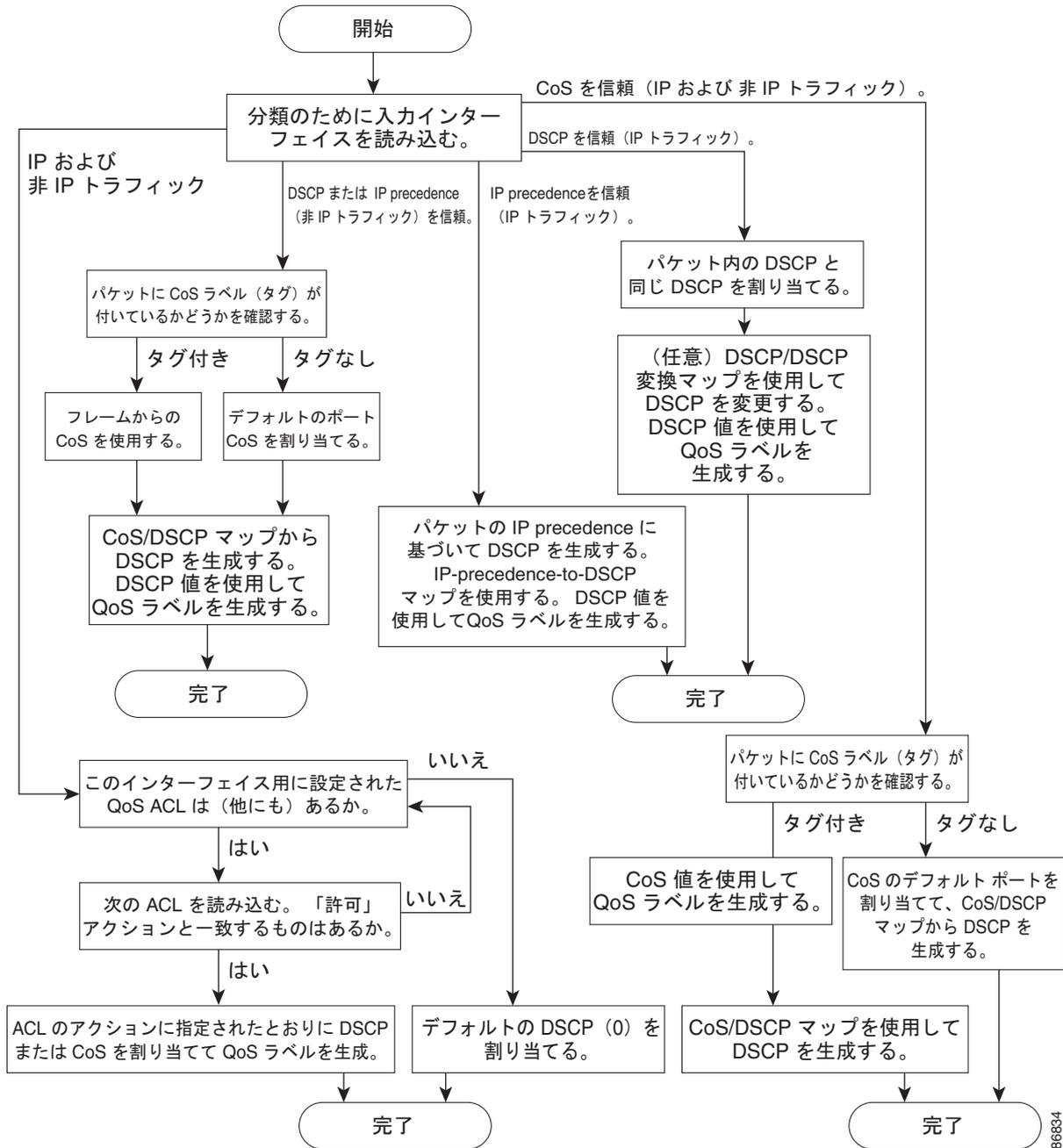
IP トラフィックには、次の分類オプションを使用できます (図 39-3 を参照)。

- 着信パケットの DSCP 値を信頼し (DSCP を信頼するようにポートを設定し)、同じ DSCP 値をパケットに割り当てます。IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ~ 63 です。
2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。
- 着信パケットの IP precedence 値を信頼し (IP precedence を信頼するようにポートを設定し)、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。IP precedence 値の範囲は 0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ) です。
- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
- 設定された IP 標準 ACL または IP 拡張 ACL (IP ヘッダーの各フィールドを調べる) に基づいて、分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」(P.39-13) を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態による分類の設定」(P.39-37) を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 39-3 分類フローチャート



86834

QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケットグループ（クラス）を定義できます。QoS のコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかり、それ以降の検索処理は中止され、QoS 処理が開始されます。



(注)

アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「[QoS ポリシーの設定](#)」(P.39-43) を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセスグループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適切な場合の対処法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

ポリシー マップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

非階層型のポリシー マップは、物理ポートまたは SVI に対して適用できます。ただし、階層型のポリシー マップに関しては、SVI に対してだけしか適用できません。階層型のポリシー マップには 2 つのレベルがあります。1 番めは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 番めはインターフェイス レベルで、SVI の物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイス レベルのアクションはインターフェイス レベルのポリシー マップで指定されます。

詳細については、「[ポリシングおよびマーキング](#)」(P.39-9) を参照してください。設定の詳細については、「[QoS ポリシーの設定](#)」(P.39-43) を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てた後で、ポリシングおよびマーキング プロセスを開始できます (図 39-4 を参照)。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「アウト オブ プロファイル」または「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP 値を変更 (マークダウン) してパケットの通過を許可するアクションなどがあります。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。ポリシング済み DSCP マップの詳細については、「[マッピング テーブル](#)」(P.39-13) を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。



(注)

すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます (ポリサーが設定されている場合)。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートまたは SVI に対してポリシングを設定できます。物理ポートでは、信頼状態を設定したり、パケットに対して新規に DSCP または IP precedence 値を設定したり、個別にまたは集約的にポリサーを定義できます。物理ポートのポリシング設定の詳細については、「[物理ポートのポリシング](#)」(P.39-10) を参照してください。SVI にポリシー マップを設定する場合、階層型のポリシー マップを作成して、ポリシー マップの 2 番目のインターフェイス レベルにだけ個別にポリサーを定義します。詳細については、「[SVI のポリシング](#)」(P.39-11) を参照してください。

ポリシー マップおよびポリシング アクションを設定したあとで、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシー を統合します。設定情報については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキ](#)

ング」(P.39-49)、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング」(P.39-53)、および「集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング」(P.39-60)を参照してください。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

- 個別：QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- 集約：QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。ポリサーの帯域幅限度を指定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。



(注) SVI には個別のポリサーだけを設定します。

ポリシングは、トークン バケット アルゴリズムを使用します。各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート (ビット/秒) で送信されます。バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション (ドロップまたはマークダウン) が実行されません。

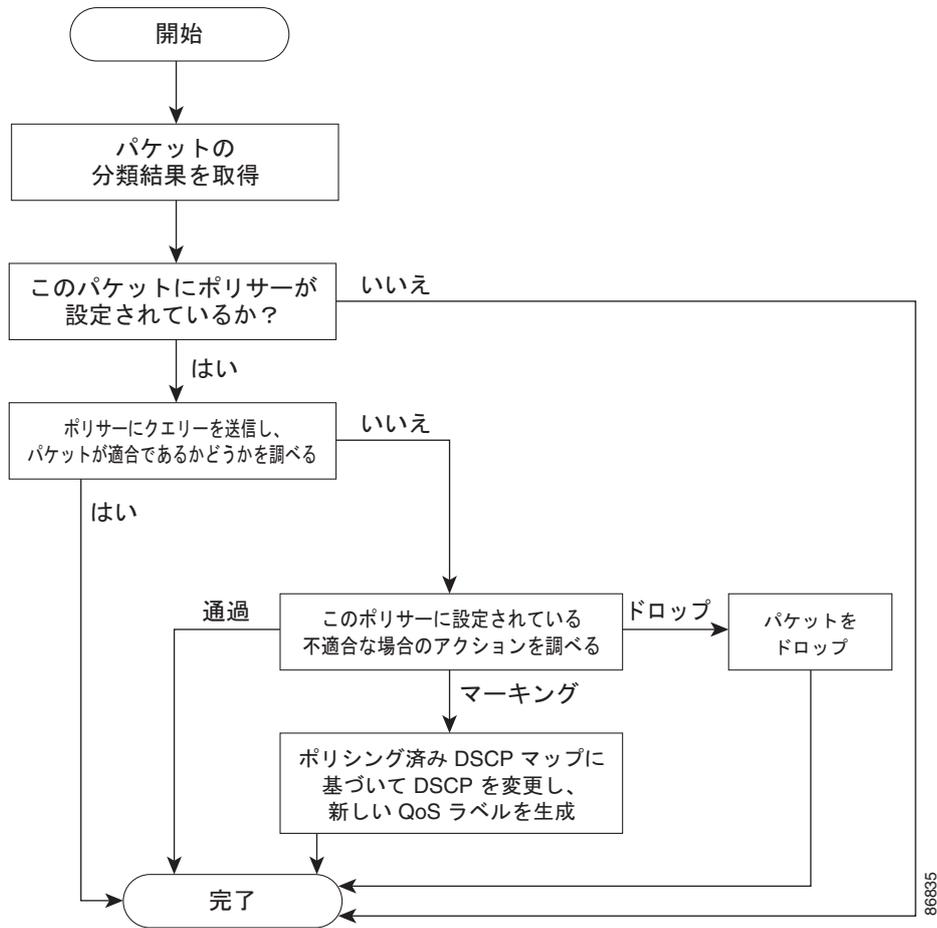
バケットが満たされる速度は、バケット深度 (**burst-byte**)、トークンが削除されるレート (**rate-bps**)、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ (バケットがオーバーフローするまでの許容最大バースト) を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの **burst-byte** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。トークンがバケットから削除される速度 (平均速度) を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの **rate-bps** オプションまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。

図 39-4 に、ポリシングおよびマーキングのプロセスを示します。次のタイプのポリシー マップを設定できます。

- 物理ポートの非階層型ポリシー マップ
- SVI に適用されたインターフェイス レベルの階層型ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップに指定します。

図 39-4 物理ポートのポリシングおよびマーキング フローチャート



SVI のポリシング



(注)

SVI に個別のポリサーで階層型のポリシー マップを設定する前に、SVI の物理ポートに対して VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップが SVI に適用されますが、個々のポリサーは、階層型のポリシー マップの 2 番目のインターフェイス レベルで指定した物理ポートのトラフィックに対してだけ影響します。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

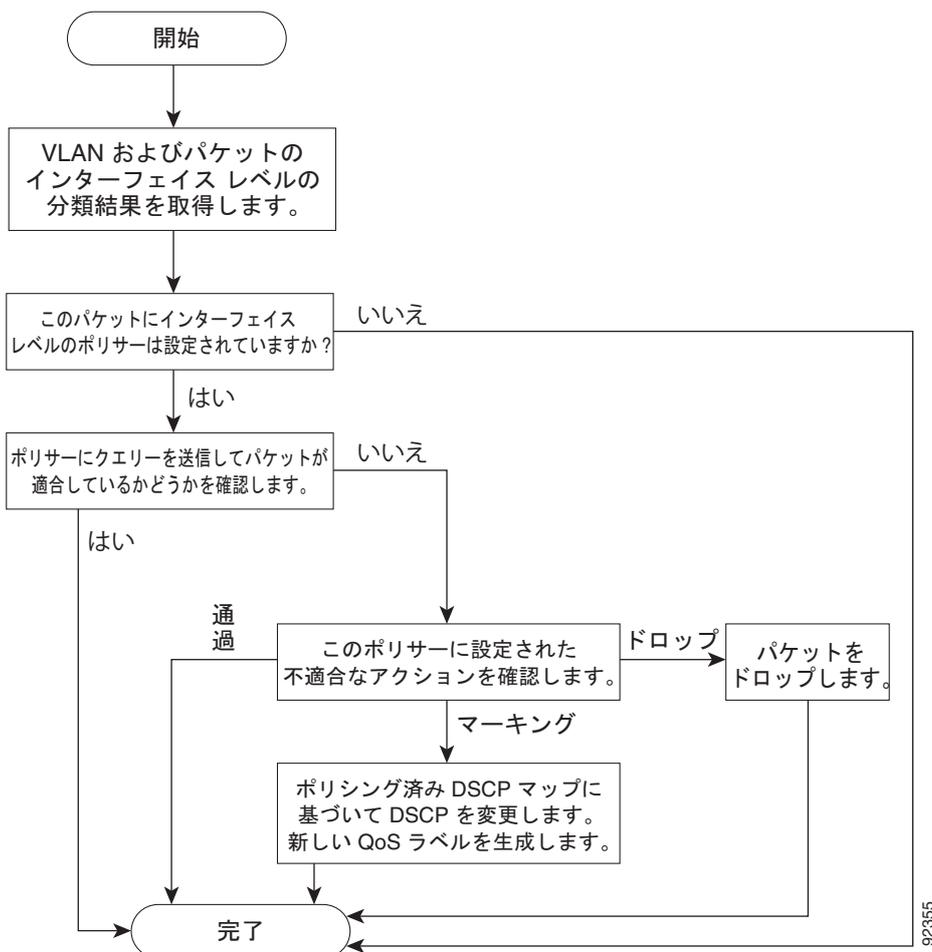
SVI にポリシーを設定する場合、次の 2 つのレベルの階層型ポリシー マップを作成および設定できます。

- **VLAN レベル**：クラス マップおよびポートの信頼状態を指定するクラスを設定することで、またはパケットに新規に DSCP や IP precedence 値を設定することでプライマリ レベルを作成します。VLAN レベルのポリシー マップは SVI の VLAN に対してだけ適用可能で、ポリサーはサポートしません。
- **インターフェイス レベル**：クラス マップおよび SVI の物理ポートに個別にポリサーを指定するクラスを設定することで、セカンダリ レベルを作成します。インターフェイス レベルのポリシー マップは個別のポリサーだけサポートし、集約ポリサーをサポートしません。VLAN レベルのポリシー マップで定義された各クラスに対して、異なるインターフェイス レベル ポリシー マップを設定できます。

階層型のポリシー マップの例は、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシー マップ、およびマーキング」(P.39-53) を参照してください。

図 39-5 に、SVI に階層型のポリシー マップが設定されている場合のポリシー およびマーキングのプロセスを示します。

図 39-5 SVI のポリシー およびマーキング フローチャート



マッピング テーブル

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用してキューを選択します。入力または出力のキューに加えて、QoS ラベルは WTD しきい値も識別します。これらのマップを設定するには、**mls qos srr-queue {input | output} dscp-map** および **mls qos srr-queue {input | output} cos-map** グローバル コンフィギュレーション コマンドを使用します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。

DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。その他のすべてのマップはスイッチ全体に適用されます。

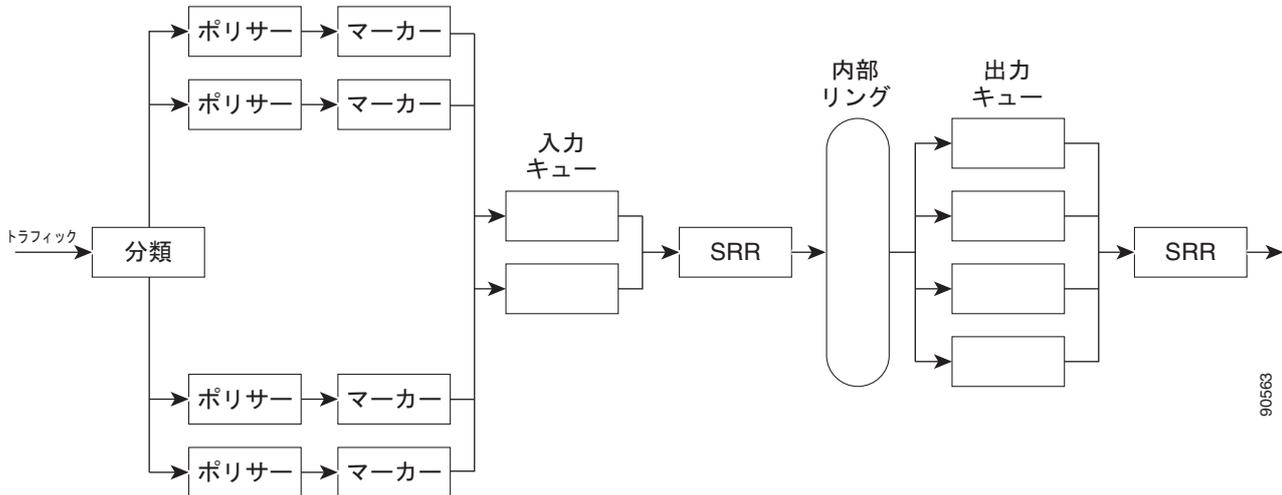
設定の詳細については、「[DSCP マップの設定](#)」(P.39-62) を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「[入力キューでのキューイングおよびスケジューリング](#)」(P.39-16) を参照してください。DSCP および CoS 出力キューしきい値マップの詳細については、「[出力キューでのキューイングおよびスケジューリング](#)」(P.39-17) を参照してください。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立っています (図 39-6 を参照)。

図 39-6 入力および出力キューの位置



すべてのポートの入力帯域幅の合計が内部リングの帯域幅を超えることがあるため、入力キューはパケットの分類、ポリシング、およびマーキングの後、パケットがスイッチファブリックに転送される前の位置に配置されています。複数の入力ポートから 1 つの出力ポートに同時にパケットが送信されて、輻輳が発生することがあるため、出力キューは内部リングの後に配置されています。

WTD

入力および出力キューは両方とも、WTD と呼ばれるテールドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると (宛先キューの空きスペースがフレームサイズより小さくなると)、フレームはドロップされます。

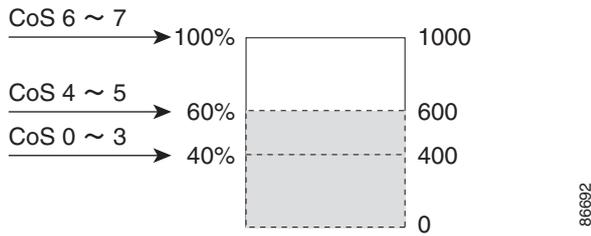
各キューには 3 つのしきい値があります。QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。3 つのしきい値のうち、2 つは設定可能 (明示的) で、1 つは設定不可能 (暗示的) です。

図 39-7 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。ドロップ割合は次のように設定されています。40% (400 フレーム)、60% (600 フレーム)、および 100% (1000 フレーム) です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます (キューフル状態)。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ~ 3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

図 39-7 WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.39-69)、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」(P.39-73)、および「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.39-75) を参照してください。

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットが内部リングに送信されます。出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有がデフォルト モードであり、これ以外のモードはサポートされていません。

シェーピング モードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バーストトラフィックの最高時と最低時を削減します。シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

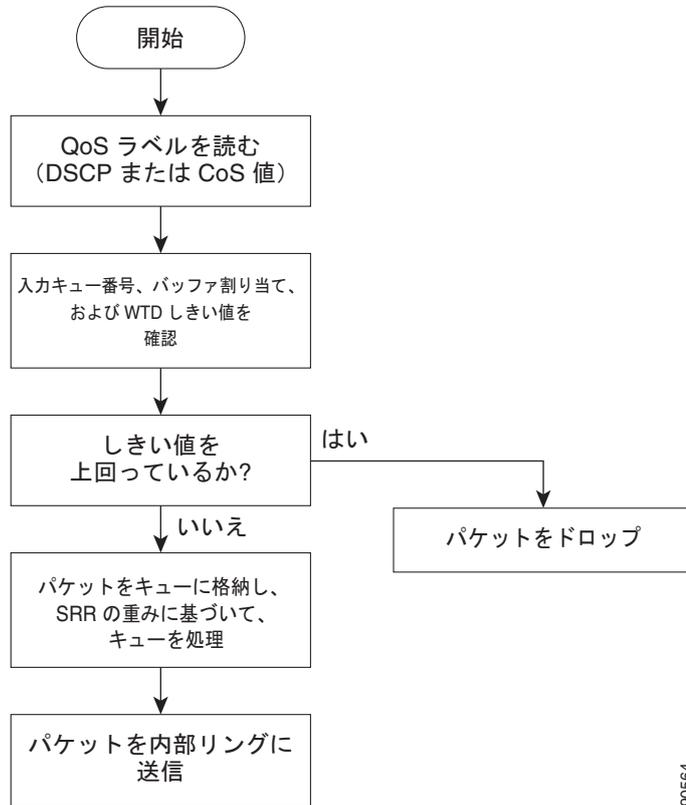
共有モードでは、各キューは設定された重みに従って帯域幅を共有します。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。シェーピングおよび共有は、インターフェイスごとに設定されます。各インターフェイスは、一意に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」(P.39-71)、「出力キューでの SRR シェーピング重みの設定」(P.39-76)、および「出力キューでの SRR 共有重みの設定」(P.39-77) を参照してください。

入力キューでのキューイングおよびスケジューリング

図 39-8 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

図 39-8 入力ポートのキューイングおよびスケジューリング フローチャート



90564



(注) 共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってのみ処理される、設定可能な入力キューを 2 つサポートしています。表 39-1 にこれらのキューの説明を示します。

表 39-1 入力キューのタイプ

キュー タイプ ¹	機能
標準	標準プライオリティと見なされるユーザトラフィック。各フローを区別するために、3 つの異なるしきい値を設定できます。 mls qos srr-queue input threshold 、 mls qos srr-queue input dscp-map 、および mls qos srr-queue input cos-map グローバル コンフィギュレーション コマンドを使用できます。
緊急	Differentiated Services (DF) 緊急転送または音声トラフィックなどのハイプライオリティ ユーザトラフィック。このトラフィックに必要な帯域幅は、 mls qos srr-queue input priority-queue グローバル コンフィギュレーション コマンドを使用して、合計トラフィックの割合として設定できます。緊急キューには帯域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}**、または **mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}** グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能 (明示的) な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能 (暗示的) なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合 (しきい値 ID 1 および ID 2 用) を割り当てるには、**mls qos srr-queue input threshold queue-id threshold-percentagel threshold-percentage2** グローバル コンフィギュレーション コマンドを使用します。各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。WTD の仕組みの詳細については、「WTD」(P.39-14) を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する (スペース量を割り当てる) には、**mls qos srr-queue input buffers percentagel percentage2** グローバル コンフィギュレーション コマンドを使用します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。帯域幅を割合として割り当てるには、**mls qos srr-queue input bandwidth weightl weight2** グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューは内部リングの負荷にかかわらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック (音声など) に使用する必要があります。

SRR は、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は **mls qos srr-queue input bandwidth weightl weight2** グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「入力キューの特性の設定」(P.39-68) を参照してください。

出力キューでのキューイングおよびスケジューリング

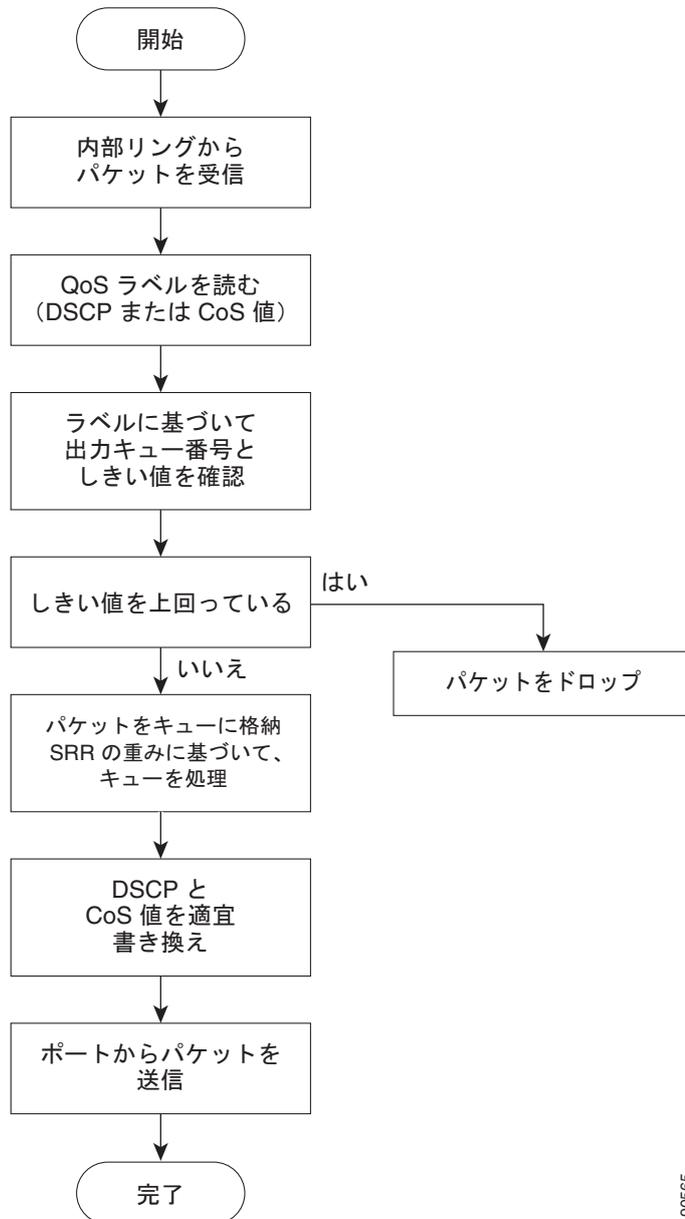
図 39-9 に、出力ポートのキューイングおよびスケジューリング フローチャートを示します。



(注)

緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の 3 つのキューが処理されます。

図 39-9 出力ポートのキューイングおよびスケジューリング フローチャート



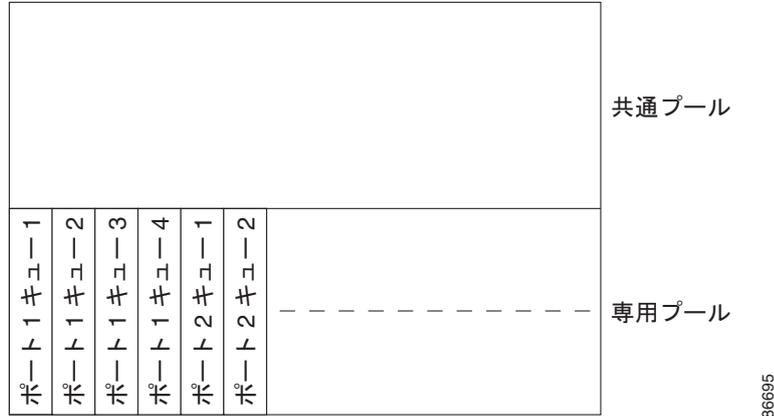
90565

各ポートは、そのうち 1 つ（キュー 1）を出力緊急キューにできる、4 つの出力キューをサポートしています。これらのキューは、キューセットごとに設定されます。出力ポートから脱退するすべてのトラフィックは、パケットに割り当てられた QoS ラベルに基づいて、これらの 4 つのキューのいずれかを通過し、しきい値の影響を受けます。

図 39-10 に出力キュー バッファを示します。バッファ スペースは共通プールと専用プールで構成されます。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかは制御されます。スイッチは、目的のキューが確保された量（限度内）を超えるバッファを消費していないかどうか、最大バッファ（限度超）をすべて消費しているかどうか、および共通プールが空である（空きバッファなし）か、または空でない（空きバッファあり）かを検出します。キューがオーバーリミット

トでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファスペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 39-10 出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファの可用性の保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティトラフィックを確実にバッファに格納できます。たとえば、バッファスペースが 400 の場合、バッファスペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ~ 4 に割り当てることができます。キュー 1 には 280 のバッファが割り当てられ、キュー 2 ~ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。たとえば、キュー用として 100 バッファがある場合、50% (50 バッファ) を確保できます。残りの 50 バッファは共通プールに戻されます。また、最大しきい値を設定することにより、いっぱいになったキューが確保量を超えるバッファを取得できるようにすることもできます。共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。`mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}`、または `mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}` グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、`show mls qos maps` 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィッククラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能 (明示的) な WTD しきい値で、もう 1 つはキューフルステートに設定済みの設定不可能 (暗示的) なしきい値です。しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値

は、キューフル ステートに設定済みで、変更できません。キューセットにポートをマッピングするには、**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。WTD しきい値の割合を変更するには、キューセット設定を変更します。WTD の仕組みの詳細については、「**WTD**」(P.39-14) を参照してください。

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share weight1 weight2 weight3 weight4** または **srr-queue bandwidth shape weight1 weight2 weight3 weight4** インターフェイス コンフィギュレーション コマンドを使用します。シェーピングと共有の違いについては、「**SRR のシェーピングおよび共有**」(P.39-15) を参照してください。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域幅重みは無視されて比率計算に使用されません。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。緊急キューをイネーブルにするには、**priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「**出力キューの特性の設定**」(P.39-72) を参照してください。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、次のようにパケットが変更されることがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されないで、

DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されないで、CoS/DSCP マップに従って DSCP が変更されることがあります。

入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。ポリシー マップの設定アクションによっても、DSCP が書き換えられます。

自動 QoS の設定

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。自動 QoS は、デフォルト (ディセーブル) の QoS 動作を使用せずに、入力および出力キューを使用します。スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

sdm prefer dual ipv4-and-ipv6 グローバル コンフィギュレーション コマンドを使用してデュアル IPv4 および IPv6 SDM テンプレートを設定すると、自動 QoS で IPv4 と IPv6 の両方のトラフィックがサポートされます。

自動 QoS コマンドを使用して Cisco IP Phone、および Cisco SoftPhone アプリケーションを実行するデバイスに接続するポートを指定します。また、アップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。自動 QoS は次の機能を実行します。

- Cisco IP Phone の有無の検知
- QoS 分類の設定
- 出力キューの設定

ここでは、次の設定について説明します。

- 「生成される自動 QoS 設定」 (P.39-21)
- 「コンフィギュレーションにおける自動 QoS の影響」 (P.39-26)
- 「自動 QoS 設定時の注意事項」 (P.39-26)
- 「VoIP 用自動 QoS のイネーブル化」 (P.39-27)
- 「自動 QoS 設定例」 (P.39-29)

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、表 39-2 に示すように、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 39-2 トラフィック タイプ、パケット ラベル、およびキュー

	VoIP ¹ データ トラフィック	VoIP Control トラフィック	ルーティング プ ロトコル トラフィック	STP BPDU ト ラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラ フィック
DSCP	46	24、26	48	56	34	—
CoS	5	3	6	7	4	—

表 39-2 トラフィック タイプ、パケット ラベル、およびキュー (続き)

	VoIP ¹ データ トラフィック	VoIP Control トラフィック	ルーティング プ ロトコル トラフィック	STP BPDU ト ラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラ フィック
CoS/入力キュー マップ	2、3、4、5、6、7 (キュー 2)					0、1 (キュー 1)
CoS/出力キュー マップ	5 (キュー 1)	3、6、7 (キュー 2)			4 (キュー 3)	2 (キュー 3) 0、1 (キュー 4)

1. VoIP = Voice over IP

表 39-3 に、入力キューに対して生成された自動 QoS の設定を示します。

表 39-3 入力キューに対する自動 QoS の設定

入力キュー	キュー番号	CoS からキューへ のマッピング	キュー ウェイト (帯域幅)	キュー (バッ ファ) サイズ
SRR 共有	1	0、1	81 %	67 %
プライオリティ	2	2、3、4、5、6、7	19 %	33 %

表 39-4 に、出力キューに対して生成される auto-QoS の設定を示します。

表 39-4 出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへの マッピング	キュー ウェイト (帯域幅)	ギガビット対応 ポートのキュー (バッファ) サイズ	10/100 イーサ ネット ポートの キュー (バッファ) サイズ
プライオリティ	1	5	最大 100%	16 %	10%
SRR 共有	2	3、6、7	10%	6 %	10%
SRR 共有	3	2、4	60%	17 %	26 %
SRR 共有	4	0、1	20%	61 %	54 %

最初のポートで auto-QoS 機能をイネーブルにすると、次の自動アクションが実行されます。

- QoS がグローバルにイネーブルになり (`mls qos` グローバル コンフィギュレーション コマンド)、そのあと、他のグローバル コンフィギュレーション コマンドが追加されます。
- Cisco IP Phone に接続されたネットワーク エッジのポートで `auto qos voip cisco-phone` インターフェイス コンフィギュレーション コマンドを入力すると、スイッチにより信頼境界の機能がイネーブルになります。スイッチは、Cisco Discovery Protocol (CDP) を使用して、Cisco IP Phone が存在するかどうかを検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、スイッチはポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone がない場合、入力分類は、パケットの QoS ラベルを信頼しないように設定されます。スイッチは、表 39-3 および表 39-4 の設定に従ってポート上の入力および出力キューを設定します。ポリシングがポリシー マップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。

- **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼働するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッチはポリシングを使用して、パケットがプロファイルの内部または外部にいるかを判断し、パケット上のアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。スイッチは、表 39-3 および表 39-4 の設定に従ってポート上の入力および出力キューを設定します。
- ネットワーク内部に接続されたポート上で、**auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケットでルーティングされないポートの CoS 値、またはルーテッドポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。スイッチは、表 39-3 および表 39-4 の設定値に従ってポートの入力キューと出力キューを設定します。

信頼境界機能の詳細については、「[ポートセキュリティを確保するための信頼境界機能の設定](#)」(P.39-39) を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone**、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにする場合、スイッチはトラフィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、表 39-5 にリストされているコマンドをポートに適用します。

表 39-5 生成される自動 QoS 設定

説明	自動的に生成されるコマンド
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# mls qos Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# no mls qos srr-queue input cos-map Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 3 0 Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 1 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 1 2 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# no mls qos srr-queue output cos-map Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 Switch(config)# mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7 Switch(config)# mls qos srr-queue output cos-map queue 3 threshold 3 2 4 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 3 0

表 39-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue input dscp-map Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 32 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47</pre>
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue output dscp-map Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7</pre>
スイッチが自動的に入力キューを設定します。キュー 2 がプライオリティ キューでキュー 1 が共有モードです。また、スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	<pre>Switch(config)# no mls qos srr-queue input priority-queue 1 Switch(config)# no mls qos srr-queue input priority-queue 2 Switch(config)# mls qos srr-queue input bandwidth 90 10 Switch(config)# mls qos srr-queue input threshold 1 8 16 Switch(config)# mls qos srr-queue input threshold 2 34 66 Switch(config)# mls qos srr-queue input buffers 67 33</pre>

表 39-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
<p>スイッチが自動的に出力キューのバッファ サイズを設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード (シェーピングまたは共有) を設定します。</p>	<pre>Switch(config)# mls qos queue-set output 1 threshold 1 138 138 92 138 Switch(config)# mls qos queue-set output 1 threshold 2 138 138 92 400 Switch(config)# mls qos queue-set output 1 threshold 3 36 77 100 318 Switch(config)# mls qos queue-set output 1 threshold 4 20 50 67 400 Switch(config)# mls qos queue-set output 2 threshold 1 149 149 100 149 Switch(config)# mls qos queue-set output 2 threshold 2 118 118 100 235 Switch(config)# mls qos queue-set output 2 threshold 3 41 68 100 272 Switch(config)# mls qos queue-set output 2 threshold 4 42 72 100 242 Switch(config)# mls qos queue-set output 1 buffers 10 10 26 54 Switch(config)# mls qos queue-set output 2 buffers 16 6 17 61 Switch(config-if)# priority-que out Switch(config-if)# srr-queue bandwidth share 10 10 60 20</pre>
<p>auto qos voip trust コマンドを入力した場合、mls qos trust cos コマンドを使用することによって、スイッチは非ルーテッドポートで受信したパケットの CoS 値を信頼するように、または mls qos trust dscp コマンドを使用することによって、ルーテッドポートで受信したパケットの DSCP 値を信頼するように、自動的に入力分類を設定します。</p>	<pre>Switch(config-if)# mls qos trust cos Switch(config-if)# mls qos trust dscp</pre>
<p>auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。</p>	<pre>Switch(config-if)# mls qos trust device cisco-phone</pre>
<p>auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。</p>	<pre>Switch(config)# mls qos map policed-dscp 24 26 46 to 0 Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap)# match ip dscp ef Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap)# match ip dscp cs3 af31 Switch(config)# policy-map AutoQoS-Police-SoftPhone Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c)# set dscp ef Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust Switch(config-pmap-c)# set dscp cs3 Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit</pre>
<p>クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ (別名 <i>AutoQoS-Police-SoftPhone</i>) を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。</p>	<pre>Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone</pre>

表 39-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
<p>auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。</p>	<pre> Switch(config)# mls qos map policed-dscp 24 26 46 to 0 Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap)# match ip dscp ef Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap)# match ip dscp cs3 af31 Switch(config)# policy-map AutoQoS-Police-CiscoPhone Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c)# set dscp ef Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust Switch(config-pmap-c)# set dscp cs3 Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit </pre>
<p>クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ (別名 <i>AutoQoS-Police-CiscoPhone</i>) を、Cisco Phone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。</p>	<pre> Switch(config-if)# service-policy input AutoQoS-Police-CiscoPhone </pre>

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになっていると、**auto qos voip** インターフェイス コンフィギュレーション コマンドおよび生成された設定が、実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- 自動 QoS は、非ルーテッドポートおよびルーテッドポートで Cisco IP Phone に VoIP のスイッチを設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼働するデバイスの VoIP 用にスイッチを設定します。
- Cisco SoftPhone を稼働するデバイスが非ルーテッドポートまたはルーテッドポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つのみをサポートします。
- auto-QoS VoIP では、**priority-queue** インターフェイス コンフィギュレーション コマンドを出力インターフェイスに使用します。ポリシー マップおよび信頼できるデバイスを Cisco IP Phone の同一インターフェイス上に設定することも可能です。

- 自動 QoS のデフォルトを利用するには、自動 QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。詳細については、「[コンフィギュレーションにおける自動 QoS の影響](#)」(P.39-26) を参照してください。
- 自動 QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。
- ルーテッドポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- 接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

VoIP 用自動 QoS のイネーブル化

QoS ドメイン内で VoIP 用の自動 QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	Cisco IP Phone に接続されたポート、Cisco SoftPhone 機能を実行する装置に接続されたポート、またはネットワーク内部の信頼性のある他のスイッチやルータに接続されたアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>auto qos voip {cisco-phone cisco-softphone trust}</code>	自動 QoS をイネーブルにします。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cisco-phone : ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話が検出された場合のみ信頼されます。 • cisco-softphone : ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。 • trust : アップリンク ポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show auto qos interface interface-id	設定を確認します。 このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示するには、 show running-config 特権 EXEC コマンドを使用します。

自動 QoS がイネーブルまたはディセーブルの場合に自動生成される QoS コマンドを表示するには、**debug auto qos** 特権 EXEC コマンドを入力してから、自動 QoS をイネーブルにします。詳細については、このリリースに対応するコマンドリファレンスにある **debug autoqos** コマンドの項を参照してください。

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、自動 QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。自動 QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、自動 QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、自動 QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

no mls qos グローバル コンフィギュレーション コマンドを使用して、自動 QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合には、パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念はありません。トラフィックは Pass-Through モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます）。

次の例では、ポートに接続されているスイッチまたはルータが信頼できる装置である場合に、auto-QoS をイネーブルにし、着信パケットで受信した QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

自動 QoS 設定例

ここでは、自動 QoS をネットワークに実装する方法について説明します (図 39-11 を参照)。QoS パフォーマンスを最適にするには、ネットワーク内部の装置すべてで自動 QoS をイネーブルにします。

図 39-11 ネットワークでの自動 QoS の設定例

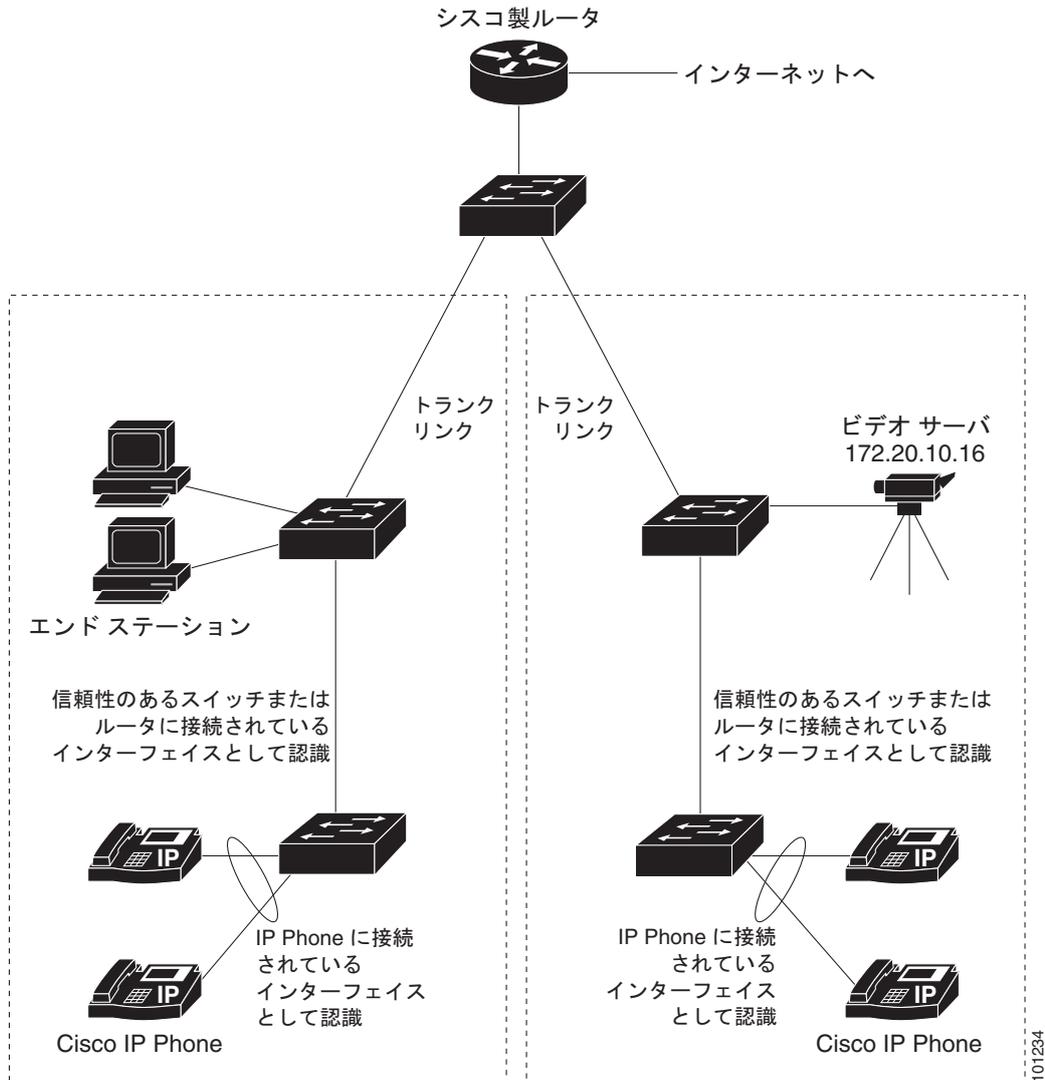


図 39-11 に、VoIP トラフィックを他のすべてのトラフィックに優先するネットワークを示します。QoS ドメインのエッジにあるワイヤリングクローゼット内のスイッチ上で、自動 QoS はイネーブルです。



(注)

自動 QoS コマンドを入力する前に標準 QoS コマンドを設定しないでください。QoS 設定は微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。

QoS ドメインのエッジにあるスイッチで VoIP トラフィックを他のトラフィックより優先させるように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>debug auto qos</code>	自動 QoS のデバッグをイネーブルにします。デバッグをイネーブルにすると、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>cdp enable</code>	CDP をグローバルにイネーブルにします。デフォルトではイネーブルに設定されています。
ステップ 4	<code>interface interface-id</code>	Cisco IP Phone に接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>auto qos voip cisco-phone</code>	ポート上で自動 QoS をイネーブルにし、そのポートが Cisco IP Phone に接続されるように指定します。 着信パケット内の QoS ラベルは、Cisco IP Phone が検出された場合だけ信頼されます。
ステップ 6	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 7		Cisco IP Phone に接続されているポートの数だけ、ステップ 4 ~ 6 を繰り返します。
ステップ 8	<code>interface interface-id</code>	信頼性のあるスイッチまたはルータに接続していると認識されるスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。図 39-11 を参照してください。
ステップ 9	<code>auto qos voip trust</code>	ポート上で自動 QoS をイネーブルにし、そのポートが信頼性のあるルータまたはスイッチに接続されるように指定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show auto qos</code>	入力内容を確認します。 このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示するには、 <code>show running-config</code> 特権 EXEC コマンドを使用します。 自動 QoS によって影響される QoS 設定の詳細については、「自動 QoS 情報の表示」(P.26-12) を参照してください。
ステップ 12	<code>copy running-config startup-config</code>	<code>auto qos voip</code> インターフェイス コンフィギュレーション コマンドおよび生成された自動 QoS 設定をコンフィギュレーション ファイル内に保存します。

自動 QoS 情報の表示

自動 QoS 設定を表示するには、`show auto qos [interface [interface-id]]` 特権 EXEC コマンドを使用します。ユーザによる設定変更を表示するには、`show running-config` 特権 EXEC コマンドを使用します。`show auto qos` コマンド出力と `show running-config` コマンド出力を比較してユーザ定義の QoS 設定を比較できます。

自動 QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- `show mls qos`
- `show mls qos maps cos-dscp`

- `show mls qos interface [interface-id] [buffers | queueing]`
- `show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-mutation | dscp-output-q | ip-prec-dscp | policed-dscp]`
- `show mls qos input-queue`
- `show running-config`

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

標準 QoS の設定

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

ここでは、次の設定について説明します。

- 「標準 QoS のデフォルト設定」(P.39-31)
- 「標準 QoS 設定時の注意事項」(P.39-34)
- 「QoS のグローバルなイネーブル化」(P.39-36) (必須)
- 「物理ポートで VLAN ベースの QoS をイネーブル化」(P.39-36) (任意)
- 「ポートの信頼状態による分類の設定」(P.39-37) (必須)
- 「QoS ポリシーの設定」(P.39-43) (必須)
- 「DSCP マップの設定」(P.39-62) (任意、DSCP/DSCP 変換マップまたはポリシング済み DSCP マップを使用する必要がない場合)
- 「入力キューの特性の設定」(P.39-68) (任意)
- 「出力キューの特性の設定」(P.39-72) (任意)

標準 QoS のデフォルト設定

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは **Pass-Through** モードでスイッチングされます（パケットは書き換えられることなくスイッチングされ、ポリシングなしのベストエフォートに分類されます）。

`mls qos` グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。ポリシー マップは設定されません。すべてのポート上のデフォルトポートの信頼性は、信頼性なし（untrusted）の状態です。入力および出力キューのデフォルト設定については、「入力キューのデフォルト設定」(P.39-32) および「出力キューのデフォルト設定」(P.39-32) を参照してください。

入力キューのデフォルト設定

表 39-6 に、QoS がイネーブルの場合の入力キューのデフォルト設定を示します。

表 39-6 入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て ¹	4	4
プライオリティ キューの帯域幅 ²	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみパケットを送信します。
2. キュー 2 はプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 39-7 に、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示します。

表 39-7 デフォルトの CoS 入力キューしきい値

CoS 値	キュー ID - しきい値 ID
0 ~ 4	1-1
5	2-1
6, 7	1-1

表 39-8 に、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示します。

表 39-8 デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ~ 39	1-1
40 ~ 47	2-1
48 ~ 63	1-1

出力キューのデフォルト設定

表 39-9 に、QoS がイネーブルの場合、各キューセットの出力キューのデフォルト設定を示します。すべてのポートはキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に設定され、レートは制限されません。

表 39-9 出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	50%	50%	50%

表 39-9 出力キューのデフォルト設定 (続き)

機能	キュー 1	キュー 2	キュー 3	キュー 4
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み (絶対) ¹	25	0	0	0
SRR 共有重み ²	25	25	25	25

1. シェーピング重みが 0 の場合、このキューはシェーピングモードで動作します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 39-10 に、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 39-10 デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2 - 1
2、3	3 - 1
4	4 - 1
5	1 - 1
6、7	4 - 1

表 39-11 に、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 39-11 デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ~ 15	2 - 1
16 ~ 31	3 - 1
32 ~ 39	4 - 1
40 ~ 47	1 - 1
48 ~ 63	4 - 1

マッピング テーブルのデフォルト設定

デフォルトの CoS/DSCP マップは、表 39-12 (P.39-63) のとおりです。

デフォルトの IP precedence/DSCP マップは、表 39-13 (P.39-64) のとおりです。

デフォルトの DSCP/CoS マップは、表 39-14 (P.39-66) のとおりです。

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする (マークダウンしない) 空のマップです。

標準 QoS 設定時の注意事項

QoS の設定をはじめめる前に、次の事項を確認してください。

- 「QoS ACL の注意事項」(P.39-34)
- 「インターフェイスへの QoS の適用」(P.39-34)
- 「ポリシングの注意事項」(P.39-35)
- 「一般的な QoS の注意事項」(P.39-35)

QoS ACL の注意事項

アクセス コントロール リスト (ACL) で QoS を設定する際の注意事項は次のとおりです。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラス マップごとに使用できる ACL は 1 つだけ、使用できる **match** クラスマップ コンフィギュレーション コマンドは 1 つだけです。ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントには、ACL 行ごとに複数の TCAM エントリが必要です。入力サービス ポリシー マップに ACL の信頼ステートメントが含まれている場合、利用可能な QoS TCAM に収めるにはアクセス リストが大きすぎる可能性があり、ポリシー マップをポートに適用する際にエラーが発生する場合があります。可能な限り、QoS ACL の行数を最小限に抑えてください。

インターフェイスへの QoS の適用

ここでは、QoS 物理ポートの設定時の注意事項について説明します。また、この説明は SVI (レイヤ 3 インターフェイス) にも適用されます。

- QoS は物理ポートおよび SVI に設定できます。物理ポートに QoS を設定する場合は、非階層型のポリシー マップを作成し、適用してください。SVI に QoS を設定する場合は、非階層型および階層型のポリシー マップを作成し、適用できます。
- ブリッジング、ルーティング、または CPU への送信のどれを行うかに関係なく、着信トラフィックは分類、ポリシング、およびマークダウン (設定されている場合) されます。ブリッジングされたフレームをドロップしたり、DSCP および CoS 値を変更したりできます。
- 物理ポートまたは SVI でポリシー マップを設定する場合には、次の注意事項に従ってください。
 - 物理ポートと SVI に同じポリシー マップを適用できません。
 - 物理ポートで VLAN ベースの QoS を設定した場合、スイッチはそのポートにあるすべてのポートベースのポリシー マップを削除します。そうすることで、物理ポートのトラフィックは、自身のポートの SVI に適用されているポリシー マップの適用を受け入れられます。
 - SVI に適用された階層型のポリシー マップでは、物理ポートのインターフェイス レベルで個別にだけポリサーを作成でき、ポートのトラフィックの帯域幅制限を指定できます。入力ポートは、トランクまたはスタティック アクセス ポイントとして設定する必要があります。階層型のポリシー マップの VLAN レベルではポリサーを設定できません。
 - スイッチは、階層型のポリシー マップで集約ポリサーをサポートしません。

- SVI に階層型のポリシー マップが適用されたあとは、インターフェイス レベルのポリシー マップを変更したり、削除したりできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。また、階層型ポリシー マップで指定されたクラス マップを追加または削除できません。

ポリシングの注意事項

ポリシングの注意事項を次に示します。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステムの内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。たとえば、ギガビット イーサネット ポートに 32 のポリサー、ファスト イーサネット ポートに 8 つのポリサーを設定したり、ギガビット イーサネット ポートに 64 のポリサー、ファスト イーサネット ポートに 5 つのポリサーを設定できます。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。
- 同じ非階層型のポリシー マップ内にある複数のトラフィック クラスで共有される集約ポリサーを作成できます。ただし、集約ポリサーを異なるポリシー マップにわたって使用できません。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランク ポートの場合、ポートを介して受信したすべての VLAN のトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- スイッチで受信された制御トラフィック（スパニングツリー Bridge Protocol Data Unit (BPDU); ブリッジプロトコル データ ユニット）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。

QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos</code>	QoS をグローバルにイネーブルにします。 デフォルト設定における QoS の動作については、「標準 QoS のデフォルト設定」(P.39-31)、「入力キューでのキューイングおよびスケジューリング」(P.39-16)、および「出力キューでのキューイングおよびスケジューリング」(P.39-17) を参照してください。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

QoS をディセーブルにするには、`no mls qos` グローバル コンフィギュレーション コマンドを使用します。

物理ポートで VLAN ベースの QoS をイネーブル化

デフォルトでは、VLAN ベースの QoS はスイッチにあるすべての物理ポートでディセーブルです。スイッチは、物理ポート ベースでだけ、クラス マップおよびポリシー マップ QoS を含む QoS を適用できます。スイッチ ポートで VLAN ベースの QoS をイネーブルにできます。

特権 EXEC モードを開始して、VLAN ベースの QoS をイネーブルにするには、次の手順を実行します。この手順には、SVI にインターフェイス レベルの階層型ポリシー マップが指定されている物理ポートが必要です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>mls qos vlan-based</code>	ポートで VLAN ベースの QoS をイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface interface-id</code>	VLAN ベースの QoS が物理ポートでイネーブルかどうかを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

物理ポートで VLAN ベースの QoS をディセーブルにする場合は、`no mls qos vlan-based` インターフェイス コンフィギュレーション コマンドを使用します。

ポートの信頼状態による分類の設定

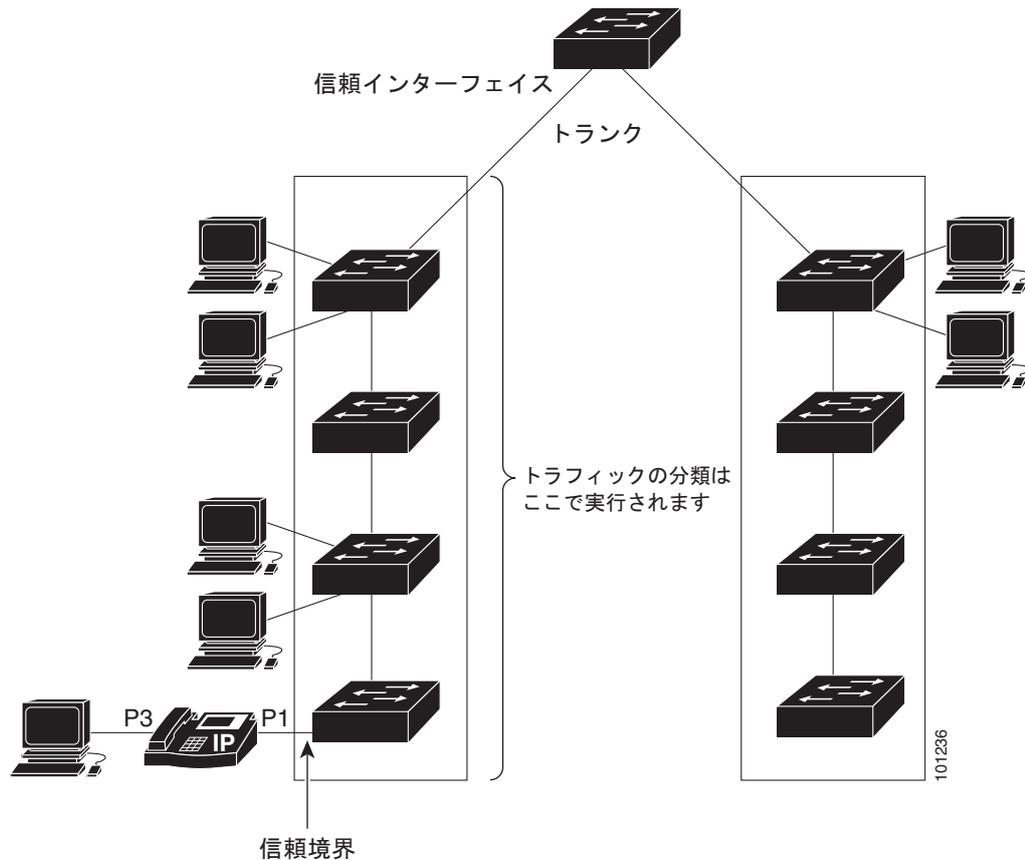
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」(P.39-43)に記載されている作業を1つまたは複数実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」(P.39-37)
- 「インターフェイスの CoS 値の設定」(P.39-39)
- 「ポートセキュリティを確保するための信頼境界機能の設定」(P.39-39)
- 「DSCP トランスペアレント モードのイネーブル化」(P.39-41)
- 「別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定」(P.39-41)

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチポートをいずれか1つの信頼状態に設定できます。図 39-12 に、ネットワーク トポロジの例を示します。

図 39-12 QoS ドメイン内のポートの信頼状態



ポートが受信したトラフィックの分類を信頼するようにポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	<code>mls qos trust [cos dscp ip-precedence]</code>	ポートの信頼状態を設定します。 デフォルトでは、ポートは <code>trusted</code> ではありません。キーワードを指定しない場合、デフォルトは <code>dscp</code> です。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cos : パケットの CoS 値を使用して入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。 • dscp : パケットの DSCP 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • ip-precedence : パケットの IP precedence 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`untrusted` ステートにポートを戻す場合は、`no mls qos trust` インターフェイス コンフィギュレーション コマンドを使用します。

デフォルトの CoS 値を変更する方法については、「[インターフェイスの CoS 値の設定](#)」(P.39-39) を参照してください。CoS/DSCP マップを設定する方法については、「[CoS/DSCP マップの設定](#)」(P.39-63) を参照してください。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

デフォルトのポート CoS 値を定義する場合、またはポート上のすべての着信パケットにデフォルトの CoS 値を割り当てる場合には、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ3	mls qos cos {default-cos override}	デフォルトのポート CoS 値を設定します。 <ul style="list-style-type: none"> <i>default-cos</i> には、ポートに割り当てるデフォルトの CoS 値を指定します。パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ~ 7 です。デフォルトは 0 です。 着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用する場合は、override キーワードを使用します。デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、 override キーワードを使用します。ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show mls qos interface	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、**no mls qos cos {default-cos | override}** インターフェイス コンフィギュレーション コマンドを使用します。

ポート セキュリティを確保するための信頼境界機能の設定

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して (図 39-12 (P.39-37) を参照)、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ (CoS = 5) にマーキングし、データ パケットをロー プライオリティ (CoS = 0) にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 IEEE 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチへ送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイ プライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、(信頼性のある CoS 設定により) PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone (Cisco IP Phone 7910、7935、7940、および 7960) の存在を検出します。電話が検出されない場合、信頼境界機能がハイ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。**switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

信頼境界機能をポート上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 3	interface interface-id	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	cdp enable	ポート上で CDP をイネーブルに設定します。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	mls qos trust cos mls qos trust dscp	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	mls qos trust device cisco-phone	Cisco IP Phone が信頼性のあるデバイスであることを指定します。 信頼境界機能と自動 QoS (auto qos voip インターフェイス コンフィギュレーション コマンド) を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show mls qos interface	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

信頼境界機能をディセーブルにするには、**no mls qos trust device** インターフェイス コンフィギュレーション コマンドを使用します。

DSCP トランスペアレント モードのイネーブル化

スイッチは透過的な DSCP 機能をサポートします。この機能は発信パケットの DSCP フィールドのみに作用します。デフォルトでは、DSCP 透過性はディセーブルです。スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service (QoS) に基づきます。

no mls qos rewrite ip dscp コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。



(注) DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプライオリティを提示する CoS 値を生成します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

特権 EXEC モードを開始して、透過的な DSCP 機能をスイッチでイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos	QoS をグローバルにイネーブルにします。
ステップ 3	no mls qos rewrite ip dscp	透過的な DSCP 機能をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

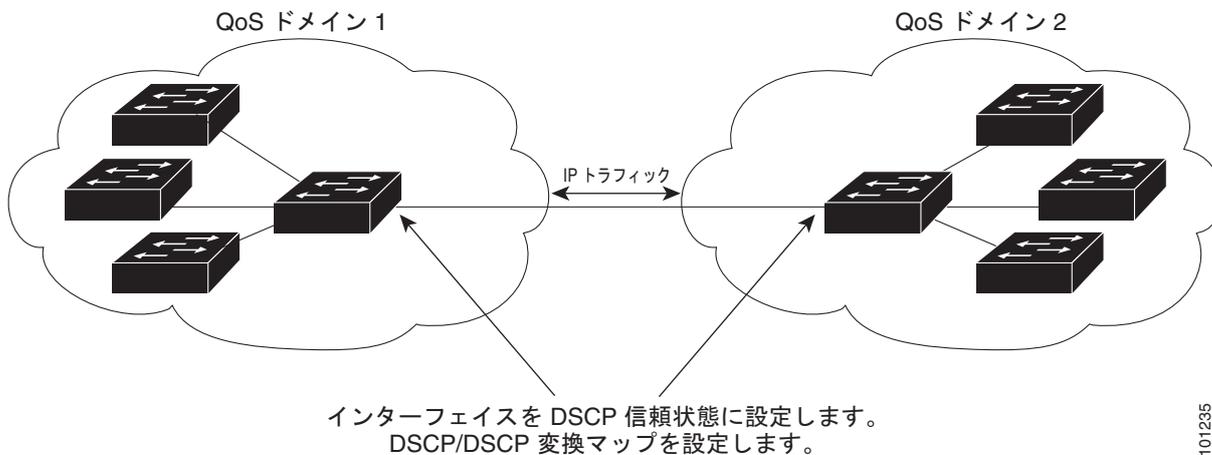
no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません (デフォルトの QoS 設定)。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust [cos | dscp]** インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます (図 39-13 を参照)。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 39-13 別の QoS ドメインとの境界ポートの DSCP 信頼状態



ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map dscp-mutation dscp-mutation-name in-dscp to out-dscp</code>	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 <ul style="list-style-type: none"> <code>dscp-mutation-name</code> には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 <code>in-dscp</code> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <code>out-dscp</code> には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	<code>interface interface-id</code>	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	<code>mls qos trust dscp</code>	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	<code>mls qos dscp-mutation dscp-mutation-name</code>	指定された DSCP trusted 入力ポートにマップを適用します。 <code>dscp-mutation-name</code> には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show mls qos maps dscp-mutation</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートを `trusted` 以外のステータスに戻すには、`no mls qos trust` インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、`no mls qos map dscp-mutation dscp-mutation-name` グローバル コンフィギュレーション コマンドを使用します。

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ~ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ (`gi0/2-mutation`) を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gi1/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/2-mutation
Switch(config-if)# end
```

QoS ポリシーの設定

QoS ポリシーを設定するには、通常、トラフィックをクラス別に分類し、各トラフィック クラスに適用するポリシーを設定し、ポリシーをポートに結合する必要があります。

基本情報については、「[分類](#)」(P.39-5) および「[ポリシングおよびマーキング](#)」(P.39-9) を参照してください。設定時の注意事項については、「[標準 QoS 設定時の注意事項](#)」(P.39-34) を参照してください。

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。ネットワーク設定に応じて、次の作業を 1 つまたは複数実行する必要があります。

- 「[ACL によるトラフィックの分類](#)」(P.39-44)
- 「[クラス マップによるトラフィックの分類](#)」(P.39-47)
- 「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.39-49)
- 「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.39-53)
- 「[集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング](#)」(P.39-60)

ACL によるトラフィックの分類

IP 標準 ACL または IP 拡張 ACL を使用することによって、IP トラフィックを分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用することによって分類できます。

IP トラフィック用に IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、アクセス リスト番号を入力します。有効範囲は 1 ~ 99 および 1300 ~ 1999 です。 <code>permit</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。<code>deny</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 <code>source</code> には、パケットの送信元となるネットワークまたはホストを指定します。<code>any</code> キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show access-lists</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、`no access-list access-list-number` グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

IP トラフィック用に IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard</code>	<p>IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、アクセス リスト番号を入力します。有効範囲は 100 ~ 199 および 2000 ~ 2699 です。 <code>permit</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。<code>deny</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 <code>protocol</code> には、IP プロトコルの名前または番号を入力します。疑問符 (?) を使用すると、使用できるプロトコル キーワードのリストが表示されます。 <code>source</code> には、パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、<code>source 0.0.0.0 source-wildcard 255.255.255.255</code> の短縮形として <code>any</code> キーワードを使用したり、<code>source 0.0.0.0</code> を表す <code>host</code> キーワードを使用します。 <code>source-wildcard</code> では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、<code>source 0.0.0.0 source-wildcard 255.255.255.255</code> の短縮形として <code>any</code> キーワードを使用したり、<code>source 0.0.0.0</code> を表す <code>host</code> キーワードを使用します。 <code>destination</code> には、パケットの宛先となるネットワークまたはホストを指定します。<code>destination</code> および <code>destination-wildcard</code> には、<code>source</code> および <code>source-wildcard</code> での説明と同じオプションを使用できます。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show access-lists</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、`no access-list access-list-number` グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック (precedence 値は 5) を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック (DSCP 値は 32) を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac access-list extended name	リスト名を指定し、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。
ステップ 3	{permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 <ul style="list-style-type: none"> <i>src-MAC-addr</i> には、パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 <i>mask</i> では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 <i>dst-MAC-addr</i> には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 (任意) <i>type mask</i> には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。<i>type</i> の範囲は 0 ~ 65535 です。通常は 16 進数で指定します。<i>mask</i> には、一致をテストする前に Ethertype に適用される don't care ビットを入力します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show access-lists [access-list-number access-list-name]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no mac access-list extended access-list-name** グローバル コンフィギュレーション コマンドを入力します。

次に、2 つの許可 (permit) ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番目のステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
```

```
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

クラス マップによるトラフィックの分類

個々のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。match ステートメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを 1 つ入力することによって定義します。



(注)

class ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。詳細については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.39-49) および「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.39-53) を参照してください。

クラス マップを作成し、トラフィックを分類するための一致条件を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	access-list access-list-number {deny permit} source [source-wildcard] または access-list access-list-number {deny permit} protocol source [source-wildcard] destination [destination-wildcard] または mac access-list extended name {permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「 ACL によるトラフィックの分類 」(P.39-44) を参照してください。 (注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

コマンド	目的
ステップ 3 class-map [match-all match-any] <i>class-map-name</i>	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定されていない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 4 match { access-group <i>acl-index-or-name</i> ip dscp <i>dscp-list</i> ip precedence <i>ip-precedence-list</i> }	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> • access-group <i>acl-index-or-name</i> には、ステップ 2 で作成した ACL の番号または名前を指定します。 • ip dscp <i>dscp-list</i> には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 • ip precedence <i>ip-precedence-list</i> には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 5 end	<p>特権 EXEC モードに戻ります。</p>
ステップ 6 show class-map	<p>設定を確認します。</p>
ステップ 7 copy running-config startup-config	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。一致条件を削除するには、**no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。

次に、*class1* というクラス マップの設定例を示します。*class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。このクラス マップによって、任意のホストから任意の宛先へのトラフィック (DSCP 値は 10) が許可されます。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
```

```
Switch#
```

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、*class2* という名前のクラスマップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラスマップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

実行対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。トラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラフィック クラスにトラフィック帯域幅限度を指定するアクション（ポリサー）や、トラフィックが不適切な場合の対処法を指定するアクション（マーキング）などを指定できます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- ポリシー マップの信頼状態およびポートの信頼状態は互いに排他的であり、最後に設定された方が有効となります。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp dscp1...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- ポートに定義したクラスごとに第 2 レベル ポリシー マップを別々に設定できます。第 2 レベルのポリシー マップは、各トラフィック クラスで実行するポリシング作業を指定します。階層型のポリシー マップの設定については、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング」(P.39-53) を参照してください。

- ポリシー マップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。

非階層型ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 class-map [match-all match-any] <i>class-map-name</i>	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定されていない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ3 policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ4 class <i>class-map-name</i>	<p>トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップ クラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ5 <code>trust [cos dscp ip-precedence]</code>	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。</p> <p>(注) このコマンドと <code>set</code> コマンドは、同じポリシー マップ内で相互に排他的になります。<code>trust</code> コマンドを入力する場合は、ステップ 6 へ進んでください。</p> <p>デフォルトでは、ポートは <code>trusted</code> ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは <code>dscp</code> です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • <code>cos</code> : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • <code>dscp</code> : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • <code>ip-precedence</code> : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.39-63) を参照してください。</p>
ステップ6 <code>set {dscp new-dscp ip precedence new-precedence}</code>	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • <code>dscp new-dscp</code> には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • <code>ip precedence new-precedence</code> には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。

	コマンド	目的
ステップ 7	police rate-bps burst-byte [exceed-action {drop policed-dscp-transmit}]	<p>分類したトラフィックにポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.39-34)を参照してください。</p> <ul style="list-style-type: none"> • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.39-65)を参照してください。
ステップ 8	exit	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	interface interface-id	<p>ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>有効なインターフェイスには、物理ポートが含まれます。</p>
ステップ 11	service-policy input policy-map-name	<p>ポリシーマップ名を指定し、入力ポートに適用します。</p> <p>サポートされるポリシー マップは、入力ポートに 1 つだけです。</p>
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show policy-map [policy-map-name [class class-map-name]]	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map policy-map-name** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class class-map-name** ポリシー マップ コンフィギュレーション コマンドを使用します。**untrusted** ステートに戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set {dscp new-dscp | ip precedence new-precedence}** ポリシー マップ コンフィギュレーション コマンドを使用します。既存のポリサーを削除するには、**no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]** ポリシー マップ コンフィギュレーション コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、**no service-policy input policy-map-name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポリシー マップを作成し、入力ポートに結合する例を示します。この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。この分類にトラフィックが一致した場合、着信パケットの DSCP 値が信頼されます。一致したトラフィックが平均トラフィック レート (48000 bps)、および標準バースト サイズ (8000 バイト) を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP はマークダウンされて、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
```

```
Switch(config)# policy-map flowlt
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input flowlt
```

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を示します。最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番目の許可ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

階層型ポリシー マップは SVI に設定できますが、他のタイプのインターフェイスには設定できません。階層型のポリシングは、VLAN レベルおよびインターフェイス レベルのポリシー マップで構成された、1 つのポリシー マップとして作成されます。

SVI では、VLAN レベルのポリシー マップに実行対象となるトラフィック クラスを指定します。アクションには、CoS、DSCP、IP precedence 値の信頼、またはトラフィック クラスの特定の DSCP、IP precedence 値の設定が含まれます。個々のポリサーで作用を受ける物理ポートを指定するには、インターフェイス レベルのポリシー マップを使用します。

階層型のポリシー マップを設定するときには、次の注意事項に従ってください。

- 階層型のポリシー マップを設定する前に、インターフェイス レベルのポリシー マップで指定した物理ポートの VLAN ベースの QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに付加できるポリシー マップは、1 つだけです。
- 1 つのポリシー マップに、それぞれ異なる一致条件とアクションを指定した複数のクラス ステートメントを指定できます。
- SVI で受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

- ポリシー マップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。
- **mls qos map ip-prec-dscp dscp1...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。**set ip dscp** コマンドを入力した場合、スイッチ コンフィギュレーションでは **set dscp** の設定として表示されます。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- VLAN ベースの QoS がイネーブルの場合、階層型のポリシー マップは直前に設定したポートベースのポリシー マップを優先します。
- 階層型のポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに影響します。VLAN レベルのポリシー マップで指定されたアクションは、その SVI のトラフィックに影響します。ポート レベルのポリシー マップのポリシングアクションは、影響のある物理インターフェイスの入力トラフィックに影響します。
- トランク ポートの階層型のポリシー マップを設定する場合、VLAN の範囲と重ならないようにしてください。範囲が重なると、ポリシー マップで指定されたアクションは、重なっている VLAN の着信トラフィックおよび発信トラフィックにも作用します。
- 集約ポリサーは階層型のポリシー マップではサポートされません。
- VLAN ベースの QoS がイネーブルになると、スイッチは VLAN マップなどの VLAN ベースの機能をサポートします。
- 階層型のポリシー マップは、プライベート VLAN のプライマリ VLAN 上にだけ設定できます。

特権 EXEC モードを開始して、階層型ポリシー マップを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>class-map [match-all match-any] class-map-name</code>	<p>VLAN レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。クラス マップについては、「クラスマップによるトラフィックの分類」(P.39-47) を参照してください。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <code>class-map-name</code> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定されていない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 3	<code>match {access-group acl-index-or-name ip dscp dscp-list ip precedence ip-precedence-list}</code>	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> • access-group acl-index-or-name には、ACL の番号または名前を指定します。 • ip dscp dscp-list には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 • ip precedence ip-precedence-list には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 4	<code>exit</code>	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 6 class-map [match-all match-any] <i>class-map-name</i>	<p>インターフェイス レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定されていない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 7 match input-interface <i>interface-id-list</i>	<p>インターフェイス レベルのクラス マップを実行する物理ポートを指定します。次の方法で、最大 6 つ指定できます。</p> <ul style="list-style-type: none"> • 単一のポート (1 つのエントリとしてカウントされます) • スペースで区切られたポートのリスト (各ポートが 1 つのエントリとしてカウントされます) • ハイフンで区切られたポートの範囲 (2 つのエントリとしてカウントされます) <p>このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。</p>
ステップ 8 exit	<p>クラスマップ コンフィギュレーション モードに戻ります。</p>
ステップ 9 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 10 policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力してインターフェイス レベルのポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されておらず、ポリサーも実行されていません。</p>
ステップ 11 class-map <i>class-map-name</i>	<p>インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシーマップのクラスマップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 12 police <i>rate-bps burst-byte</i> [exceed-action { drop policed-dscp-transmit }]	<p>分類したトラフィックにそれぞれポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.39-34)を参照してください。</p> <ul style="list-style-type: none"> • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.39-65)を参照してください。
ステップ 13 exit	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 14 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 15 policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力することによって VLAN レベルのポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ 16 class <i>class-map-name</i>	<p>VLAN レベルのトラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシーマップのクラスマップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 17 trust [cos dscp ip-precedence]	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。</p> <p>(注) このコマンドと set コマンドは、同じポリシー マップ内で相互に排他的になります。trust コマンドを入力する場合は、ステップ 18 を省略してください。</p> <p>デフォルトでは、ポートは trusted ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは dscp です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • cos : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • dscp : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • ip-precedence : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.39-63) を参照してください。</p>
ステップ 18 set {dscp new-dscp ip precedence new-precedence}	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • dscp new-dscp には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • ip precedence new-precedence には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。
ステップ 19 service-policy policy-map-name	<p>インターフェイスレベルのポリシーマップ名を指定し (ステップ 10 を参照)、VLAN レベルのポリシー マップと連動させます。</p> <p>VLAN レベルのポリシー マップで複数のクラスが指定されている場合、Cisco IOS Release 12.2(25)SED 以降は、各クラスで別々の service-policy policy-map-name コマンドを使用できます。</p>
ステップ 20 exit	<p>ポリシーマップ コンフィギュレーション モードに戻ります。</p>
ステップ 21 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 22 interface interface-id	<p>階層型のポリシー マップを適用する SVI を指定し、インターフェイス コンフィギュレーション モードを開始します。</p>

	コマンド	目的
ステップ 23	<code>service-policy input policy-map-name</code>	VLAN レベルのポリシーマップ名を指定し、SVI にそれを適用します。前のステップとこのコマンドを使用して、他の SVI にポリシーマップを適用します。 階層型 VLAN レベルのポリシーマップに複数のインターフェイスレベルのポリシーマップがある場合、すべてのクラスが <code>service-policy policy-map-name</code> コマンドで指定されている同じ VLAN レベルのポリシーマップに設定されている必要があります。
ステップ 24	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 25	<code>show policy-map [policy-map-name [class class-map-name]]</code> または <code>show mls qos vlan-based</code>	設定を確認します。
ステップ 26	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、`no policy-map policy-map-name` グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、`no class class-map-name` ポリシー マップ コンフィギュレーション コマンドを使用します。

ポリシー マップで `untrusted` ステートに戻すには、`no trust` ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、`no set {dscp new-dscp | ip precedence new-precedence}` ポリシーマップ コンフィギュレーション コマンドを使用します。

インターフェイス レベルのポリシー マップの既存のポリサーを削除するには、`no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` ポリシーマップ コンフィギュレーション コマンドを使用します。階層型のポリシー マップとポートの対応付けを削除するには、`no service-policy input policy-map-name` インターフェイス コンフィギュレーション コマンドを使用します。

次に、階層型のポリシー マップの作成方法を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
```

次に、SVI に新しいマップを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input g3/0/1 - g3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 7
```

```

Switch(config-pmap-c) # service-policy port-plcmap-1
Switch(config-pmap-c) # exit
Switch(config-pmap) # class cm-2
Switch(config-pmap-c) # match ip dscp 2
Switch(config-pmap-c) # service-policy port-plcmap-1
Switch(config-pmap) # exit
Switch(config-pmap) # class cm-3
Switch(config-pmap-c) # match ip dscp 3
Switch(config-pmap-c) # service-policy port-plcmap-2
Switch(config-pmap) # exit
Switch(config-pmap) # class cm-4
Switch(config-pmap-c) # trust dscp
Switch(config-pmap) # exit
Switch(config) # interface vlan 10
Switch(config-if) # ser input vlan-plcmap
Switch(config-if) # exit
Switch(config) # exit
Switch#

```

次の例では、子レベルのポリシー マップがクラス下に添付されるタイミング、そのクラスのアクションが指定される必要があるタイミングを示します。

```

Switch(config) # policy-map vlan-plcmap
Switch(config-pmap) # class cm-5
Switch(config-pmap-c) # set dscp 7
Switch(config-pmap-c) # service-policy port-plcmap-1
Switch(config-pmap-c) # exit
Switch(config-pmap) # exit
Switch(config) # exit

```

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシー マップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップにだけ設定できます。

集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop policed-dscp-transmit}</code>	<p>同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。</p> <p>デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.39-34) を参照してください。</p> <ul style="list-style-type: none"> • <code>aggregate-policer-name</code> には、集約ポリサーの名前を指定します。 • <code>rate-bps</code> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <code>burst-byte</code> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.39-65) を参照してください。
ステップ3	<code>class-map [match-all match-any] class-map-name</code>	必要に応じて、トラフィックを分類するクラス マップを作成します。詳細については、「クラス マップによるトラフィックの分類」(P.39-47) を参照してください。
ステップ4	<code>policy-map policy-map-name</code>	<p>ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>詳細については、「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」(P.39-49) を参照してください。</p>
ステップ5	<code>class class-map-name</code>	<p>トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。</p> <p>詳細については、「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」(P.39-49) を参照してください。</p>
ステップ6	<code>police aggregate aggregate-policer-name</code>	<p>同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。</p> <p><code>aggregate-policer-name</code> には、ステップ 2 で指定した名前を入力します。</p>
ステップ7	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ8	<code>interface interface-id</code>	<p>ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>有効なインターフェイスには、物理ポートが含まれます。</p>

	コマンド	目的
ステップ 9	<code>service-policy input policy-map-name</code>	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show mls qos aggregate-policer [aggregate-policer-name]</code>	設定を確認します。
ステップ 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された集約ポリサーをポリシー マップから削除するには、**no police aggregate aggregate-policer-name** ポリシー マップ コンフィギュレーション モードを使用します。集約ポリサーおよびそのパラメータを削除するには、**no mls qos aggregate-policer aggregate-policer-name** グローバル コンフィギュレーション コマンドを使用します。

次に、集約ポリサーを作成して、ポリシー マップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。トラフィックが平均レート (48000 bps)、および標準バースト サイズ (8000 バイト) を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP がマークダウンされて、送信されます。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

DSCP マップの設定

ここでは、次の設定について説明します。

- 「CoS/DSCP マップの設定」(P.39-63) (任意)
- 「IP precedence/DSCP マップの設定」(P.39-64) (任意)
- 「ポリシング済み DSCP マップの設定」(P.39-65) (任意、マップのヌル設定が不適切な場合以外)

- 「DSCP/CoS マップの設定」(P.39-66) (任意)
- 「DSCP/DSCP 変換マップの設定」(P.39-67) (任意、マップのヌル設定が不適切な場合以外)

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。

表 39-12 に、デフォルトの CoS/DSCP マップを示します。

表 39-12 デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mls qos map cos-dscp dscp1...dscp8</code>	CoS/DSCP マップを変更します。 <i>dscp1...dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mls qos maps cos-dscp</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos cos-dscp` グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp
```

```
Cos-dscp map:
cos:    0  1  2  3  4  5  6  7
```

```
-----
dscp: 10 15 20 25 30 35 40 45
```

IP precedence/DSCP マップの設定

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。

表 39-13 に、デフォルトの IP precedence/DSCP マップを示します。

表 39-13 デフォルトの IP Precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map ip-prec-dscp <i>dscp1...dscp8</i>	IP precedence/DSCP マップを変更します。 <i>dscp1...dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos maps ip-prec-dscp	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
  ipprec:  0  1  2  3  4  5  6  7
  -----
          dscp: 10 15 20 25 30 35 40 45
```

ポリシング済み DSCP マップの設定

ポリシングおよびマーキングアクションによって得られる新しい値に DSCP 値をマークダウンするには、ポリシング済み DSCP マップを使用します。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>mls qos map policed-dscp dscp-list to mark-down-dscp</code>	ポリシング済み DSCP マップを変更します。 <ul style="list-style-type: none"> <code>dscp-list</code> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <code>mark-down-dscp</code> には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mls qos maps policed-dscp</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos policed-dscp` グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 50 ~ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :   00 01 02 03 04 05 06 07 08 09
  1 :   10 11 12 13 14 15 16 17 18 19
  2 :   20 21 22 23 24 25 26 27 28 29
  3 :   30 31 32 33 34 35 36 37 38 39
  4 :   40 41 42 43 44 45 46 47 48 49
  5 :   00 00 00 00 00 00 00 00 58 59
  6 :   60 61 62 63
```



(注)

このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。

表 39-14 に、デフォルトの DSCP/CoS マップを示します。

表 39-14 デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0 ~ 7	0
8 ~ 15	1
16 ~ 23	2
24 ~ 31	3
32 ~ 39	4
40 ~ 47	5
48 ~ 55	6
56 ~ 63	7

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

特権 EXEC モードで開始し、次の手順に従って DSCP/CoS マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map dscp-cos dscp-list to cos</code>	DSCP/CoS マップを変更します。 <ul style="list-style-type: none"> <code>dscp-list</code> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <code>cos</code> には、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ~ 63、CoS の範囲は 0 ~ 7 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps dscp-to-cos</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos dscp-cos` グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
0 :    00 00 00 00 00 00 00 00 00 01
1 :    01 01 01 01 01 01 00 02 02 02
2 :    02 02 02 02 00 03 03 03 03 03
```

```

3 :   03 03 00 04 04 04 04 04 04 04
4 :   00 05 05 05 05 05 05 05 00 06
5 :   00 06 06 06 06 06 07 07 07 07
6 :   07 07 07 07

```



(注) 上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。

DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します (入力変換)。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を使用してパケットを処理します。スイッチは、新しい DSCP 値とともにそのパケットをポートへ送じます。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map dscp-mutation <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを変更します。 <ul style="list-style-type: none"> <i>dscp-mutation-name</i> には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 <i>in-dscp</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>out-dscp</i> には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	interface interface-id	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	mls qos dscp-mutation <i>dscp-mutation-name</i>	指定された DSCP trusted 入力ポートにマップを適用します。 <i>dscp-mutation-name</i> には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mls qos maps dscp-mutation	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos dscp-mutation dscp-mutation-name** グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。明示的に設定されていないすべてのエントリは変更されません（空のマップで指定された値のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
mutation1:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 00 10 10
1 : 10 10 10 10 14 15 16 17 18 19
2 : 20 20 20 23 24 25 26 27 28 29
3 : 30 30 30 30 30 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```



(注)

上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

入力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- 各キューに（DSCP 値または CoS 値によって）割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック（音声など）の有無

ここでは、次の設定について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.39-69) (任意)
- 「入力キュー間のバッファ スペースの割り当て」(P.39-70) (任意)
- 「入力キュー間の帯域幅の割り当て」(P.39-71) (任意)
- 「入力プライオリティ キューの設定」(P.39-71) (任意)

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 mls qos srr-queue input dscp-map queue <i>queue-id</i> threshold <i>threshold-id</i> dscp1...dscp8 または mls qos srr-queue input cos-map queue <i>queue-id</i> threshold <i>threshold-id</i> cos1...cos8	<p>DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。</p> <p>デフォルトでは、DSCP 値 0 ~ 39 および 48 ~ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ~ 47 はキュー 2 およびしきい値 1 にマッピングされます。</p> <p>デフォルトでは、CoS 値 0 ~ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。</p> <ul style="list-style-type: none"> <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 <i>dscp1...dscp8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。 <i>cos1...cos8</i> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
ステップ3 mls qos srr-queue input threshold <i>queue-id</i> threshold-percentage1 threshold-percentage2	<p>入力キューに 2 つの WTD しきい値の割合 (しきい値 1 および 2 用) を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。</p> <ul style="list-style-type: none"> <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。 <i>threshold-percentage1 threshold-percentage2</i> の範囲は、1 ~ 100 です。各値はスペースで区切ります。 <p>各しきい値は、キューに割り当てられたキュー記述子の総数に対する割合です。</p>
ステップ4 end	特権 EXEC モードに戻ります。
ステップ5 show mls qos maps	<p>設定を確認します。</p> <p>DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点にキュー ID およびしきい値 ID があります。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。</p> <p>CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。</p>
ステップ6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの CoS 入力キューしきい値マップまたはデフォルトの DSCP 入力キューしきい値マップに戻すには、**no mls qos srr-queue input cos-map**、または **no mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD しきい値の割合に戻すには、**no mls qos srr-queue input threshold queue-id** グローバル コンフィギュレーション コマンドを使用します。

次の例では、DSCP 値 0～6 を、入力キュー 1 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20～26 は、入力キュー 1 とドロップしきい値 70% のしきい値 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

この例では、50% の WTD しきい値が DSCP 値 (0～6) に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値 (20～26) よりも先にドロップされます。

入力キュー間のバッファ スペースの割り当て

2 つのキュー間で入力バッファを分割する比率を定義します (スペース量を割り当てます)。バッファ割り当てと帯域幅割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量が制御されます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input buffers percentage1 percentage2	入力キュー間にバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 <i>percentage1 percentage2</i> の範囲は、0～100 です。各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos interface buffer または show mls qos input-queue	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos srr-queue input buffers** グローバル コンフィギュレーション コマンドを使用します。

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。帯域幅割り当てとバッファ割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量を制御できます。入力キューで SRR が動作するのは、共有モードの場合のみです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	mls qos srr-queue input bandwidth weight1 weight2	入力キューに共有ラウンド ロビン重みを割り当てます。 <i>weight1</i> および <i>weight2</i> のデフォルト設定は 4 です (帯域幅の 1/2 が 2 つのキューで等しく共有されます)。 <i>weight1</i> および <i>weight2</i> の範囲は、1 ~ 100 です。各値はスペースで区切ります。 SRR は、 mls qos srr-queue input priority-queue queue-id bandwidth weight グローバル コンフィギュレーション コマンドの bandwidth キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は mls qos srr-queue input bandwidth weight1 weight2 グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。詳細については、「 入力プライオリティ キューの設定 」(P.39-71) を参照してください。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show mls qos interface queuing または show mls qos input-queue	入力内容を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/ (25+75)、キュー 2 が 75/ (25+75) です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

入力プライオリティ キューの設定

プライオリティ キューは、優先して進める必要があるトラフィックに限り使用してください (遅延とジッタを最小限にとどめる必要のある音声トラフィックなど)。

プライオリティ キューは、オーバーサブスクリプトリングに激しいネットワーク トラフィックが発生している状況で (バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームがドロップされている場合)、遅延およびジッタを軽減するように帯域幅の一部が保証されています。

SRR は、`mls qos srr-queue input priority-queue queue-id bandwidth weight` グローバル コンフィギュレーション コマンドの `bandwidth` キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に、SRR は `mls qos srr-queue input bandwidth weight1 weight2` グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code>	<p>キューをプライオリティ キューとして割り当て、内部リングが輻輳している場合にリングの帯域幅を保証します。</p> <p>デフォルトのプライオリティ キューはキュー 2 です。このキューには帯域幅の 10% が割り当てられています。</p> <ul style="list-style-type: none"> <code>queue-id</code> で指定できる範囲は 1 ~ 2 です。 <code>bandwidth weight</code> には、内部リングの帯域幅に対する割合を割り当てます。指定できる範囲は 0 ~ 40 です。値が大きい場合はリング全体に影響が及び、パフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos interface queueing</code> または <code>show mls qos input-queue</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no mls qos srr-queue input priority-queue queue-id` グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、`mls qos srr-queue input priority-queue queue-id bandwidth 0` を入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 および 2 に割り当てられている帯域幅比率は $4/(4+4)$ です。SRR は最初、設定された 10% の帯域幅をキュー 1 (プライオリティ キュー) にサービスします。その後、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット (ポートごとの 4 つの出力キュー) に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キュー セットに割り当てる固定バッファ スペースの量

- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

ここでは、次の設定について説明します。

- 「設定時の注意事項」(P.39-73)
- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」(P.39-73) (任意)
- 「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.39-75) (任意)
- 「出力キューでの SRR シェーピング重みの設定」(P.39-76) (任意)
- 「出力キューでの SRR 共有重みの設定」(P.39-77) (任意)
- 「出力緊急キューの設定」(P.39-78) (任意)
- 「出力インターフェイスの帯域幅の制限」(P.39-79) (任意)

設定時の注意事項

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して `shaped` モードは `shared` モードを無効にし、SRR はこのキューに `shaped` モードでサービスを提供します。
- 出力緊急キューがディセーブルで、SRR シェーピング重みが設定されていない場合、SRR はこのキューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファの可用性の保証、WTD の設定、およびキューセットの最大割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。

各しきい値はキューに割り当てられたバッファの割合です。このパーセント値を指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

キューセットのメモリ割り当てとドロップしきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos queue-set output <i>qset-id</i> buffers <i>allocation1</i> ... <i>allocation4</i></code>	<p>キューセットにバッファを割り当てます。</p> <p>デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます (25、25、25、25)。各キューがバッファ スペースの 1/4 を持ちます。</p> <ul style="list-style-type: none"> • <i>qset-id</i> には、キューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • <i>allocation1</i> ... <i>allocation4</i> には、キューセット内のキューごとに 1 つずつ、合計 4 つのパーセンテージを指定します。<i>allocation1</i>、<i>allocation3</i>、<i>allocation4</i> の場合、使用可能な範囲は 0 ~ 99 です。<i>allocation2</i> の場合、範囲は 1 ~ 100 です (CPU バッファを含める)。 <p>トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。</p>
ステップ 3	<code>mls qos queue-set output <i>qset-id</i> threshold <i>queue-id</i> <i>drop-threshold1</i> <i>drop-threshold2</i> <i>reserved-threshold</i> <i>maximum-threshold</i></code>	<p>WTD を設定し、バッファの可用性を保証し、キューセット (ポートごとに 4 つの出力キュー) の最大メモリ割り当てを設定します。</p> <p>デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべてのキューの最大は 400% に設定されています。</p> <ul style="list-style-type: none"> • <i>qset-id</i> には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。 • <i>queue-id</i> には、コマンドの実行対象となるキューセット内の特定のキューを入力します。指定できる範囲は 1 ~ 4 です。 • <i>drop-threshold1</i> <i>drop-threshold2</i> には、キューの割り当てメモリの割合として表される 2 つの WTD しきい値を指定します。指定できる範囲は 1 ~ 3200% です。 • <i>reserved-threshold</i> には、割り当てメモリの割合として表されるキューに保証 (確保) されるメモリ サイズを入力します。指定できる範囲は 1 ~ 100% です。 • <i>maximum-threshold</i> を指定すると、いっぱいになったキューが確保量を超えるバッファを取得できるようになります。この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。指定できる範囲は 1 ~ 3200% です。
ステップ 4	<code>interface <i>interface-id</i></code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>queue-set <i>qset-id</i></code>	<p>キューセットにポートをマッピングします。</p> <p><i>qset-id</i> には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。デフォルトは 1 です。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<code>show mls qos interface [interface-id] buffers</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no mls qos queue-set output qset-id buffers` グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD の割合に戻すには、`no mls qos queue-set output qset-id threshold [queue-id]` グローバル コンフィギュレーション コマンドを使用します。

次の例では、ポートをキューセット 2 にマッピングする方法を示します。出力キュー 1 にはバッファスペースの 40%、出力キュー 2、3、および 4 には 20% が割り当てられます。キュー 2 のドロップしきい値は割り当てメモリの 40 および 60% に設定され、割り当てメモリの 100% が保証 (確保) され、パケットがドロップされるまでこのキューが使用できる最大メモリが 200% に設定されます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# queue-set 2
```

出力キューおよび ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

DSCP または CoS 値を出力キューおよび ID にマッピングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8</code> または <code>mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8</code>	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ~ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ~ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ~ 39 および 48 ~ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ~ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 <ul style="list-style-type: none"> • <code>queue-id</code> で指定できる範囲は 1 ~ 4 です。 • <code>threshold-id</code> で指定できる範囲は 1 ~ 3 です。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいつぱいの状態に対して設定されます。 • <code>dscp1...dscp8</code> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 63 です。 • <code>cos1...cos8</code> には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps</code>	設定を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点 queuer ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、`no mls qos srr-queue output dscp-map` または `no mls qos srr-queue output cos-map` グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

出力キューでの SRR シェーピング重みの設定

各キューに割り当てられる使用可能な帯域幅の量を指定できます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。シェーピング重みの詳細については、「[SRR のシェーピングおよび共有](#)」(P.39-15) を参照してください。共有重みの詳細については、「[出力キューでの SRR 共有重みの設定](#)」(P.39-77) を参照してください。

ポートにマッピングされた 4 つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	srr-queue bandwidth shape weight1 weight2 weight3 weight4	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 <i>weight1 weight2 weight3 weight4</i> には、シェーピングされるポートの割合を制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比率 ($1/\text{weight}$) によって制御されます。各値はスペースで区切ります。指定できる範囲は 0 ~ 65535 です 重み 0 を設定した場合は、対応するキューが共有モードで動作します。 srr-queue bandwidth shape コマンドで指定された重みは無視され、 srr-queue bandwidth share インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface interface-id queuing	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

次に、キュー 1 に帯域幅のシェーピングを設定する例を示します。キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8 (12.5%) です。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

出力キューでの SRR 共有重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。



(注) 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

ポートにマッピングされた 4 つの出力キューに共有重みを割り当てて、帯域幅の共有をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>srr-queue bandwidth share weight1 weight2 weight3 weight4</code>	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です (各キューに帯域幅の 1/4 が割り当てられています)。 <code>weight1 weight2 weight3 weight4</code> には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。有効値は 1 ~ 255 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface interface-id queueing</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth share` インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー 1、2、3、および 4 に対して $1/(1+2+3+4)$ 、 $2/(1+2+3+4)$ 、 $3/(1+2+3+4)$ 、および $4/(1+2+3+4)$ になります (それぞれ、10、20、30、および 40%)。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のすべてのパケットより高く設定できます。SRR は、このキューが空になるまで処理してから他のキューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ3	<code>interface interface-id</code>	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	<code>priority-queue out</code>	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、 srr-queue bandwidth shape または srr-queue bandwidth share コマンドの <i>weight1</i> が無視されます（比率計算に使用されません）。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show running-config</code>	設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

出力緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

出インターフェイスの帯域幅の制限

出力ポートの帯域幅は制限できます。たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。



(注)

出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

出力ポートの帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	レート制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>srr-queue bandwidth limit weight1</code>	ポートの上限となるポート速度の割合を指定します。指定できる範囲は 10 ~ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show mls qos interface [interface-id] queueing</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth limit` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。回線レートは接続速度の 80% (800 Mbps) に低下します。ただし、ハードウェアはライン レートを 6% 単位で調整しているため、この値は厳密ではありません。

標準 QoS 情報の表示

標準 QoS 情報を表示するには、表 39-15 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 39-15 標準 QoS 情報を表示するためのコマンド

コマンド	目的
<code>show class-map [class-map-name]</code>	トラフィックを分類するための一致条件を定義した QoS クラス マップを表示します。
<code>show mls qos</code>	グローバル QoS コンフィギュレーション情報を表示します。
<code>show mls qos aggregate-policer [aggregate-policer-name]</code>	集約ポリサーの設定を表示します。
<code>show mls qos input-queue</code>	入力キューの QoS 設定を表示します。
<code>show mls qos interface [interface-id] [buffers policers queueing statistics]</code>	バッファ割り当て、ポリサーが設定されるポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。
<code>show mls qos maps [cos-dscp cos-input-q cos-output-q dscp-cos dscp-input-q dscp-mutation dscp-mutation-name dscp-output-q ip-prec-dscp policed-dscp]</code>	QoS マッピング情報を表示します。
<code>show mls qos queue-set [qset-id]</code>	出力キューの QoS 設定を表示します。
<code>show mls qos vlan vlan-id</code>	指定の SVI に適用されたポリシー マップを表示します。
<code>show policy-map [policy-map-name [class class-map-name]]</code>	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 (注) 着信トラフィックの分類情報を表示する場合は、 <code>show policy-map interface</code> 特権 EXEC コマンドを使用しないでください。 <code>control-plane</code> および <code>interface</code> キーワードはサポートされていません。表示される統計情報は無視してください。
<code>show running-config include rewrite</code>	透過的な DSCP 設定を表示します。



CHAPTER 40

EtherChannel およびリンクステート トラッキングの設定

この章では、IE 3000 スイッチに EtherChannel を設定する手順について説明します。EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用すると、ワイヤリング クローゼットおよびデータ センタ間の帯域幅を拡張できます。EtherChannel はネットワーク上でボトルネックの発生が見込まれるところに、任意に配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャンネル内の他のリンクにトラフィックをリダイレクトします。この章では、リンクステート トラッキングを設定する方法についても説明します。



(注)

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

- 「EtherChannel の概要」 (P.40-1)
- 「EtherChannel の設定」 (P.40-9)
- 「EtherChannel、PAgP、および LACP ステータスの表示」 (P.40-21)
- 「リンクステート トラッキングの概要」 (P.40-22)
- 「リンクステート トラッキングの設定」 (P.40-24)

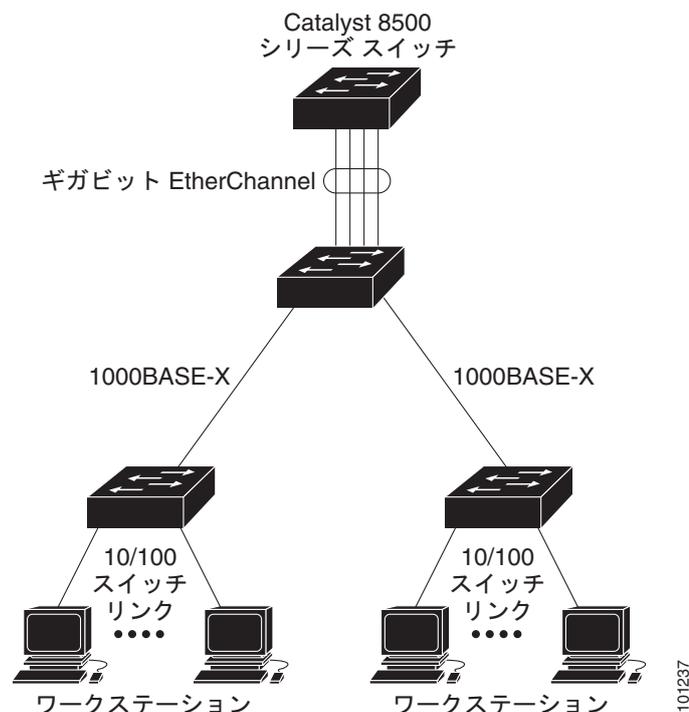
EtherChannel の概要

- 「EtherChannel の概要」 (P.40-2)
- 「ポートチャンネル インターフェイス」 (P.40-3)
- 「ポート集約プロトコル」 (P.40-4)
- 「LACP」 (P.40-6)
- 「EtherChannel の On モード」 (P.40-7)
- 「ロード バランシングおよび転送方式」 (P.40-7)

EtherChannel の概要

EtherChannel は、単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます (図 40-1 を参照)。

図 40-1 一般的な EtherChannel 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 800Mbps (ファスト EtherChannel) または 8 Gbps (ギガビット EtherChannel) の全二重帯域幅を提供します。各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel の数は 6 に制限されています。EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。詳細については、第 14 章「インターフェイス特性の設定」を参照してください。



(注) レイヤ 3 EtherChannel は、IP サービス イメージが稼働しているスイッチでだけサポートされます。

詳細については、「EtherChannel 設定時の注意事項」(P.40-10) を参照してください。

EtherChannel は、Port Aggregation Protocol (PAgP; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、または On のいずれかのモードに設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。互換性のないポートは独立ステートになり、他の単一リンクのようにデータ トラフィックを伝送し続けます。ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を on モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel のもう一方の端 (他のスイッチ上) も、同じように on モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生します。

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

ポートチャネル インターフェイス

EtherChannel を作成すると、ポート チャネル論理インターフェイスも作成されます。

- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを動的に作成します。

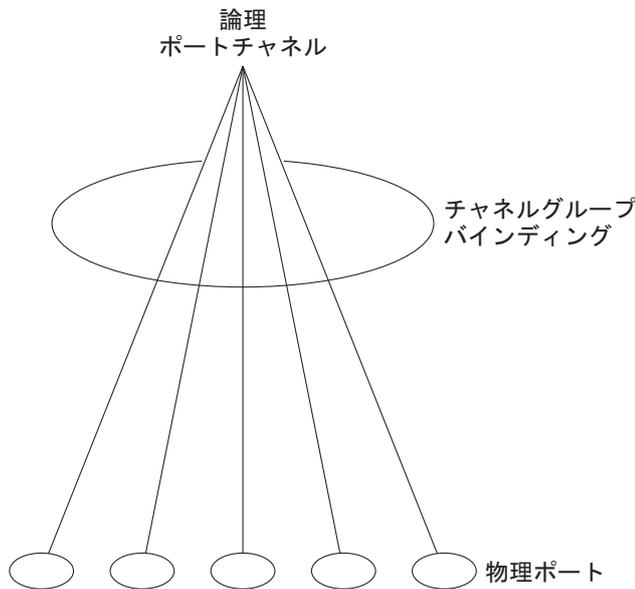
また、**interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group channel-group-number** コマンドを使用する必要があります。**channel-group-number** は **port-channel-number** と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

レイヤ 2 およびレイヤ 3 ポートのいずれの場合も、**channel-group** コマンドを実行すると、物理ポートと論理インターフェイスがバインドされます (図 40-2 を参照)。

各 EtherChannel には、1 から 6 の番号が付けられたポートチャネル論理インターフェイスがあります。このポートチャネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定された番号に対応します。

図 40-2 物理ポート、論理ポートチャンネル、およびチャンネル グループの関係



EtherChannel の設定後、ポートチャンネル インターフェイスに適用した設定変更は、そのポートチャンネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャンネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、`spanning-tree` コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

ポート集約プロトコル

Port Aggregation Protocol (PAgP) はシスコ独自のプロトコルで、Cisco スイッチおよび PAgP をサポートするベンダーによってライセンス供与されたスイッチでのみ稼働します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャンネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランッキング ステータス、およびトランッキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、PAgP は単一スイッチ ポートとして、スパンニングツリーにそのグループを追加します。

PAgP モード

表 40-1 に、**channel-group** インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel PAgP モードを示します。

表 40-1 EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランッキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

PAgP モードが異なっても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャンネル グループにポートを結合し、このポートが伝送に使用されます。

PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出

仮想スイッチは、Virtual Switch Link (VSL; 仮想スイッチ リンク) により接続された複数の Catalyst 6500 コア スイッチであり、それらのスイッチ間で制御情報とデータ トラフィックを伝送します。スイッチのうちの 1 つはアクティブ モードです。その他のスイッチはスタンバイ モードです。冗長性のため、リモート スイッチはリモート サテライト リンク (RSL) によって仮想スイッチに接続されます。

2 つのスイッチ間の VSL に障害が発生すると、一方のスイッチは他方のスイッチのステータスを認識しません。両方のスイッチがアクティブ モードになり、ネットワークを、重複したコンフィギュレーション (IP アドレスおよびブリッジ ID の重複を含む) を伴うデュアルアクティブの状態にする可能性があります。ネットワークがダウンする場合があります。

デュアルアクティブの状態を防止するために、コア スイッチは PAgP Protocol Data Unit (PDU; プロトコル データ ユニット) を RSL を介してリモート スイッチに送信します。PAgP PDU はアクティブ スイッチを識別し、リモート スイッチは、コア スイッチが同期化するように PDU をコア スイッチに転送します。アクティブ スイッチに障害が発生した場合、またはアクティブ スイッチがリセットされた場合は、スタンバイ スイッチがアクティブ スイッチの役割を引き継ぎます。VSL がダウンした場合は、1 つのコア スイッチが他のコア スイッチのステータスを認識して状態を変更しません。

PAgP と他の機能との相互作用

Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) および Cisco Discovery Protocol (CDP) は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP Protocol Data Unit (PDU; プロトコル データ ユニット) を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

LACP

LACP は IEEE 802.3ad で定義されており、Cisco スイッチが IEEE 802.3ad プロトコルに適合したスイッチ間のイーサネット チャンネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク (チャンネルまたは集約ポート) に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一スイッチ ポートとして、スパニングツリーにそのグループを追加します。

LACP モード

表 40-2 に、`channel-group` インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel LACP モードを示します。

表 40-2 EtherChannel LACP モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

LACP モードが異なっても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- どのポートも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートとは EtherChannel を形成できません。

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを渡します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

LACP が LACP PDU を送受信するのは、LACP が **active** モードまたは **passive** モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャンネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されていたとしても、互換性のないポートは **suspended** ステートになります。



注意

on モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパンニングツリー ループが発生することがあります。

ロード バランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャンネル内の 1 つのリンクを選択する数値に縮小することによって、チャンネル内のリンク間でトラフィックのロード バランシングを行います。EtherChannel のロード バランシングには、MAC アドレスまたは IP アドレス、送信元アドレスや宛先アドレスのどちらか一方、またはその両方のアドレスを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャンネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャンネル ポートを使用しますが、送信元ホストが同じパケットは同じチャンネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されている宛先ホストの MAC アドレスに基づいてチャンネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャンネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャンネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のスイッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャンネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、IP アドレスが異なるパケットはそれぞれ異なるチャンネル ポートを使用しますが、IP アドレスが同じパケットは同じチャンネル ポートを使用します。

宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャンネル ポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャンネル ポートで送信されます。

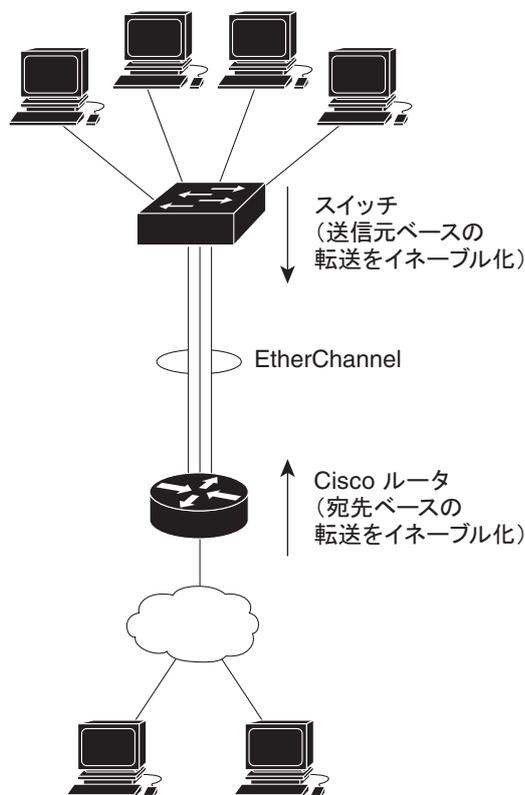
送信元/宛先 IP アドレスベース転送の場合、パケットは EtherChannel に送信されて、着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたものです。特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャンネル ポートを使用できます。

ロード バランシング方式ごとに利点異なります。ロード バランシング方式は、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。

図 40-3 では、4 つのワークステーションからデータを集約しているスイッチからの EtherChannel がルータと通信しています。ルータは単一 MAC アドレス デバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

設定で一番種類が多くなるオプションを使用してください。たとえば、チャンネル上のトラフィックが単一 MAC アドレスのみを宛先とする場合、宛先 MAC アドレスを使用すると、チャンネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなる場合があります。

図 40-3 負荷の分散および転送方式



101239

EtherChannel の設定

ここでは、次の設定について説明します。

- 「EtherChannel のデフォルト設定」 (P.40-10)
- 「EtherChannel 設定時の注意事項」 (P.40-10)
- 「レイヤ 2 EtherChannel の設定」 (P.40-11) (必須)
- 「レイヤ 3 EtherChannel の設定」 (P.40-14) (必須)
- 「EtherChannel ロード バランシングの設定」 (P.40-17) (任意)
- 「PAgP 学習方式およびプライオリティの設定」 (P.40-18) (任意)
- 「LACP ホットスタンバイ ポートの設定」 (P.40-19) (任意)



(注) 必ず、ポートを正しく設定してください。詳細については、「EtherChannel 設定時の注意事項」(P.40-10) を参照してください。



(注) EtherChannel の設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネルインターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

EtherChannel のデフォルト設定

表 40-3 に、EtherChannel のデフォルト設定を示します。

表 40-3 EtherChannel のデフォルト設定

機能	デフォルト設定
チャンネル グループ	割り当てなし
ポートチャンネル論理インターフェイス	未定義
PAgP モード	デフォルトなし
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システム プライオリティおよびスイッチ MAC アドレス
ロード バランシング	着信パケットの送信元 MAC アドレスに基づいてスイッチ上で負荷を分散

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- 648 を超える数の EtherChannel をスイッチで設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- LACP EtherChannel は、同じタイプのイーサネット ポートを最大 16 まで使用して設定します。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。shutdown インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
 - 許可 VLAN リスト
 - 各 VLAN のスパニングツリーパス コスト
 - 各 VLAN のスパニングツリー ポート プライオリティ
 - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。

- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP が稼働している複数の EtherChannel グループは、同じスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- EtherChannel の一部として Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 宛先ポートを設定しないでください。
- プライベート VLAN ポートを EtherChannel の一部として設定しないでください。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がスイッチ インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をスイッチ上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除してください。
- レイヤ 2 EtherChannel の場合
 - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
 - トランク ポートから EtherChannel を設定する場合は、すべてのトランクでトランッキング モード (ISL (スイッチ間リンク) または IEEE 802.1Q) が同じであることを確認してください。EtherChannel ポートのトランクのモードが一致していないと、予想外の結果になる可能性があります。
 - EtherChannel は、トランッキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
 - スパニングツリーパス コストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリーパス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。
- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャンネル内の物理ポートでなく、ポートチャンネル論理インターフェイスに割り当ててください。

レイヤ 2 EtherChannel の設定

2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャンネル グループにポートを割り当てます。このコマンドにより、ポートチャンネル論理インターフェイスが自動的に作成されます。

■ EtherChannel の設定

レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
ステップ 3	<code>switchport mode {access trunk}</code> <code>switchport access vlan vlan-id</code>	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ~ 4094 です。

コマンド	目的
ステップ4 channel-group <i>channel-group-number</i> mode { auto [non-silent] desirable [non-silent] on } { active passive }	<p>チャンネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。</p> <p><i>channel-group-number</i> の範囲は 1 ~ 648 です。</p> <p>mode には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • auto : PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • desirable : PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • on : PAgP や LACP を使用しないで、ポートを強制的にチャンネル化します。on モードでは、使用可能な EtherChannel が存在するのは、on モードのポート グループが、on モードの別のポート グループに接続する場合だけです。 • non-silent : (任意) PAgP 対応のデバイスに接続されたスイッチのポートが auto または desirable モードの場合に、非サイレント動作を行うようにこのポートを設定します。non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイルサーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネル グループにポートを結合し、このポートが伝送に使用されます。 • active : LACP デバイスが検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • passive : ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 <p>スイッチおよびデバイスのモードの互換性に関する情報については、「PAgP モード」(P.40-5) および「LACP モード」(P.40-6) を参照してください。</p>
ステップ5 end	特権 EXEC モードに戻ります。
ステップ6 show running-config	設定を確認します。
ステップ7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel グループからポートを削除するには、**no channel-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャンネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティック アクセス ポートとして、LACP モードが **active** であるチャンネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel を設定するには、ポートチャンネル論理インターフェイスを作成し、そのポートチャンネルにイーサネット ポートを組み込みます。次に設定方法を説明します。

ポートチャンネル論理インターフェイスの作成

レイヤ 3 EtherChannel を設定する場合、まず **interface port-channel** グローバル コンフィギュレーション コマンドを使用し、ポートチャンネル論理インターフェイスを手動で作成しなければなりません。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して論理インターフェイスをチャンネル グループに配置します。



(注) 物理ポートから EtherChannel に IP アドレスを移動するには、物理ポートから IP アドレスを削除してから、その IP アドレスをポートチャンネル インターフェイス上で設定する必要があります。

レイヤ 3 EtherChannel 用のポートチャンネル インターフェイスを作成するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>port-channel-number</i>	ポートチャンネル論理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 <i>port-channel-number</i> の範囲は 1 ~ 486 です。
ステップ 3	no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 4	ip address <i>ip-address mask</i>	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show etherchannel <i>channel-group-number detail</i>	設定を確認します。

	コマンド	目的
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ8		レイヤ 3 EtherChannel にイーサネット ポートを割り当てます。詳細については、「物理インターフェイスの設定」(P.40-15) を参照してください。

ポートチャネルを削除するには、`no interface port-channel port-channel-number` グローバル コンフィギュレーション コマンドを使用します。

次に、論理ポート チャネル 5 を作成し、IP アドレスとして 172.10.20.10 を割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

物理インターフェイスの設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 個をアクティブに、最大 8 個をスタンバイ モードにできます。
ステップ3	<code>no ip address</code>	この物理ポートに割り当てられている IP アドレスをすべて削除します。
ステップ4	<code>no switchport</code>	ポートをレイヤ 3 モードにします。

コマンド	目的
ステップ 5 <code>channel-group channel-group-number mode {auto [non-silent] desirable [non-silent] on} {active passive}</code>	<p>チャンネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。</p> <p><code>channel-group-number</code> の範囲は 1 ~ 486 です。この番号は、「ポートチャンネル論理インターフェイスの作成」(P.40-14) で設定した <code>port-channel-number</code> (論理ポート) と同一である必要があります。</p> <p><code>mode</code> には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • auto : PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • desirable : PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • on : PAgP や LACP を使用しないで、ポートを強制的にチャンネル化します。<code>on</code> モードでは、使用可能な EtherChannel が存在するのは、<code>on</code> モードのポート グループが、<code>on</code> モードの別のポート グループに接続する場合だけです。 • non-silent : (任意) PAgP 対応のパートナーに接続されたスイッチのポートが auto または desirable モードの場合に、非サイレント動作を行うようにこのポートを設定します。non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネル グループにポートを結合し、このポートが伝送に使用されます。 • active : LACP デバイスが検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • passive : ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 <p>スイッチおよびデバイスのモードの互換性に関する情報については、「PAgP モード」(P.40-5) および「LACP モード」(P.40-6) を参照してください。</p>
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、EtherChannel を設定する例を示します。2 つのポートは、LACP モードが **active** であるチャンネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

EtherChannel ロード バランシングの設定

ここでは、送信元ベースまたは宛先ベースの転送方式を使用することによって、EtherChannel のロード バランシングを設定する手順について説明します。詳細については、「[ロード バランシングおよび転送方式](#)」(P.40-7) を参照してください。

EtherChannel のロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>port-channel load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}</code>	EtherChannel のロード バランシング方式を設定します。 デフォルトは src-mac です。 次のいずれかの負荷分散方式を選択します。 <ul style="list-style-type: none"> • dst-ip : 宛先ホスト IP アドレスに基づいて負荷を分散します。 • dst-mac : 着信パケットの宛先ホスト MAC アドレスに基づいて負荷を分散します。 • src-dst-ip : 送信元および宛先ホスト IP アドレスに基づいて負荷を分散します。 • src-dst-mac : 送信元および宛先ホスト MAC アドレスに基づいて負荷を分散します。 • src-ip : 送信元ホスト IP アドレスに基づいて負荷を分散します。 • src-mac : 着信パケットの送信元 MAC アドレスに基づいて負荷を分散します。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show etherchannel load-balance</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel のロード バランシングをデフォルトの設定に戻すには、**no port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

PAgP 学習方式およびプライオリティの設定

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャンネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカル デバイ스에 手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要があります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホット スタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるように、ポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。



(注)

CLI (コマンドライン インターフェイス) で **physical-port** キーワードを指定した場合でも、スイッチがサポートするのは、集約ポート上でのアドレス ラーニングのみです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドはスイッチ ハードウェアに影響を及ぼしませんが、物理ポートによるアドレス ラーニングだけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

スイッチのリンク パートナーが物理ラーナー (Catalyst 1900 シリーズ スイッチなど) である場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して、IE 3000 スイッチを物理ポート ラーナーとして設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。このように設定すると、送信元アドレスの学習元である EtherChannel 内の同じポートを使用して、パケットが Catalyst 1900 スイッチに送信されます。**pagp learn-method** コマンドは、このような場合のみ使用してください。

スイッチを PAgP 物理ポート ラーナーとして設定し、バンドル内の同じポートがパケット送信元として選択されるようにプライオリティを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ3	<code>pagp learn-method physical-port</code>	PAgP 学習方式を選択します。 デフォルトでは、 aggregation-port learning が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、パケットが送信元に送信されます。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。 ラーナーである別のスイッチに接続するには、 physical-port を選択します。 port-channel load-balance グローバル コンフィギュレーション コマンドは、必ず src-mac に設定してください（「EtherChannel ロード バランシングの設定」(P.40-17) を参照）。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ4	<code>pagp port-priority priority</code>	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 <i>priority</i> に指定できる範囲は 0 ~ 255 です。デフォルトは 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ6	<code>show running-config</code> または <code>show pagp channel-group-number internal</code>	設定を確認します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

プライオリティをデフォルト設定に戻すには、**no pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。学習方式をデフォルト設定に戻すには、**no pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

LACP ホットスタンバイ ポートの設定

イネーブルの場合、LACP はチャンネル内の LACP 互換ポート数を最大に設定しようとします（最大 16 ポート）。同時にアクティブになれる LACP リンクは 8 つだけです。リンクが追加されるとソフトウェアによってホットスタンバイモードになります。アクティブ リンクの 1 つが非アクティブになると、ホットスタンバイモードのリンクが代わりにアクティブになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホットスタンバイポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID (スイッチの MAC アドレス)
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイモードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の (2 つの) 手順を使用します。はじめに、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。詳細については、「LACP システム プライオリティの設定」(P.40-20) および「LACP ポート プライオリティの設定」(P.40-20) を参照してください。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済みの各チャンネルに対しては、システム プライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます (ポートステート フラグが H になっています)。

LACP システム プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lacp system-priority priority	LACP システム プライオリティを設定します。 <i>priority</i> に指定できる範囲は 1 ~ 65535 です。デフォルトは 32768 です。 値が小さいほど、システムプライオリティは高くなります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config または show lacp sys-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LACP システム プライオリティをデフォルトの値に戻すには、**no lacp system-priority** グローバル コンフィギュレーション コマンドを使用します。

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さい値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャンネルでアクティブになります。**show etherchannel summary** 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます (ポートステート フラグが H になっています)。



(注) LACP がすべての互換ポートを集約できない場合（たとえば、ハードウェアの制約が大きいリモートシステム）、EtherChannel 中でアクティブにならないポートはすべてホットスタンバイステートになり、チャンネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>lacp port-priority priority</code>	LACP ポート プライオリティを設定します。 <i>priority</i> に指定できる範囲は 1 ~ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code> または <code>show lacp [channel-group-number] internal</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

LACP ポート プライオリティをデフォルト値に戻すには、`no lacp port-priority` インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel、PAgP、および LACP ステータスの表示

表 40-4 EtherChannel、PAgP、および LACP ステータスを表示するためのコマンド

コマンド	説明
<code>show etherchannel [channel-group-number {detail port port-channel protocol summary}] {detail load-balance port port-channel protocol summary}</code>	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロード バランシング方式またはフレーム配布方式、ポート、ポートチャンネル、プロトコルの情報も表示されます。
<code>show pagp [channel-group-number] {counters internal neighbor}</code>	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
<code>show pagp [channel-group-number] dual-active</code>	デュアルアクティブ検出ステータスが表示されます。
<code>show lacp [channel-group-number] {counters internal neighbor}</code>	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。

PAgP チャンネルグループ情報およびトラフィック カウンタをクリアするには、`clear pagp [channel-group-number counters | counters]` 特権 EXEC コマンドを使用します。

LACP チャンネルグループ情報およびトラフィック カウンタをクリアするには、**clear lacp {channel-group-number counters | counters}** 特権 EXEC コマンドを使用します。

出力内の各フィールドについては、このリリースのコマンド リファレンスを参照してください。

リンクステート トラッキングの概要

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンクステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ NIC アダプタ チューニング機能とともに使用すると、ネットワークで冗長性が実現されます。サーバ ネットワーク アダプタが、チューニングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ インターフェイスでリンクが消失した場合、接続はセカンダリ インターフェイスに透過的に変更されます。



(注)

ポートの集合 (EtherChannel)、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。

図 40-4 (P.40-24) は、リンクステート トラッキングを使用して設定されたネットワークを示しています。リンクステート トラッキングをイネーブルにするには、*link-state group* を作成し、リンクステート グループに割り当てるインターフェイスを指定します。リンクステート グループでは、これらのインターフェイスはまとめてバンドルされます。ダウンストリーム インターフェイスは、アップストリーム インターフェイスにバインドされます。サーバに接続されたインターフェイスはダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチおよびネットワーク 装置に接続されたインターフェイスはアップストリーム インターフェイスと呼ばれます。

図 40-4 の設定により、ネットワーク トラフィック フローのバランスが、次のように保たれます。

- スイッチと他のネットワーク デバイスへのリンクの場合
 - サーバ 1 とサーバ 2 は、プライマリ リンクにスイッチ A を使用し、セカンダリ リンクにスイッチ B を使用しています。
 - サーバ 3 とサーバ 4 は、プライマリ リンクにスイッチ B を使用し、セカンダリ リンクにスイッチ A を使用しています。
- スイッチ A のリンクステート グループ 1
 - スイッチ A はリンクステート グループ 1 を介して、プライマリ リンクをサーバ 1 およびサーバ 2 に使用します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
 - ポート 5 およびポート 6 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。
- スイッチ A のリンクステート グループ 2
 - スイッチ A はリンクステートグループ 2 を介して、セカンダリ リンクをサーバ 3 およびサーバ 4 に使用します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
 - ポート 7 およびポート 8 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。
- スイッチ B のリンクステート グループ 2

- スイッチ B はリンクステートグループ 2 を介して、プライマリ リンクをサーバ 3 およびサーバ 4 に使用します。ポート 3 はサーバ 3 に、ポート 4 はサーバ 4 にそれぞれ接続されます。ポート 3 およびポート 4 はリンクステート グループ 2 でダウンストリーム インターフェイスとして使用します。
- ポート 5 およびポート 6 は、リンクステート グループ 2 を介して分散スイッチ 2 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 2 でアップストリーム インターフェイスとして使用します。
- スイッチ B のリンクステート グループ 1
 - スイッチ B はリンクステート グループ 1 を介して、セカンダリ リンクをサーバ 1 およびサーバ 2 に使用します。ポート 1 はサーバ 1 に、ポート 2 はサーバ 2 にそれぞれ接続されます。ポート 1 およびポート 2 はリンクステート グループ 1 でダウンストリーム インターフェイスとして使用します。
 - ポート 7 およびポート 8 は、リンクステート グループ 1 を介して分散スイッチ 1 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 1 でアップストリーム インターフェイスとして使用します。

分散スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リンクステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。これらは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアップストリーム インターフェイス間の相互作用です。

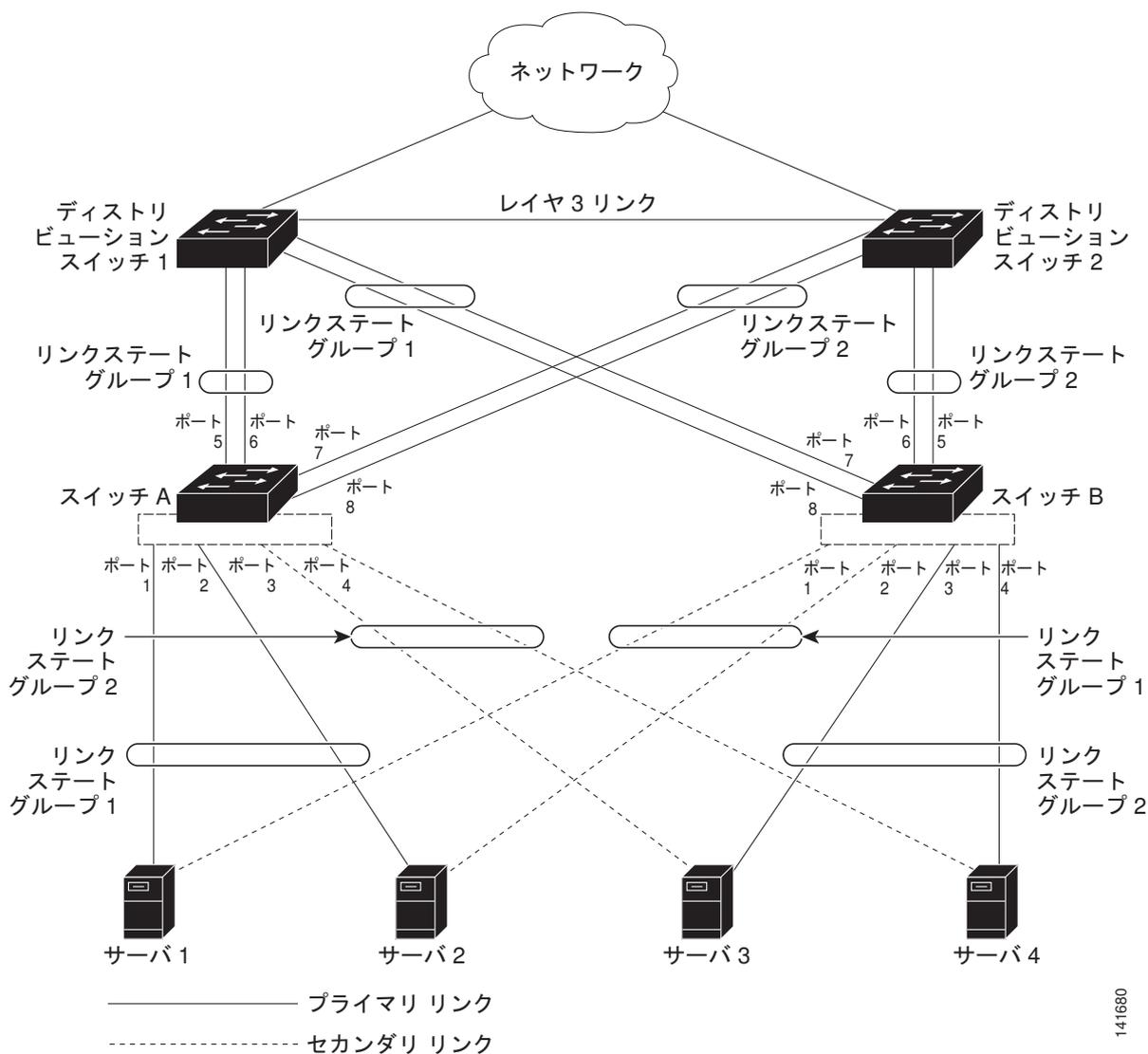
- アップストリーム インターフェイスがリンクアップ ステートの場合、ダウンストリーム インターフェイスをリンクアップ ステートに変更したり、リンクアップ ステートのままにしたりすることができます。
- すべてのアップストリーム インターフェイスが利用不能になった場合、リンクステート トラッキングが自動的にダウンストリーム インターフェイスを `errdisable` ステートにします。サーバ間の接続は、自動的にプライマリ サーバインターフェイスからセカンダリ サーバインターフェイスに変更されます。

スイッチ A のリンクステート グループ 1 からリンクステート グループ 2 への接続の変更例については、[図 40-4 \(P.40-24\)](#) を参照してください。ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンクダウン ステートに変更されます。サーバ 1 およびサーバ 2 の接続については、リンクステート グループ 1 からリンクステート グループ 2 へ変更します。ダウンストリーム ポート 3 およびダウンストリーム ポート 4 は、リンクグループ 2 であるためステートを変更しません。

- リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ステートは変更されないままになります。サーバはこのアップストリーム接続が切断されたことを認識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。複数のダウンストリーム インターフェイスを復旧させるには、リンクステート グループをディセーブルにします。

図 40-4 一般的なリンクステートトラッキングの設定



141680

リンクステートトラッキングの設定

- 「デフォルトのリンクステートトラッキングの設定」 (P.40-25)
- 「リンクステートトラッキングの設定時の注意事項」 (P.40-25)
- 「リンクステートトラッキングの設定」 (P.40-25)
- 「リンクステートトラッキングステータスの表示」 (P.40-26)

デフォルトのリンクステート トラッキングの設定

リンクステート グループは定義されておらず、リンクステート トラッキングはどのグループでもイネーブルではありません。

リンクステート トラッキングの設定時の注意事項

設定上の問題を回避するために、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスを、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義することはできません。その逆も同様です。
- インターフェイスは、複数のリンクステート グループのメンバにはなれません。
- スイッチ 1 つにつき、設定できるリンクステート グループは 2 つだけです。

リンクステート トラッキングの設定

リンクステート グループを設定し、そのグループにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>link state track number</code>	リンクステート グループを作成して、リンクステート トラッキングをイネーブルにします。グループ番号は 1 ~ 2 に設定できます。デフォルトは 1 です。
ステップ 3	<code>interface interface-id</code>	物理インターフェイスまたはインターフェイスの範囲を設定して、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセス モードまたはトランク モード (IEEE 802.1q) のスイッチ ポート、ルーテッド ポート、EtherChannel インターフェイス (スタティックまたは LACP) にバンドルされた、トランク モードの複数ポートが含まれます。
ステップ 4	<code>link state group [number] {upstream downstream}</code>	リンク ステート グループを指定し、そのグループでインターフェイスを upstream または downstream のインターフェイスとして設定します。グループ番号は 1 ~ 2 で、デフォルト値は 1 です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、リンクステート グループを作成してインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range gigabitethernet1/1 -2
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet1/1
```

```
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/2
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

リンクステート グループをディセーブルにするには、**no link state track number** グローバル コンフィギュレーション コマンドを使用します。

リンクステート トラッキング ステータスの表示

show link state group コマンドを使用してリンクステート グループの情報を表示します。キーワードを指定せずにこのコマンドを入力すると、すべてのリンクステート グループの情報が表示されます。特定のグループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、**detail** キーワードを入力します。

次の例では、**show link state group 1** コマンドの出力を示します。

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

次の例では、**show link state group detail** コマンドの出力を示します。

```
Switch> show link state group detail

(Up):Interface up      (Dwn):Interface Down  (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis) Fa1/6(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa1/6(Dwn) Fa1/7(Dwn) Fa1/8(Dwn)
Downstream Interfaces : Fa1/2(Dis) Fa1/3(Dis) Fa1/4(Dis) Fa1/5(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER 41

IP ユニキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP バージョン 4 (IPv4) ユニキャスト ルーティングを設定する方法について説明します。ルーティングをイネーブルにするには、スイッチが IP サービス イメージを実行している必要があります。



(注)

スイッチが IP サービス イメージを実行している場合、IP バージョン 6 (IPv6) ユニキャスト ルーティングもイネーブルにして、IPv4 トラフィックに加えて IPv6 トラフィックを転送するようにインターフェイスを設定できます。スイッチに IPv6 を設定する手順については、[第 42 章「IPv6 ユニキャスト ルーティングの設定」](#)を参照してください。

IP ユニキャスト設定情報の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。この章で使用されるコマンドの構文および使用方法の詳細については、次のコマンド リファレンスを参照してください。これらのマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』

この章で説明する内容は、次のとおりです。

- 「IP ルーティングの概要」 (P.41-2)
- 「ルーティングを設定する手順」 (P.41-3)
- 「IP アドレス指定の設定」 (P.41-4)
- 「IP ユニキャスト ルーティングのイネーブル化」 (P.41-19)
- 「RIP の設定」 (P.41-20)
- 「OSPF の設定」 (P.41-26)
- 「EIGRP の設定」 (P.41-35)
- 「BGP の設定」 (P.41-43)
- 「ISO CLNS ルーティングの設定」 (P.41-65)
- 「Multi-VRF CE の設定」 (P.41-76)

- 「プロトコル独立機能の設定」(P.41-90)
- 「IP ネットワークのモニタリングおよびメンテナンス」(P.41-106)



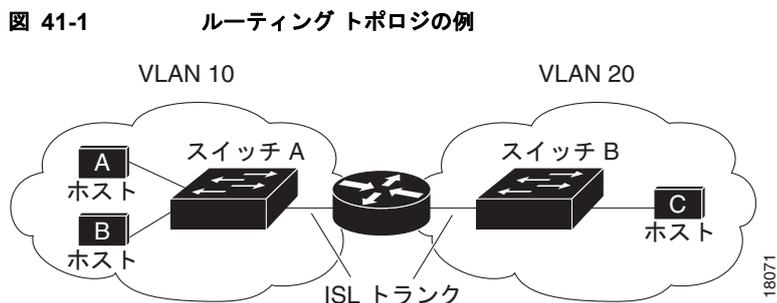
(注)

スイッチにルーティングパラメータを設定する場合、使用できるユニキャストルート数が最大となるようにシステムリソースを割り当てるには、**sdm prefer routing** グローバルコンフィギュレーションコマンドを使用し、ルーティングテンプレートに **Switch Database Management (SDM)** 機能を設定します。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」、またはこのリリースのコマンドリファレンスの **sdm prefer** コマンドを参照してください。

IP ルーティングの概要

一部のネットワーク環境で、VLAN (仮想 LAN) は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャストドメインのサイズを制御し、ローカルトラフィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワークデバイスが相互に通信するには、VLAN 間でトラフィックをルーティング (VLAN 間ルーティング) するレイヤ 3 デバイス (ルータ) が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 41-1 に基本的なルーティングトポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティングテーブルを調べて正しい発信インターフェイスを判別し、VLAN20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ルーティングタイプ

ルータおよびレイヤ 3 スイッチは、次の 3 つの方法でパケットをルーティングできます。

- デフォルトルーティング
- 事前にプログラミングされているトラフィックのスタティックルートの使用
- ルーティングプロトコルによるルートの動的な計算

デフォルト ルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しないため、パケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

ルータでは、トラフィックを転送する最適ルートを動的に計算するため、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには次の 2 つのタイプがあります。

- ディスタンスベクトル プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンスベクトル プロトコルは 1 つまたは複数のメトリックを使用し、最適なルートを計算します。これらのプロトコルは、簡単に設定、使用できます。
- リンクステート プロトコルを使用するルータでは、ルータ間の Link-State Advertisement (LSA; リンクステート アドバタイズメント) の交換に基づき、ネットワーク トポロジに関する複雑なデータベースを保持します。LSA はネットワークのイベントによって起動され、コンバージェンス時間、またはこれらの変更への対応時間を短縮します。リンクステート プロトコルはトポロジの変更にすばやく対応しますが、ディスタンスベクトル プロトコルよりも多くの帯域幅およびリソースが必要になります。

スイッチでサポートされているディスタンスベクトル プロトコルは、RIP およびボーダー ゲートウェイ プロトコル (BGP) です。RIP は最適パスを決定するために単一の距離メトリック (コスト) を使用し、BGP はパス ベクトル メカニズムを追加します。また、Open Shortest Path First (OSPF) リンクステート プロトコル、および従来の Interior Gateway Routing Protocol (IGRP) にリンクステート ルーティング機能の一部を追加して効率化を図った Enhanced IGRP (EIGRP) もサポートされています。

Cisco IOS Release 12.2(58)SE 以降の IP サービス フィーチャ セットでは、前のリリースでサポートされていた OSPFv2 NSF Cisco フォーマットに加えて、OSPFv2 NSF IETF フォーマットもサポートされます。この機能の詳細については、『[NSF—OSPF \(RFC 3623 OSPF Graceful Restart\)](#)』を参照してください。

Cisco IOS Release 12.2(58)SE 以降の IP サービス フィーチャ セットでは、EIGRP Cisco NSF ルーティングがサポートされています。それにより、コンバージェンスの時間が短くなり、スタック マスター 変更後のトラフィック損失がなくなります。この NSF 機能の詳細については、『[Configuring Nonstop Forwarding](#)』のガイドを参照してください。

ルーティングを設定する手順

スイッチ上で、IP ルーティングはデフォルトでディセーブルとなっているため、ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。IP ルーティング設定情報の詳細については、『[Cisco IOS IP Configuration Guide, Release 12.2](#)』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

- ルーテッド ポート : **no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポートです。
- スイッチ仮想インターフェイス (SVI) : **interface vlan vlan_id** グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。

- レイヤ 3 モードの EtherChannel ポート チャンネル: `interface port-channel port-channel-number` グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャンネルグループにバインドして作成されたポートチャンネル論理インターフェイス。詳細については、「[レイヤ 3 EtherChannel の設定](#)」(P.40-14) を参照してください。



(注)

スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「[ネットワーク インターフェイスへの IP アドレスの割り当て](#)」(P.41-5) を参照してください。



(注)

スイッチは、各ルーテッド ポートおよび SVI に割り当てられた IP アドレスを持つことができます。ソフトウェアに、設定できるルーテッド ポートおよび SVI の個数制限はありません。ただし、ハードウェアによって制限されるため、この数と実装されている機能の数および量との相互関係によって、CPU 利用率が影響を受けることがあります。システム メモリをルーティング用に最適化するには、`sdm prefer routing` グローバル コンフィギュレーション コマンドを使用します。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバーシップを割り当てます。詳細については、[第 16 章「VLAN の設定」](#) を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルに設定します。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します (任意)。

IP アドレス指定の設定

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。ここでは、さまざまな IP アドレス指定機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- 「[アドレス指定のデフォルト設定](#)」(P.41-4)
- 「[ネットワーク インターフェイスへの IP アドレスの割り当て](#)」(P.41-5)
- 「[アドレス解決方法の設定](#)」(P.41-8)
- 「[IP ルーティングがディセーブルの場合のルーティング支援機能](#)」(P.41-11)
- 「[ブロードキャスト パケットの処理方法の設定](#)」(P.41-14)
- 「[IP アドレスのモニタリングおよびメンテナンス](#)」(P.41-18)

アドレス指定のデフォルト設定

表 41-1 に、アドレス指定のデフォルト設定を示します。

表 41-1 アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義
ARP	ARP キャッシュに永続的なエントリはありません カプセル化：標準イーサネット形式の ARP 14400 秒（4 時間）
IP ブロードキャスト アドレス	255.255.255.255（すべて 1）
IP クラスレス ルーティング	イネーブル
IP デフォルト ゲートウェイ	ディセーブル
IP ダイレクト ブロードキャスト	ディセーブル（すべての IP ダイレクト ブロードキャストがドロップされます）
IP ドメイン	ドメイン リスト：ドメイン名は未定義 ドメイン検索：イネーブル ドメイン名：イネーブル
IP 転送プロトコル	ヘルパー アドレスが定義されているか、またはユーザ データグラム プロトコル（UDP）フラッディングが設定されている場合、デフォルトポートでは UDP 転送がイネーブルとなります ローカル ブロードキャスト：ディセーブル スパンニングツリー プロトコル（STP）：ディセーブル ターボフラッディング：ディセーブル
IP ヘルパー アドレス	ディセーブル
IP ホスト	ディセーブル
ICMP Router Discovery Protocol（IRDP）	ディセーブル イネーブルの場合のデフォルト： <ul style="list-style-type: none"> ブロードキャスト IRDP アドバタイズメント アドバタイズメント間の最大インターバル：600 秒 アドバタイズメント間の最小インターバル：最大インターバルの 0.75 倍 プリファレンス：0
IP プロキシ ARP	イネーブル
IP ルーティング	ディセーブル
IP サブネットゼロ	ディセーブル

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166『Internet Numbers』には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1つのプライマリ IP アドレスを設定できます。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネットマスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

IP アドレスおよびネットワーク マスクをレイヤ 3 インターフェイスに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	ip address ip-address subnet-mask	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 5	no shutdown	インターフェイスをイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [interface-id] show ip interface [interface-id] show running-config interface [interface-id]	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LAN ベース イメージを実行しているスイッチでは、SVI のみに IP アドレスを割り当てることができ、その後 SVI のスタティック ルートを設定します。スイッチは、16 のユーザ設定のスタティック ルートをサポートします。「[スタティック ユニキャスト ルートの設定](#)」(P.41-92) を参照してください。他のルーティング設定はサポートされません。

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなります。

すべてが 1 のサブネット (131.108.255.0) は使用可能です。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます（ただし推奨できません）。

サブネット ゼロをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip subnet-zero	インターフェイス アドレスおよびルーティングのアップデート時にサブネット ゼロの使用をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

クラスレス ルーティング

ルーティングを行うように設定されたスイッチで、クラスレス ルーティング動作はデフォルトでイネーブルとなっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛てにパケットをルータが受信すると、ルータは最適なスーパーネット ルートにパケットを転送します。スーパーネットは、単一の大規模アドレス空間をシミュレートするために使用されるクラス C アドレス空間の連続ブロックで構成されています。スーパーネットは、クラス B アドレス空間の急速な枯渇を回避するために設計されました。

図 41-2 では、クラスレス ルーティングがイネーブルとなっています。ホストがパケットを 120.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛てにパケットを受信したルータは、パケットを廃棄します。

図 41-2 IP クラスレス ルーティングがイネーブルの場合

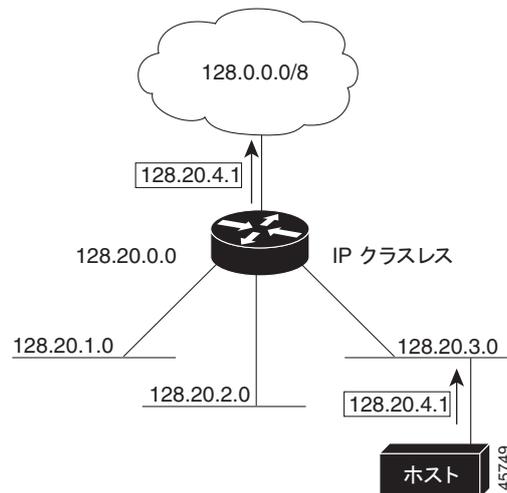
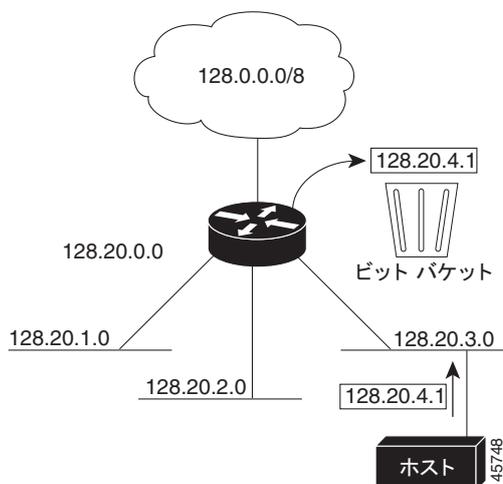


図 41-3 では、ネットワーク 128.20.0.0 のルータはサブネット 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ホストがパケットを 120.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 41-3 IP クラスレスルーティングがディセーブルの場合



認識されないサブネット宛てのパケットが最適なスーパーネット ルートに転送されないようにするには、クラスレスルーティング動作をディセーブルにします。

クラスレスルーティングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	no ip classless	クラスレスルーティング動作をディセーブルにします。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して、デフォルト ルートがないネットワークのサブネット宛てパケットが最適なスーパーネット ルートに転送されるようにするには、**ip classless** グローバル コンフィギュレーション コマンドを使用します。

アドレス解決方法の設定

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレス (MAC アドレス) と、デバイスが属するネットワークを特定するネットワーク アドレスがあります。

ローカルアドレス (MAC アドレス) は、パケット ヘッダーのデータ リンク層 (レイヤ 2) セクションに格納されて、データ リンク (レイヤ 2) デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、「アドレス解決」と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、「逆アドレス解決」と呼びます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- ARP : IP アドレスを MAC アドレスと関連付けるために使用されます。ARP は IP アドレスを入力と解釈し、対応する MAC アドレスを学習します。次に、IP アドレス/MAC アドレス アソシエーションを ARP キャッシュにストアし、すぐに取り出せるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) で規定されています。
- プロキシ ARP : ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ (ルータ) が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能 (ローカル MAC アドレスでなく IP アドレスを要求する点を除く) を持つ Reverse Address Resolution Protocol (RARP) を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、`ip rarp-server address` インターフェイス コンフィギュレーション コマンドを使用します。

RARP の詳細については、『Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2』を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

アドレス解決を設定するために必要な作業は次のとおりです。

- 「[スタティック ARP キャッシュの定義](#)」 (P.41-9)
- 「[ARP カプセル化の設定](#)」 (P.41-10)
- 「[プロキシ ARP のイネーブル化](#)」 (P.41-11)

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間を動的にマッピングできます。ほとんどのホストでは動的 アドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するために使用される永続的なエントリを、ARP キャッシュに確保できます。また、指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

IP アドレスと MAC アドレスの間でスタティック マッピングを行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	arp ip-address hardware-address type	ARP キャッシュ内で IP アドレスを MAC (ハードウェア) アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。 <ul style="list-style-type: none"> • arpa : ARP カプセル化 (イーサネット インターフェイス用) • snap : SNAP カプセル化 (トークン リングおよび FDDI インターフェイス用) • sap : HP の ARP タイプ
ステップ 3	arp ip-address hardware-address type [alias]	(任意) 指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 4	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 5	arp timeout seconds	(任意) ARP キャッシュ エントリがキャッシュに保持される期間を設定します。デフォルト値は 14400 秒 (4 時間) です。指定できる範囲は 0 ~ 2147483 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [interface-id]	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 8	show arp または show ip arp	ARP キャッシュの内容を表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ARP キャッシュからエントリを削除するには、**no arp ip-address hardware-address type** グローバル コンフィギュレーション コマンドを使用します。ARP キャッシュから非スタティック エントリをすべて削除するには、**clear arp-cache** 特権 EXEC コマンドを使用します。

ARP カプセル化の設定

IP インターフェイスでは、イーサネット ARP 形式の ARP カプセル化 (**arpa** キーワードで表される) がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

ARP カプセル化タイプを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	arp {arpa snap}	ARP カプセル化方法を指定します。 <ul style="list-style-type: none"> • arpa : ARP • snap : SNAP

	コマンド	目的
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show interfaces [<i>interface-id</i>]	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

プロキシ ARP のイネーブル化

デフォルトでは、プロキシ ARP が使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

ディセーブルになっているプロキシ ARP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface <i>interface-id</i>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ3	ip proxy-arp	インターフェイスでプロキシ ARP をイネーブルにします。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show ip interface [<i>interface-id</i>]	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスでプロキシ ARP をディセーブルにするには、**no ip proxy-arp** インターフェイス コンフィギュレーション コマンドを使用します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを学習できます。

- 「プロキシ ARP」 (P.41-11)
- 「デフォルト ゲートウェイ」 (P.41-12)
- 「IRDP」 (P.41-12)

プロキシ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカルイーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを調

べます。最適なルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

プロキシ ARP は、デフォルトでイネーブルに設定されています。ディセーブル化されたプロキシ ARP をイネーブルにするには、「[プロキシ ARP のイネーブル化](#)」(P.41-11) を参照してください。プロキシ ARP は、他のルータでサポートされているかぎり有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) リダイレクト メッセージを返信するという方法で、ホストが使用するローカル ルータを定義します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

IP ルーティングがディセーブルの場合にデフォルト ゲートウェイ (ルータ) を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip default-gateway ip-address</code>	デフォルト ゲートウェイ (ルータ) を設定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip redirects</code>	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、`no ip default-gateway` グローバル コンフィギュレーション コマンドを使用します。

IRDP

ルータ ディスカバリを使用すると、スイッチは IRDP を使用し、他のネットワークへのルートを動的に学習します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。スイッチは Routing Information Protocol (RIP; ルーティング情報プロトコル) ルーティングのアップデートを受信し、この情報を使用してルータの場所を推測することもできます。実際のところ、ルーティング デバイスによって送信されたルーティング テーブルは、スイッチにストアされません。どのシステムがデータを送信しているのかが記録されるだけです。IRDP を使用する利点は、プライオリティと、パケットを受信されなくなってからデバイスがダウンしていると思なされるまでの期間の両方をルータごとに指定できることです。

検出された各デバイスは、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

インターフェイスで IRDP ルーティングを行う場合は、インターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータを変更することもできます。

インターフェイス上で IRDP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip irdp	インターフェイス上で IRDP 処理をイネーブルにします。
ステップ 4	ip irdp multicast	(任意) IP ブロードキャストの代わりに、マルチキャスト アドレス (224.0.0.1) に IRDP アドバタイズを送信します。 (注) このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 5	ip irdp holdtime seconds	(任意) アドバタイズが有効である IRDP 期間を設定します。デフォルト値は maxadvertinterval 値の 3 倍です。 maxadvertinterval 値よりも大きな値 (9000 秒以下) を指定する必要があります。 maxadvertinterval 値を変更すると、この値も変更されます。
ステップ 6	ip irdp maxadvertinterval seconds	(任意) アドバタイズ間の IRDP の最大インターバルを設定します。デフォルト値は 600 秒です。
ステップ 7	ip irdp minadvertinterval seconds	(任意) アドバタイズ間の IRDP の最小インターバルを設定します。デフォルト値は maxadvertinterval 値の 0.75 倍です。 maxadvertinterval を変更すると、この値も新しいデフォルト値 (maxadvertinterval の 0.75 倍) に変更されます。
ステップ 8	ip irdp preference number	(任意) デバイスの IRDP プリファレンス レベルを設定します。指定できる範囲は -2^{31} ~ 2^{31} です。デフォルトは 0 です。大きな値を設定すると、ルータのプリファレンス レベルも高くなります。
ステップ 9	ip irdp address address [number]	(任意) プロキシアドバタイズを行うために必要な IRDP アドレスとプリファレンスを指定します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show ip irdp	IRDP 値を表示し、設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

maxadvertinterval 値を変更すると、**holdtime** 値および **minadvertinterval** 値も変更されます。最初に **maxadvertinterval** 値を変更し、次に **holdtime** 値または **minadvertinterval** 値のいずれかを手動で変更することが重要です。

IRDP ルーティングをディセーブルにするには、**no ip irdp** インターフェイス コンフィギュレーション コマンドを使用します。

ブロードキャスト パケットの処理方法の設定

IP インターフェイス アドレスを設定したあとで、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛てのデータ パケットです。2 種類のブロードキャストがサポートされています。

- **ダイレクトブロードキャストパケット**：特定のネットワークまたは一連のネットワークに送信されます。ダイレクトブロードキャストアドレスには、ネットワークまたはサブネットフィールドが含まれます。
- **フラディングブロードキャストパケット**：すべてのネットワークに送信されます。



(注)

storm-control インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャストトラフィックを制限することもできます。詳細については、[第 29 章「ポート単位のトラフィック制御の設定」](#)を参照してください。

ルータはローカル ケーブルまでの範囲を制限して、ブロードキャスト ストームを防ぎます。ブリッジ (インテリジェントなブリッジを含む) はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームを伝播します。ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャストアドレスとして使用するように設定できます。スイッチをはじめ、多数の実装機能では、ブロードキャストメッセージを転送するためのアドレス方式が複数サポートされています。

これらの方式をイネーブルにするには、次に示す作業を実行します。

- 「[ダイレクトブロードキャストから物理ブロードキャストへの変換のイネーブル化](#)」 (P.41-14)
- 「[UDP ブロードキャスト パケットおよびプロトコルの転送](#)」 (P.41-15)
- 「[IP ブロードキャスト アドレスの確立](#)」 (P.41-16)
- 「[IP ブロードキャストのフラディング](#)」 (P.41-17)

ダイレクトブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP ダイレクトブロードキャストがドロップされるため、転送されることはありません。IP ダイレクトブロードキャストがドロップされると、ルータが DoS 攻撃 (サービス拒絶攻撃) にさらされる危険が少なくなります。

ブロードキャストが物理 (MAC レイヤ) ブロードキャストになるインターフェイスでは、IP ダイレクトブロードキャストの転送をイネーブルにできます。 **ip forward-protocol** グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが、ダイレクトブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、[第 38 章「ACL によるネットワークセキュリティの設定」](#)を参照してください。

インターフェイス上で IP ダイレクトブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ3	ip directed-broadcast [access-list-number]	インターフェイス上で、ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御するアクセスリストを指定できます。アクセスリストを指定すると、アクセスリストで許可されている IP パケットだけが変換可能になります。 (注) ip directed-broadcast インターフェイス コンフィギュレーション コマンドは VPN Routing/Forwarding (VRF; VPN ルーティング/転送) インターフェイスで設定でき、こうすると VRF 認識になります。ダイレクトブロードキャストトラフィックが VRF 内でだけルーティングされます。
ステップ4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ5	ip forward-protocol {udp [port] nd sdns}	ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。 <ul style="list-style-type: none"> • udp : UDP データグラムを転送します。 <i>port</i> : (任意) 転送される UDP サービスを制御する宛先ポートです。 • nd : ND データグラムを転送します。 • sdns : SDNS データグラムを転送します。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show ip interface [interface-id] または show running-config	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ダイレクトブロードキャストから物理ブロードキャストへの変換をディセーブルにするには、**no ip directed-broadcast** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

UDP ブロードキャスト パケットおよびプロトコルの転送

UDP は IP のホスト間レイヤ プロトコルで、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレスのセッションを 2 つのエンドシステム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、名前に関する情報を検索します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、通常 UDP ブロードキャストは転送されません。この状況を改善するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk (ND) プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と ND の両方の転送がイネーブルになっています。『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2』の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP フォワーディング エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol (DHCP) 情報を伝達します。

インターフェイスで UDP ブロードキャスト パケットの転送をイネーブルにし、宛先アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip helper-address address	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ip forward-protocol {udp [port] nd sdns}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip interface [interface-id] または show running-config	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定アドレスへのブロードキャスト パケットの転送をディセーブルにするには、**no ip helper-address** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

IP ブロードキャスト アドレスの確立

最も一般的な (デフォルトの) IP ブロードキャスト アドレスは、すべて 1 で構成されているアドレス (255.255.255.255) です。ただし、任意の形式の IP ブロードキャスト アドレスを生成するようにスイッチを設定することもできます。

インターフェイス上で IP ブロードキャスト アドレスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	ip broadcast-address ip-address	デフォルト値と異なるブロードキャスト アドレス (128.1.255.255 など) を入力します。
ステップ 4	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ5	<code>show ip interface [interface-id]</code>	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャスト アドレスを確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの IP ブロードキャスト アドレスに戻すには、**no ip broadcast-address** インターフェイス コンフィギュレーション コマンドを使用します。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IP ヘルパー アドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットを、フラッディングできます。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されます。

フラッディングを行う場合、パケットは次の条件を満たす必要があります (これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです)。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。
- パケットは Trivial File Transfer Protocol (TFTP)、ドメイン ネーム システム (DNS)、Time、NetBIOS、ND、または BOOTP パケット、または **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの Time To Live (TTL; 存続可能時間) 値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスを設定します。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内に伝播されるにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされた UDP データグラムがインターフェイスから送信されると (場合によっては宛先アドレスが変更される)、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

ブリッジング スパニングツリー データベースを使用し、UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip forward-protocol spanning-tree</code>	ブリッジング スパニングツリー データベースを使用し、UDP データグラムをフラッディングします。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。

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

IP ブロードキャストのフラッドディンクをディセーブルにするには、**no ip forward-protocol spanning-tree** グローバル コンフィギュレーション コマンドを使用します。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッドディンクを使用し、スパニングツリーベースの UDP フラッドディンクを約 4 ~ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

スパニングツリーベースのフラッドディンクを高速化するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip forward-protocol turbo-flood	スパニングツリー データベースを使用し、UDP データグラムのフラッドディンクを高速化します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip forward-protocol turbo-flood** グローバル コンフィギュレーション コマンドを使用します。

IP アドレスのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になっている場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を削除できます。表 41-2 に、内容をクリアするために使用するコマンドを示します。

表 41-2 キャッシュ、テーブル、データベースをクリアするコマンド

コマンド	目的
clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュをクリアします。
clear host {name *}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {network [mask] *}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティング パスなど、特定の統計情報を表示できます。表 41-3 に、IP を消去および表示するために使用する特権 EXEC コマンドを示します。

表 41-3 キャッシュ、テーブル、データベースを表示するコマンド

コマンド	目的
show arp	ARP テーブルのエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します (エイリアス)。
show ip arp	IP ARP キャッシュを表示します。
show ip interface [interface-id]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDP 値を表示します。
show ip masks address	ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [address [mask]] [protocol]	ルーティング テーブルの現在のステートを表示します。
show ip route summary	ルーティング テーブルの現在のステートをサマリー形式で表示します。

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スイッチング モード、IP ルーティングはディセーブルとなっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

IP ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティングをイネーブルにします
ステップ 3	router ip_routing_protocol	(注) IP ルーティング プロトコルを指定します。このステップでは、他のコマンドを実行することもできます。たとえば、 network (RIP) ルータ コンフィギュレーション コマンドを使用し、ルーティングするネットワークを指定できます。特定のプロトコルの詳細については、この章の後半および『Cisco IOS IP Configuration Guide, Release 12.2』を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング プロトコルとして RIP を使用し、IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
```

```
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

ここで、選択したルーティングプロトコルのパラメータを設定できます。具体的な手順は次のとおりです。

- 「RIP の設定」 (P.41-20)
- 「OSPF の設定」 (P.41-26)
- 「EIGRP の設定」 (P.41-35)
- 「BGP の設定」 (P.41-43)
- 「プロトコル独立機能の設定」 (P.41-90) (任意)

RIP の設定

RIP は、小規模な同種ネットワーク間で使用するために作成された Interior Gateway Protocol (IGP) です。RIP は、ブロードキャスト UDP データパケットを使用してルーティング情報を交換するディスタンスベクトルルーティングプロトコルです。このプロトコルは RFC 1058 に文書化されています。RIP の詳細については、『*IP Routing Fundamentals*』(Cisco Press 刊)を参照してください。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート (アドバタイズメント) を送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマークされます。240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティングテーブルエントリをすべて削除します。

RIP では、各ルートの値を評価するためにホップカウントが使用されます。ホップカウントは、ルート内で経由されるルータ数です。直接接続されているネットワークのホップカウントは 0 です。ホップカウントが 16 のネットワークに到達できません。このように範囲 (0 ~ 15) が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワークパスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルトネットワークが RIP によって取得された場合、またはルータが最終ゲートウェイで、RIP がデフォルトメトリックによって設定されている場合、スイッチはデフォルトネットワークをアドバタイズします。RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しないと、RIP アップデート中にアドバタイズされません。

ここでは、次の設定について説明します。

- 「RIP のデフォルト設定」 (P.41-20)
- 「基本的な RIP パラメータの設定」 (P.41-21)
- 「RIP 認証の設定」 (P.41-23)
- 「サマリーアドレスおよびスプリットホライズンの設定」 (P.41-24)

RIP のデフォルト設定

表 41-4 に、RIP のデフォルト設定を示します。

表 41-4 RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報送信元	ディセーブル
デフォルト メトリック	自動メトリック変換 (組み込み)
IP RIP 認証キーチェーン	認証なし 認証モード: クリア テキスト
IP RIP 受信バージョン	version ルータ コンフィギュレーション コマンドに準拠
IP RIP 送信バージョン	version ルータ コンフィギュレーション コマンドに準拠
IP RIP の起動	version ルータ コンフィギュレーション コマンドに準拠
IP スプリット ホライズン	メディアにより異なる
ネイバー	未定義
ネットワーク	指定なし
オフセット リスト	ディセーブル
出力遅延	0 ミリ秒
タイマー基準	<ul style="list-style-type: none"> • 更新: 30 秒 • 無効: 180 秒 • ホールドダウン: 180 秒 • フラッシュ: 240 秒
アップデート送信元の検証	イネーブル
バージョン	RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。IE 3000 スイッチでは、ネットワーク番号を設定するまで RIP コンフィギュレーション コマンドは無視されます。

RIP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip routing	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合だけ、必須です)。
ステップ3	router rip	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	network <i>network number</i>	ネットワークを RIP ルーティング プロセスに関連付けます。複数の network コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合だけ可能です。 (注) RIP コマンドを有効にするためにネットワーク番号を設定する必要があります。
ステップ 5	neighbor <i>ip-address</i>	(任意) ルーティング情報を交換する隣接ルータを定義します。このステップを使用すると、RIP (通常はブロードキャスト プロトコル) からのルーティングアップデートが非ブロードキャスト ネットワークに到達するようになります。
ステップ 6	offset list [<i>access-list number</i> <i>name</i>] { in out } <i>offset</i> [<i>type number</i>]	(任意) オフセット リストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 7	timers basic <i>update invalid holddown flush</i>	(任意) ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ~ 4294967295 秒です。 <ul style="list-style-type: none"> • <i>update</i> : ルーティング アップデートの送信間隔。デフォルトは 30 秒です。 • <i>invalid</i> : ルートが無効と宣言されたあとの時間。デフォルト値は 180 秒です。 • <i>holddown</i> : ルートがルーティング テーブルから削除されるまでの時間。デフォルト値は 180 秒です。 • <i>flush</i> : ルーティング アップデートが延期される時間。デフォルトは 240 秒です。
ステップ 8	version { 1 2 }	(任意) RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトの場合、スイッチではバージョン 1 および 2 を受信しますが、バージョン 1 だけを送信します。 インターフェイス コマンド ip rip {send receive} version 1 2 1 2 を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 9	no auto summary	(任意) 自動サマライズをディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィックスがサマライズされます。サマライズをディセーブルにし (RIP バージョン 2 だけ)、クラスフル ネットワーク境界にサブネットおよびホストルーティング情報をアドバタイズします。
ステップ 10	no validate-update-source	(任意) 着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の場合で使用する場合は、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 11	output-delay <i>delay</i>	(任意) 送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなる RIP アップデートのパケットに、パケット間遅延が追加されません。パケットを低速なデバイスに送信する場合は、8 ~ 50 ミリ秒のパケット間遅延を追加できます。

	コマンド	目的
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ip protocols	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをオフにするには、**no router rip** グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと現在のステータスを表示するには、**show ip protocols** 特権 EXEC コマンドを使用します。RIP データベースのサマリー アドレス エントリを表示するには、**show ip rip database** 特権 EXEC コマンドを使用します。

RIP 認証の設定

RIP バージョン 1 では、認証がサポートされていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連のキーは、キー チェーンによって決まります。キー チェーンが設定されていないと、デフォルトの場合でも認証は実行されません。「[認証キーの管理](#)」(P.41-105) に記載されている作業も実行してください。

RIP 認証がイネーブルであるインターフェイスでは、プレーン テキストと MD5 という 2 つの認証モードがサポートされています。デフォルトはプレーン テキストです。

インターフェイスに RIP 認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	ip rip authentication key-chain name-of-chain	RIP 認証をイネーブルにします。
ステップ 4	ip rip authentication mode [text md5]	プレーン テキスト認証 (デフォルト) または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface [interface-id]	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を禁止するには、**no ip rip authentication key-chain** インターフェイス コンフィギュレーション コマンドを使用します。

サマリー アドレスおよびスプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。



(注) ルートを適切にアドバタイズするため、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常はこの機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカル IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。



(注) スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

サマライズされたローカル IP アドレスをアドバタイズし、インターフェイスのスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip address ip-address subnet-mask	IP アドレスおよび IP サブネットを設定します。
ステップ 4	ip summary-address rip ip address ip-network mask	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。
ステップ 5	no ip split horizon	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip interface interface-id	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP サマライズをディセーブルにするには、**no ip summary-address rip** ルータ コンフィギュレーション コマンドを使用します。

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスがまだレイヤ 2 モード（デフォルト）の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。



(注) スプリット ホライズンがイネーブルである場合、(**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される) 自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンスベクトル ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報の発信元であるインターフェイス上の、ルータによって、その情報がアドバタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます (特にリンクが壊れている場合)。



(注) ルートを適切にアドバタイズするために、アプリケーションがスプリット ホライズンをディセーブルにする必要がある場合を除き、通常この機能をディセーブルにしないでください。

インターフェイスでスプリット ホライズンをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ3	ip address ip-address subnet-mask	IP アドレスおよび IP サブネットを設定します。
ステップ4	no ip split-horizon	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show ip interface interface-id	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スプリット ホライズン メカニズムをイネーブルにするには、**ip split-horizon** インターフェイス コンフィギュレーション コマンドを使用します。

OSPF の設定

ここでは、OSPF の設定方法について簡単に説明します。OSPF コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』の「OSPF Commands」を参照してください。



(注)

OSPF では、各メディアがブロードキャスト ネットワーク、非ブロードキャスト ネットワーク、ポイントツーポイント ネットワークに分類されます。スイッチでは、ブロードキャスト ネットワーク（イーサネット、トークンリング、FDDI）およびポイントツーポイント ネットワーク（ポイントツーポイント リンクとして設定されたイーサネット インターフェイス）がサポートされます。

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。シスコの実装では、RFC1253 の OSPF Management Information Base (MIB; 管理情報ベース) がサポートされています。

シスコの実装は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって取得したルートを取り込むことができます。OSPF ルートを RIP に伝達することもできます。
- エリア内の隣接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータのデッドインターバルと hello インターバル、認証キーなどがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area (NSSA) がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された *Area Border Router* (ABR; エリア境界ルータ)、および *Autonomous System Boundary Router* (ASBR; 自律システム境界ルータ) 間で調整する必要があります。最小設定では、すべてのデフォルト パラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

ここでは、次の設定について説明します。

- 「OSPF のデフォルト設定」(P.41-27)
- 「基本的な OSPF パラメータの設定」(P.41-28)
- 「OSPF インターフェイスの設定」(P.41-29)
- 「OSPF エリア パラメータの設定」(P.41-31)
- 「その他の OSPF パラメータの設定」(P.41-32)
- 「LSA グループ ページングの変更」(P.41-34)
- 「ループバック インターフェイスの設定」(P.41-34)
- 「OSPF のモニタリング」(P.41-35)

OSPF のデフォルト設定

表 41-5 に、OSPF のデフォルト設定を示します。

表 41-5 OSPF のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：デフォルト コストは未定義 再送信インターバル：5 秒 送信遅延：1 秒 プライオリティ：1 hello インターバル：10 秒 デッド インターバル：hello インターバルの 4 倍 認証なし パスワードの指定なし MD5 認証はディセーブル
エリア	認証タイプ：0（認証なし） デフォルト コスト：1 範囲：ディセーブル スタブ：スタブ エリアは未定義 NSSA：NSSA エリアは未定義
自動コスト	100 Mb/s
デフォルト情報送信元	ディセーブル イネーブルの場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルトはタイプ 2 です。
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換
距離 OSPF	dist1（エリア内のすべてのルート）：110 dist2（エリア間のすべてのルート）：110 および dist3（他のルーティング ドメインからのルート）：110
OSPF データベース フィルタ	ディセーブル すべての発信 LSA がインターフェイスにフラッディングされます。
IP OSPF 名検索	ディセーブル
隣接関係変更ログ	イネーブル
ネイバー	指定なし
ネイバー データベース フィルタ	ディセーブル すべての発信 LSA はネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル
NSF ¹ 認識	イネーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
ルータ ID	OSPF ルーティング プロセスは未定義

表 41-5 OSPF のデフォルト設定 (続き)

機能	デフォルト設定
サマリー アドレス	ディセーブル
タイマー LSA グループのペーシング	240 秒
タイマー Shortest Path First (SPF)	spf delay : 5 秒。 spf-holdtime : 10 秒。
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル : 10 秒 再送信インターバル : 5 秒 送信遅延 : 1 秒 デッド インターバル : 40 秒 認証キー : キーは未定義 メッセージダイジェスト キー (MD5) : キーは未定義

1. NSF = Nonstop Forwarding

OSPF NSF 認識

IP サービス イメージは IPv4 の OSPF NSF 認識をサポートしています。隣接ルータが NSF 対応で、レイヤ 3 スイッチでは、プライマリ RP に障害が発生してルータのバックアップ RP によって引き継がれる前に、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide, Release 12.2*』を参照してください。

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに関連付ける IP アドレスの範囲を指定して、この範囲に関連付けるエリア ID を割り当てる必要があります。Cisco IOS Release 12.2(58)SE 以降、IP サービス イメージを実行しているスイッチでは、Cisco OSPFv2 NSF フォーマットと IETF OSPFv2 NSF フォーマットのいずれかを設定できます。

OSPF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられ、内部で使用される識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。

コマンド	目的
ステップ3 nsf cisco [enforce global] または nsf ietf [restart-interval seconds]	(任意) OSPF での Cisco NSF 動作をイネーブルにします。 enforce global キーワードを指定すると、非 NSF 認識のネイバー ネットワーキング デバイスが検出されたときに NSF 再起動がキャンセルされます。 (任意) OSPF での IETF NSF 動作をイネーブルにします。 restart-interval キーワードでは、グレースフル リスタート間隔の長さを秒単位で指定します。指定できる範囲は 1 ~ 1800 です。デフォルトは 120 です。
ステップ4 network address wildcard-mask area area-id	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。単一のコマンドにワイルドカード マスクを指定し、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進数または IP アドレスを指定できます。
ステップ5 end	特権 EXEC モードに戻ります。
ステップ6 show ip protocols	設定を確認します。
ステップ7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスを終了するには、**no router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ (**hello** インターバル、**デッド** インターバル、**認証キー**など) については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。



(注) **ip ospf** インターフェイス コンフィギュレーション コマンドはすべてオプションです。

OSPF インターフェイス パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ3 ip ospf cost	(任意) インターフェイスでパケットを送信するコストを明示的に指定します。

	コマンド	目的
ステップ 4	<code>ip ospf retransmit-interval seconds</code>	(任意) LSA 送信間隔を秒数で指定します。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は 5 秒です。
ステップ 5	<code>ip ospf transmit-delay seconds</code>	(任意) リンク ステート アップデート パケットを送信するまでの予測待ち時間を秒数で設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルトは 1 秒です。
ステップ 6	<code>ip ospf priority number</code>	(任意) ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。有効な範囲は 0 ~ 255 です。デフォルトは 1 です。
ステップ 7	<code>ip ospf hello-interval seconds</code>	(任意) OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ~ 65535 秒です。デフォルトは 10 秒です。
ステップ 8	<code>ip ospf dead-interval seconds</code>	(任意) 最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。ネットワークのすべてのノードで同じ値を指定する必要があります。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。
ステップ 9	<code>ip ospf authentication-key key</code>	(任意) 隣接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列 (最大 8 バイト長) を指定できます。同じネットワーク上のすべての隣接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。
ステップ 10	<code>ip ospf message-digest-key keyid md5 key</code>	(任意) MDS 認証をイネーブルにします。 <ul style="list-style-type: none"> • <i>keyid</i> : 1 ~ 255 の ID • <i>key</i> : 最大 16 バイトの英数字パスワード
ステップ 11	<code>ip ospf database-filter all out</code>	(任意) インターフェイスへの OSPF LSA パケットのフラッドイングを阻止します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip ospf interface [interface-name]</code>	OSPF に関連するインターフェイス情報を表示します。
ステップ 14	<code>show ip ospf neighbor detail</code>	ネイバー スイッチの NSF 認証ステータスを表示します。出力には、次のいずれかが表示されます。 <ul style="list-style-type: none"> • <i>Options is 0x52</i> <i>LLS Options is 0x1 (LR)</i> これらの行の両方が表示される場合、ネイバー スイッチが NSF 認識です。 • <i>Options is 0x42</i> : ネイバー スイッチが NSF 認識でないことを示します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

OSPF エリア パラメータの設定

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および NSSA への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。スタブエリアに外部ルートに関する情報は送信されませんが、代わりに、自律システム (AS) 外の宛先に対するデフォルトの外部ルートが、エリア境界ルータ (ABR) によって生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッドングされませんが、再配信することによって、エリア内の AS 外部ルートをインポートできます。

経路集約は、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリー ルートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリー ルートをアドバタイズするように ABR を設定できます。



(注) OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

エリア パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	area area-id authentication	(任意) 特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	area area-id authentication message-digest	(任意) エリアに関して MD5 認証をイネーブルにします。
ステップ 5	area area-id stub [no-summary]	(任意) エリアをスタブ エリアとして定義します。 no-summary キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブ エリアに送信できなくなります。
ステップ 6	area area-id nssa [no-redistribution] [default-information-originate] [no-summary]	(任意) エリアを NSSA として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 <ul style="list-style-type: none"> no-redistribution : ルータが NSSA ABR の場合、redistribute コマンドを使用して、ルートを NSSA でなく通常のエリアにインポートする場合に選択します。 default-information-originate : タイプ 7 LSA を NSSA にインポートするようにする場合に、ABR で選択します。 no-redistribution : サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	area area-id range address mask	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	<code>show ip ospf [process-id]</code>	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。
	<code>show ip ospf [process-id [area-id]] database</code>	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

その他の OSPF パラメータの設定

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- 経路集約：他のプロトコルからのルートを再配信すると（「[ルート マップによるルーティング情報の再配信](#)」(P.41-95) を参照)、各ルータは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワーク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。
- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーン リンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定できません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に ASBR になります。ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用される Domain Name Server (DNS) 名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅 (*bw*) は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。
- アドミニストレーティブ ディスタンスは、ルーティング情報送信元の信頼性を表す数値です。0 ~ 255 の整数を指定でき、値が大きいほど信頼性は低下します。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって学習した別のルーティング ドメインからのルート（外部）の 3 つの異なるアドミニストレーティブ ディスタンスが使用されます。どのアドミニストレーティブ ディスタンスの値でも変更できます。
- 受動インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに **hello** パケットを送信しないようにするには、送信側デバイスを受動インターフェイスに設定する必要があります。両方のデバイスは受信側インターフェイス宛ての **hello** パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。

- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

上記の OSPF パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	summary-address address mask	(任意) 1 つのサマリールートだけがアドバタイズされるように、再配信されたルートアドレスおよび IP サブネット マスクを指定します。
ステップ 4	area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [trans] [[authentication-key key] message-digest-key keyid md5 key]]	(任意) 仮想リンクを確立し、パラメータを設定します。パラメータ定義については「OSPF インターフェイスの設定」(P.41-29)、仮想リンクのデフォルト設定については表 41-5 (P.41-27) を参照してください。
ステップ 5	default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]	(任意) 強制的に OSPF ルーティング ドメインにデフォルト ルートを生成するように ASBR を設定します。パラメータはすべて任意です。
ステップ 6	ip ospf name-lookup	(任意) DNS 名検索を設定します。デフォルトはディセーブルです。
ステップ 7	ip auto-cost reference-bandwidth ref-bw	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	distance ospf {[inter-area dist1] [inter-area dist2] [external dist3]}	(任意) OSPF の距離の値を変更します。各タイプのルートのデフォルト距離は 110 です。有効値は 1 ~ 255 です。
ステップ 9	passive-interface type number	(任意) 指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	timers throttle spf spf-delay spf-holdtime spf-wait	(任意) ルート計算タイマーを設定します。 <ul style="list-style-type: none"> • spf-delay : SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ~ 600000 です。ミリ秒です。 • spf-holdtime : 最初と 2 番目の SPF 計算の間の遅延。指定できる範囲は 1 ~ 600000 ミリ秒です。 • spf-wait : SPF 計算の最大待機時間 (ミリ秒)。指定できる範囲は 1 ~ 600000 ミリ秒です。
ステップ 11	ospf log-adj-changes	(任意) ネイバー ステートが変更されたとき、Syslog メッセージを送信します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ip ospf [process-id [area-id]] database	特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「OSPF のモニタリング」(P.41-35) を参照してください。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LSA グループ ペーシングの変更

OSPF LSA グループ ペーシング機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用できるようになります。デフォルトでこの機能はイネーブルとなっています。デフォルトのペーシング インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ ペーシング インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。たとえば、データベース内に約 10,000 個の LSA が格納されている場合は、ペーシング インターバルを短くすると便利です。小さなデータベース (40 ~ 100 LSA) を使用する場合は、ペーシング インターバルを長くし、10 ~ 20 分に設定してください。

OSPF LSA ペーシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>timers lsa-group-pacing seconds</code>	LSA のグループ ペーシングを変更します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、`no timers lsa-group-pacing` ルータ コンフィギュレーション コマンドを使用します。

ループバック インターフェイスの設定

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信します。ループバック インターフェイスが IP アドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

ループバック インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface loopback 0</code>	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip address address mask</code>	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip interface</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

表 41-6 に、統計情報を表示するために使用する特権 EXEC コマンドの一部を示します。**show ip ospf database** 特権 EXEC コマンドのオプションおよび表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』を参照してください。

表 41-6 IP OSPF 統計情報の表示コマンド

コマンド	目的
show ip ospf [<i>process-id</i>]	OSPF ルーティング プロセスに関する一般的な情報を表示します。
show ip ospf [<i>process-id</i>] database [router] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [router] [self-originate] show ip ospf [<i>process-id</i>] database [router] [adv-router [<i>ip-address</i>]] show ip ospf [<i>process-id</i>] database [network] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [summary] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [asbr-summary] [<i>link-state-id</i>] show ip ospf [<i>process-id</i>] database [external] [<i>link-state-id</i>] show ip ospf [<i>process-id area-id</i>] database [database-summary]	OSPF データベースに関連する情報を表示します。
show ip ospf border-routes	内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
show ip ospf interface [<i>interface-name</i>]	OSPF に関連するインターフェイス情報を表示します。
show ip ospf neighbor [<i>interface-name</i>] [<i>neighbor-id</i>] detail	OSPF インターフェイス ネイバー情報を表示します。
show ip ospf virtual-links	OSPF に関連する仮想リンク情報を表示します。

EIGRP の設定

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクトル アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンス テクノロジーには、拡散更新アルゴリズム (DUAL) と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算に含まれません。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するとき問題となるのは、トランスポート レイヤのホップ カウンタだけです。IP パケットが 15 台の

ルータを経由し、宛先方向のネクスト ホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステートが変更された場合、ルーティング テーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：完全更新パケットを受信ごとに処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しないネイバー探索メカニズム：このメカニズムを使用し隣接ルータに関する情報を取得します。
- Variable-Length Subnet Mask (VLSM; 可変長サブネット マスク)
- 任意のルート集約
- 大規模ネットワークへの対応

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- **ネイバー探索および回復**：直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。ルータは、ネイバーが到達不能または動作不能になったことも検出する必要があります。ネイバー探索および回復は、サイズの小さな hello パケットを定期的送信することにより、わずかなオーバーヘッドで実現されます。hello パケットが受信されているかぎり、Cisco ISO ソフトウェアは、ネイバーが有効に機能していると学習します。このように判別された場合、隣接ルータはルーティング情報を交換できます。
- **信頼できるトランスポート プロトコル**：EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率を高めるため、信頼性は必要な場合にだけ確保されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーにそれぞれ hello パケットを確実に送信する必要はありません。したがって、EIGRP はパケットへの確認応答が不要であることを知らせる、レシーバ宛の情報をパケットに格納し、単一のマルチキャスト hello を送信します。他のタイプのパケット（アップデートなど）の場合は、確認応答（ACK パケット）を要求します。信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチキャスト パケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。
- **DUAL 有限状態マシン**：すべてのルート計算に関する決定プロセスを統合し、すべてのネイバーによってアドバタイズされたすべてのルートをトラッキングします。DUAL は距離情報（メトリックともいう）を使用して、効率的な、ループのないパスを選択し、さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス（ルーティング ループに関連しないことが保証されている）を持つ、パケット転送に使用される隣接ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、この結果、新しい後継ルータが決定されます。ルートの再計算に要する時間によって、コンバージェンス時間が変わります。再計算はプロセッサに負荷がかかるため、必要でない場合は、再計算しないようにしてください。トポロジが変更されると、DUAL は適切な後継ルータの有無を調べます。適切な後継ルータが存在する場合は、それらを探して使用し、不要な再計算を回避します。
- **プロトコル依存モジュール**：ネットワーク層プロトコル特有の作業を行います。たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。また、EIGRP パケットを解析したり、DUAL に受信した新しい情報を通知したりします。EIGRP は DUAL にルーティング決定を行うように要求しますが、結果は IP ルーティング テーブルにストアされます。EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

ここでは、次の設定について説明します。

- 「EIGRP のデフォルト設定」 (P.41-37)
- 「基本的な EIGRP パラメータの設定」 (P.41-39)
- 「EIGRP インターフェイスの設定」 (P.41-40)
- 「EIGRP ルート認証の設定」 (P.41-40)
- 「EIGRP スタブ ルーティングの設定」 (P.41-42)
- 「EIGRP のモニタリングおよびメンテナンス」 (P.41-43)

EIGRP のデフォルト設定

表 41-7 に、EIGRP のデフォルト設定を示します。

表 41-7 EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	ディセーブル クラスフル ネットワーク境界を通過するとき、この境界にサブプレフィックスはサマライズされません。
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。 <ul style="list-style-type: none"> • 帯域幅：0 以上の kb/s • 遅延 (10 マイクロ秒)：0 または 39.1 ナノ秒の倍数である任意の正の数値 • 信頼性：0 ~ 255 の任意の数値 (255 の場合は信頼性が 100%) • 負荷：0 ~ 255 の数値で表される有効帯域幅 (255 の場合は 100% の負荷) • MTU：バイトで表されたルートの MTU サイズ (0 または任意の正の整数)
ディスタンス	内部距離：90 外部距離：170
EIGRP の隣接関係変更ログ	ディセーブル 隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅比率	50%
IP hello 間隔	低速 Nonbroadcast Multiaccess (NBMA; 非ブロードキャスト マルチアクセス) ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速 NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義

表 41-7 EIGRP のデフォルト設定 (続き)

機能	デフォルト設定
メトリック重み	tos : 0、k1 および k3 : 1、k2、k4、および k5 : 0
ネットワーク	指定なし
NSF ¹ 認識	イネーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分
差異	1 (等コストロード バランシング)。

1. NSF = Nonstop Forwarding

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。



(注)

ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の両方が設定された移行ルータを指定する必要があります。この場合は、この次の項に記載されているステップ 1 ~ 3 を実行してください (「[スプリット ホライズンの設定](#)」(P.41-25) も参照)。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP NSF 認識

EIGRP NSF 認識機能は IP サービス イメージの IPv4 でサポートされています。隣接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

この機能をディセーブルにできません。この機能の詳細については、次の URL の『*EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080160010.html

基本的な EIGRP パラメータの設定

EIGRP を設定するには、特権 EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外のステップはオプションです。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router eigrp autonomous-system number</code>	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他の EIGRP ルータへのルート特定し、ルーティング情報をタグ付けします。
ステップ 3	<code>network network-number</code>	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 4	<code>eigrp log-neighbor-changes</code>	(任意) EIGRP 隣接関係変更のログギングをイネーブルにし、ルーティング システムの安定性を監視します。
ステップ 5	<code>metric weights tos k1 k2 k3 k4 k5</code>	(任意) EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。  注意 メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。
ステップ 6	<code>offset list [access-list number name] {in out} offset [type number]</code>	(任意) オフセット リストをルーティング メトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増やします。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 7	<code>auto-summary</code>	(任意) ネットワークレベル ルートへのサブネット ルートの自動サマライズをイネーブルにします。
ステップ 8	<code>ip summary-address eigrp autonomous-system-number address mask</code>	(任意) サマリー集約を設定します。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show ip protocols</code>	設定を確認します。
ステップ 11	<code>show ip protocols</code>	設定を確認します。 NSF 認識の場合、出力に次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

EIGRP インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	<code>ip bandwidth-percent eigrp percent</code>	(任意) インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。
ステップ 4	<code>ip summary-address eigrp autonomous-system-number address mask</code>	(任意) 指定されたインターフェイスのサマリー集約アドレスを設定します (auto-summary がイネーブルの場合は、通常設定する必要はありません)。
ステップ 5	<code>ip hello-interval eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスの hello タイム インターバルを変更します。指定できる範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 60 秒、その他のすべてのネットワークでは 5 秒です。
ステップ 6	<code>ip hold-time eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。指定できる範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルト値は 180 秒、その他のすべてのネットワークでは 15 秒です。  注意 ホールド タイムを調整する前に、シスコのテクニカルサポートにお問い合わせください。
ステップ 7	<code>no ip split-horizon eigrp autonomous-system-number</code>	(任意) スプリット ホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show ip eigrp interface</code>	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	<code>ip authentication mode eigrp autonomous-system md5</code>	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	<code>ip authentication key-chain eigrp autonomous-system key-chain</code>	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>key chain name-of-chain</code>	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	<code>key number</code>	キーチェーン コンフィギュレーション モードで、キー番号を識別します。
ステップ 8	<code>key-string text</code>	キーチェーン コンフィギュレーション モードで、キー スtring を識別します。
ステップ 9	<code>accept-lifetime start-time {infinite end-time duration seconds}</code>	(任意) キーを受信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および <i>duration</i> は infinite です。
ステップ 10	<code>send-lifetime start-time {infinite end-time duration seconds}</code>	(任意) キーを送信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および <i>duration</i> は infinite です。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show key chain</code>	認証キー情報を表示します。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

EIGRP スタブルルーティングの設定

EIGRP スタブルルーティング機能は、エンドユーザの近くにルーテッドトラフィックを移動することでリソースの利用率を低減させます。

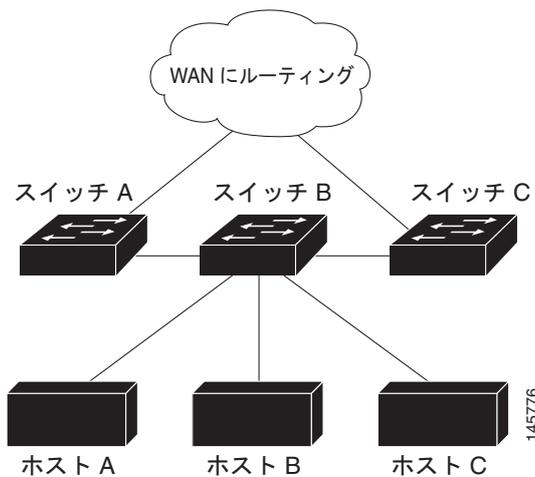
EIGRP スタブルルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、EIGRP スタブルルーティングを設定しているスイッチ経由です。スイッチは、ユーザインターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッドトラフィックを送信します。

EIGRP スタブルルーティングを使用しているときは、EIGRP を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモートルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティングアップデートに対するすべてのクエリーに応答します。

スタブルルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブルルータに照会しません。また、スタブピアを持つルータは、そのピアについては照会しません。スタブルルータは、配布ルータに依存して適切なアップデートをすべてのピアに送信します。

図 41-4 では、スイッチ B が EIGRP スタブルルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティックルート、再配信ルート、およびサマリールートをスイッチ A と C にアドバタイズします。スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 41-4 EIGRP スタブルルータ設定



(注) **igmp stub** ルータ コンフィギュレーション コマンドを入力すると、**igmp stub connected summary** コマンドだけが機能します。CLI ヘルプには **receive-only** および **static** キーワードが表示され、これらのキーワードを入力することができますが、IP ベース イメージを稼働するスイッチでは常に、**connected** および **summary** キーワードが設定されているかのように動作します。

EIGRP スタブルルーティングの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.2』の「Configuring EIGRP Stub Routing」を参照してください。

EIGRP のモニタリングおよびメンテナンス

ネイバー テーブルからネイバーを削除できます。さらに、各種 EIGRP ルーティング統計情報を表示することもできます。表 41-8 に、ネイバー削除および統計情報表示用の特権 EXEC コマンドを示します。表示されるフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』を参照してください。

表 41-8 IP EIGRP の clear および show コマンド

コマンド	目的
<code>clear ip eigrp neighbors [if-address interface]</code>	ネイバー テーブルからネイバーを削除します。
<code>show ip eigrp interface [interface] [as number]</code>	EIGRP に設定されているインターフェイスに関する情報を表示します。
<code>show ip eigrp neighbors [type-number]</code>	EIGRP によって検出されたネイバーを表示します。
<code>show ip eigrp topology [autonomous-system-number] [[ip-address] mask]</code>	指定されたプロセスの EIGRP トポロジテーブルを表示します。
<code>show ip eigrp traffic [autonomous-system-number]</code>	すべてまたは特定の EIGRP プロセスの送受信パケット数を表示します。

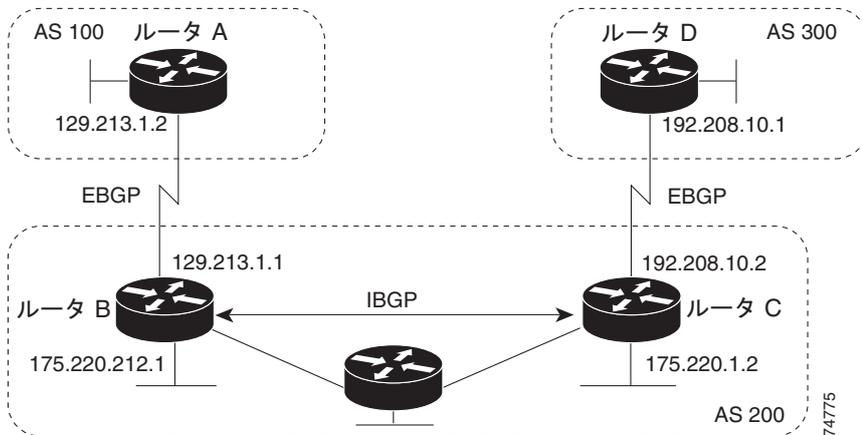
BGP の設定

BGP は、Exterior Gateway Protocol (EGP; エクステリア ゲートウェイ プロトコル) です。AS 間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムを設定するために使用されます。AS は、同じ管理下で動作して RIP や OSPF などの IGP を境界内で実行し、EGP を使用して相互接続されるルータで構成されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。BGP の詳細については、『Internet Routing Architectures』(Cisco Press 刊)、および Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] にある『Cisco IP and IP Routing Configuration Guide』の「Configuring BGP」の章を参照してください。

BGP コマンドおよびキーワードの詳細については、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』の「IP Routing Protocols」を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B 「Cisco IOS Release 15.0(1)SE でサポートされていないコマンド」を参照してください。

BGP アップデートを交換する場合、同じ AS に属するルータは *Internal BGP* (IBGP) を実行し、異なる AS に属するルータは *External BGP* (EBGP) を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、ルーティング アップデートが AS 間で交換されるか (EBGP)、または AS 内で交換されるか (IBGP) という点で異なります。図 41-5 に、EBGP と IBGP の両方が稼働するネットワークを示します。

図 41-5 EBGP、IBGP、および複数の AS



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼働する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達することを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。BGP はトランスポート プロトコルとして TCP を使用します（特にポート 179）。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。図 41-5 では、ルータ A と B、ルータ B と C、およびルータ C と D がそれぞれ BGP ピアです。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない AS マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼働しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼働し、2 つのネイバーが相互に到達する限り、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（*連合*および*ルート リフレクタ*）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアはキープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGP の場合、各ルートはネットワーク番号、情報が通過した自律システムのリスト（*自律システム パス*）、および他のパス属性リストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをプルーニングしたり、AS レベル ポリシー判断を行うために使用できます。

Cisco IOS が稼働しているルータまたはスイッチが IBGP ルートを選択または使用するのには、ネクストホップルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP は属性値に基づいてパスを選択します。BGP 属性の詳細については、「[BGP 判断属性の設定](#)」(P.41-52) を参照してください。

BGP バージョン 4 では Classless Interdomain Routing (CIDR; クラスレス ドメイン間ルーティング) がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。CIDR は、BGP 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズをサポートします。

ここでは、次の設定について説明します。

- 「BGP のデフォルト設定」 (P.41-45)
- 「BGP ルーティングのイネーブル化」 (P.41-48)
- 「ルーティング ポリシー変更の管理」 (P.41-51)
- 「BGP 判断属性の設定」 (P.41-52)
- 「ルート マップによる BGP フィルタリングの設定」 (P.41-54)
- 「ネイバーによる BGP フィルタリングの設定」 (P.41-55)
- 「BGP フィルタリング用のプレフィックス リストの設定」 (P.41-56)
- 「BGP コミュニティ フィルタリングの設定」 (P.41-57)
- 「BGP ネイバーおよびピア グループの設定」 (P.41-59)
- 「集約アドレスの設定」 (P.41-61)
- 「ルーティング ドメイン連合の設定」 (P.41-62)
- 「BGP ルート リフレクタの設定」 (P.41-62)
- 「ルート ダンプニングの設定」 (P.41-63)
- 「BGP のモニタリングおよびメンテナンス」 (P.41-64)

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Routing Protocols」で「Configuring BGP」の章を参照してください。特定コマンドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』を参照してください。これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B 「Cisco IOS Release 15.0(1)SE でサポートされていないコマンド」を参照してください。

BGP のデフォルト設定

表 41-9 に、BGP の基本的なデフォルト設定を示します。すべての特性のデフォルトについては、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』の特定のコマンドを参照してください。

表 41-9 BGP のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：未定義
AS パス アクセス リスト	未定義
自動サマリー	イネーブル
最適パス	<ul style="list-style-type: none"> • ルータはルートを選択する場合に AS パスを考慮し、外部 BGP ピアからの類似ルートは比較されない • ルータ ID の比較：ディセーブル

表 41-9 BGP のデフォルト設定 (続き)

機能	デフォルト設定
BGP コミュニティ リスト	<ul style="list-style-type: none"> 番号：未定義。コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 フォーマット：シスコ デフォルト フォーマット (32 ビット番号)
BGP 連合 ID/ピア	<ul style="list-style-type: none"> ID：未設定 ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル
BGP ローカル初期設定	100。指定できる範囲は 0～4294967295 です (大きな値を推奨)。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズなし
BGP ルート ダンプニング	デフォルトでは、ディセーブルです。イネーブルの場合は、次のようになります。 <ul style="list-style-type: none"> 半減期は 15 分 再使用は 750 (10 秒増分) 抑制は 2000 (10 秒増分) 最大抑制時間は半減期の 4 倍 (60 分)
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元 (プロトコルまたはネットワーク再配信)	ディセーブル
デフォルト メトリック	自動メトリック変換 (組み込み)
ディスタンス	<ul style="list-style-type: none"> 外部ルート アドミニストレーティブ ディスタンス：20 (有効値は 1～255) 内部ルート アドミニストレーティブ ディスタンス：200 (有効値は 1～255) ローカル ルート アドミニストレーティブ ディスタンス：200 (有効値は 1～255)
ディストリビュート リスト	<ul style="list-style-type: none"> 入力 (アップデート中に受信されたネットワークをフィルタリング)：ディセーブル 出力 (アップデート中のネットワークのアドバタイズを抑制)：ディセーブル
内部ルート再配信	ディセーブル
IP プレフィックス リスト	未定義
Multi Exit Discriminator (MED)	<ul style="list-style-type: none"> 常に比較：ディセーブル。異なる AS 内のネイバーからのパスに対して、MED を比較しません。 最適パスの比較：ディセーブル 最悪パスである MED の除外：ディセーブル 決定的な MED 比較：ディセーブル

表 41-9 BGP のデフォルト設定 (続き)

機能	デフォルト設定
ネイバー	<ul style="list-style-type: none"> • アドバタイズメント インターバル: 外部ピアの場合は 30 秒、内部ピアの場合は 5 秒 • ロギング変更: イネーブル • 条件付きアドバタイズ: ディセーブル • デフォルト送信元: ネイバーに送信されるデフォルト ルートはなし • 説明: なし • ディストリビュート リスト: 未定義 • 外部 BGP マルチホップ: 直接接続されたネイバーだけを許可 • フィルタ リスト: 使用しない • 受信したプレフィックスの最大数: 制限なし • ネクスト ホップ (BGP ネイバーのネクスト ホップとなるルータ): ディセーブル • パスワード: ディセーブル • ピア グループ: 定義なし、割り当てメンバーなし • プレフィックス リスト: 指定なし • リモート AS (ネイバー BGP テーブルへのエントリ追加): ピア定義なし • プライベート AS 番号の削除: ディセーブル • ルート マップ: ピアへの適用なし • コミュニティ属性送信: ネイバーへの送信なし。 • シャットダウンまたはソフト再設定: ディセーブル • タイマー: 60 秒、ホールドタイム: 180 秒 • アップデート送信元: 最適ローカル アドレス • バージョン: BGP バージョン 4 • 重み: BGP ピアによって学習されたルート: 0、ローカル ルータから取得されたルート: 32768
NSF ¹ 認識	<p>ディセーブル。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。</p> <p>(注) NSF 認識は、グレースフル リスタートをイネーブルにすることで、IPv4 でイネーブルにできます。</p>
ルート リフレクタ	未設定
同期化 (BGP および IGP)	イネーブル
テーブル マップ アップデート	ディセーブル
タイマー	キープアライブ: 60 秒、ホールドタイム: 180 秒

1. NSF = Nonstop Forwarding

NSF 認識

BGP NSF 認識機能は IP サービス イメージの IPv4 でサポートされています。BGP ルーティングでこの機能をイネーブルにするには、グレースフルリスタートをイネーブルにする必要があります。隣接ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断せずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、隣接ルータからパケットを転送し続けます。

詳細については、次の URL の『*BGP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015fedeh.html

BGP ルーティングのイネーブル化

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ~ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズ対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または AS 内のすべてのルータで BGP が稼働している場合は、同期化をディセーブルにし、IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束するようにします。

BGP ルーティングをイネーブルにして BGP ルーティング プロセスを確立し、ネイバーを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合にだけ必須)。
ステップ 3	router bgp autonomous-system	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ~ 65535 です。64512 ~ 65535 は、プライベート AS 番号専用です。

	コマンド	目的
ステップ 4	network <i>network-number</i> [mask <i>network-mask</i>] [route-map <i>route-map-name</i>]	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。
ステップ 5	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i>	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6	neighbor { <i>ip-address</i> <i>peer-group-name</i> } remove-private-as	(任意) 発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7	no synchronization	(任意) BGP と IGP の同期化をディセーブルにします。
ステップ 8	no auto-summary	(任意) 自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに追加されます。
ステップ 9	bgp fast-external-fallover	(任意) 外部ネイバー間のリンクが切断された場合、BGP セッションを自動的にリセットします。デフォルトで、セッションは即座にリセットされません。
ステップ 10	bgp graceful-restart	(任意) NSF 認識をスイッチでイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show ip bgp network <i>network-number</i> または show ip bgp neighbor	設定を確認します。 NSF 認識 (グレースフル リスタート) がネイバーでイネーブルにされていることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised and received</i> スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised</i>
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP AS を削除するには、**no router bgp autonomous-system** グローバル コンフィギュレーション コマンドを使用します。BGP テーブルからネットワークを削除するには、**no network network-number** ルータ コンフィギュレーション コマンドを使用します。ネイバーを削除するには、**no neighbor {ip-address | peer-group-name} remote-as number** ルータ コンフィギュレーション コマンドを使用します。ネイバーにアップデート内のプライベート AS 番号を追加するには、**no neighbor {ip-address |**

`peer-group-name}` **remove-private-as** ルータ コンフィギュレーション コマンドを使用します。同期化を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 41-5 に示されたルータ上で BGP を設定する例を示します。

ルータ A :

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B :

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C :

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D :

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼働していることを確認するには、**show ip bgp neighbors** 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors
```

```
BGP neighbor is 129.213.1.1, remote AS 200, external link
  BGP version 4, remote router ID 175.220.212.1
  BGP state = established, table version = 3, up for 0:10:59
  Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
  Minimum time between advertisement runs is 30 seconds
  Received 2828 messages, 0 notifications, 0 in queue
  Sent 2826 messages, 0 notifications, 0 in queue
  Connections established 11; dropped 10
```

state = established 以外の情報が出力された場合、ピアは稼働していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。継続的にテーブルバージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 B「Cisco IOS Release 15.0(1)SE でサポートされていないコマンド」を参照してください。

ルーティング ポリシー変更の管理

ピアのルーティング ポリシーには、インバウンドまたはアウトバウンド ルーティング テーブル アップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。このあとで BGP フィルタ、重量、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハードリセットとソフトリセットの 2 つのタイプがあります。事前に設定を行わなくても、ソフトリセットを使用できます。事前設定なしにソフトリセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。ソフトリセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報を動的に交換したり、それぞれのアウトバウンド ルーティング テーブルをあとで再アドバタイズできます。

- ソフトリセットによってネイバーからインバウンドアップデートが生成された場合、このリセットは *ダイナミック インバウンド ソフト リセット* といいます。
- ソフトリセットによってネイバーに一連のアップデートが送信された場合、このリセットは *アウトバウンド ソフト リセット* といいます。

ソフト インバウンドリセットが発生すると、新規インバウンドポリシーが有効になります。ソフトアウトバウンドリセットが発生すると、BGP セッションがリセットされずに、新規ローカルアウトバウンドポリシーが有効になります。アウトバウンドポリシーのリセット中に新しい一連のアップデートが送信されると、新規インバウンドポリシーも有効になる場合があります。

表 41-10 に、ハードリセットとソフトリセットの利点および欠点を示します。

表 41-10 ハードリセットとソフトリセットの利点および欠点

リセットタイプ	利点	欠点
ハードリセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供された BGP、IP、および FIB テーブルのプレフィックスが失われます。推奨しません。
発信ソフトリセット	ルーティング テーブル アップデートが設定、保管されません。	インバウンドルーティング テーブル アップデートがリセットされません。
ダイナミック インバウンドソフトリセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブル アップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります。

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>show ip bgp neighbors</code>	ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 <i>Received route refresh capability from peer</i>
ステップ 2	<code>clear ip bgp {* address peer-group-name}</code>	指定された接続上でルーティング テーブルをリセットします。 <ul style="list-style-type: none"> すべての接続をリセットする場合は、アスタリスク (*) を入力します。 特定の接続をリセットする場合は、IP address を入力します。 ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	<code>clear ip bgp {* address peer-group-name} soft out</code>	(任意) 指定された接続上でインバウンド ルーティング テーブルをリセットするには、アウトバウンド ソフト リセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 <ul style="list-style-type: none"> すべての接続をリセットする場合は、アスタリスク (*) を入力します。 特定の接続をリセットする場合は、IP address を入力します。 ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	<code>show ip bgp</code> <code>show ip bgp neighbors</code>	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断属性の設定

BGP スピーカーが複数の AS から受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されている属性値、および BGP で設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィックスに対する 2 つの EBGP パスを学習するとき、最適パスを選択して IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルで、同じネイバー AS から複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスが IP ルーティング テーブルに格納されます。その後、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロード バランシングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するために属性を評価する順序が決まります。

1. パスで指定されているネクスト ホップが到達不能な場合、このアップデートは削除されます。BGP ネクスト ホップ属性 (ソフトウェアによって自動判別される) は、宛先に到達するために使用されるネクスト ホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクストホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドを使用します。
2. 最大の重みのパスを推奨します (シスコ独自のパラメータ)。ウェイト属性はルータにローカルであるため、ルーティング アップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト属性は 32768 で、それ以外のパスのウェイト属性は 0 です。最大の重みのルートを推奨します。重みを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。

3. ローカル プリファレンス値が最大のルートを推奨します。ローカル プリファレンスはルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル初期設定属性のデフォルト値は 100 です。ローカル プリファレンスを設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼働する BGP から送信されたルートを推奨します。
5. AS パスが最短のルートを推奨します。
6. 送信元タイプが最小のルートを推奨します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック属性が最小のルートを推奨します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部 (IBGP) パスより、外部 (EBGP) パスを推奨します。
9. 最も近い IGP ネイバー (最小の IGP メトリック) を通って到達できるルートを推奨します。ルータは、AS 内の最短の内部パス (BGP のネクストホップへの最短パス) を使用し、宛先に到達するためです。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。
 - 最適ルートと目的のルートがともに外部ルートである
 - 最適ルートと目的のルートの両方が、同じネイバー AS からのルートである
 - **maximum-paths** がイネーブルである
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック (仮想) アドレスですが、実装に依存することがあります。

同じ判断属性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router bgp <i>autonomous-system</i>	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3	bgp best-path as-path ignore	(任意) ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4	neighbor {<i>ip-address</i> <i>peer-group-name</i>} next-hop-self	(任意) ネクストホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクストホップの処理をディセーブルにします。
ステップ 5	neighbor {<i>ip-address</i> <i>peer-group-name</i>} weight <i>weight</i>	(任意) ネイバー接続に重みを割り当てます。指定できる値は 0 ~ 65535 です。最大の重みのルートを推奨します。別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカルルータから送信されたルートのデフォルトの重みは 32768 です。
ステップ 6	default-metric <i>number</i>	(任意) 推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルータも、この値に設定されます。指定できる範囲は 1 ~ 4294967295 です。最小値を推奨します。

	コマンド	目的
ステップ 7	<code>bgp bestpath med missing-as-worst</code>	(任意) MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	<code>bgp always-compare med</code>	(任意) 異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間でだけ比較されます。
ステップ 9	<code>bgp bestpath med confed</code>	(任意) 連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	<code>bgp deterministic med</code>	(任意) 同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	<code>bgp default local-preference value</code>	(任意) デフォルトのローカルプリファレンス値を変更します。指定できる範囲は 0 ~ 4294967295 で、デフォルト値は 100 です。最大のローカルプリファレンス値を推奨します。
ステップ 12	<code>maximum-paths number</code>	(任意) IP ルーティングテーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティングテーブルに追加されます。指定できる範囲は 1 ~ 16 です。複数の値を指定すると、パス間のロードバランシングが可能になります (スイッチソフトウェアでは最大 32 の等コストルーティングが許可されていますが、スイッチハードウェアはルートあたり 17 パス以上は使用しません)。
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show ip bgp</code> <code>show ip bgp neighbors</code>	ルーティングテーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルトステートに戻すには、このコマンドの **no** 形式を使用します。

ルートマップによる BGP フィルタリングの設定

BGP 内でルートマップを使用すると、ルーティング情報を制御、変更したり、ルーティングドメイン間でルートを再配信する条件を定義できます。ルートマップの詳細については、「[ルートマップによるルーティング情報の再配信](#)」(P.41-95) を参照してください。各ルートマップには、ルートマップを識別する名前 (マップタグ) およびオプションのシーケンス番号が付いています。

ルートマップを使用してネクストホップ処理をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>route-map map-tag [[permit deny] sequence-number]</code>	ルートマップを作成し、ルートマップ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ3	<code>set ip next-hop ip-address [...ip-address] [peer-address]</code>	(任意) ネクストホップ処理をディセーブルにするようにルート マップを設定します。 <ul style="list-style-type: none"> インバウンドルート マップの場合は、一致するルートのネクストホップをネイバー ピアアドレスに設定し、サードパーティのネクストホップを上書きします。 BGP ピアのアウトバウンドルート マップの場合は、ネクストホップをローカル ルータのピアアドレスに設定して、ネクストホップ計算をディセーブルにします。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show route-map [map-name]</code>	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート マップを削除するには、`no route-map map-tag` コマンドを使用します。ネクストホップ処理を再びイネーブルにするには、`no set ip next-hop ip-address` コマンドを使用します。

ネイバーによる BGP フィルタリングの設定

BGP アドバタイズメントをフィルタリングするには、`as-path access-list` グローバル コンフィギュレーション コマンドや `neighbor filter-list` ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。`neighbor distribute-list` ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。`distribute-list` フィルタはネットワーク番号に適用されます。`distribute-list` コマンドの詳細については、「[ルーティング アップデートのアドバタイズおよび処理の制御](#)」(P.41-103) を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、さまざまな属性を変更したりできます。ルート マップは、インバウンドアップデートまたはアウトバウンドアップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。インバウンドおよびアウトバウンドの両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには `match as-path access-list` ルート マップ コマンド、コミュニティに基づくマッチングには `match community-list` ルート マップ コマンド、ネットワークに基づくマッチングには `ip access-list` グローバル コンフィギュレーション コマンドが必要です。

ネイバー単位のルート マップを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>router bgp autonomous-system</code>	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ3	<code>neighbor {ip-address peer-group name} distribute-list {access-list-number name} {in out}</code>	(任意) アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 (注) <code>neighbor prefix-list</code> ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。

	コマンド	目的
ステップ 4	neighbor { <i>ip-address</i> <i>peer-group name</i> } route-map <i>map-tag</i> { in out }	(任意) ルート マップを適用し、着信または発信ルートをフィルタリングします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip bgp neighbors	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ネイバーからアクセス リストを削除するには、**no neighbor distribute-list** コマンドを使用します。ネイバーからルート マップを削除するには、**no neighbor route-map map-tag** ルータ コンフィギュレーション コマンドを使用します。

BGP AS パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現を使用するアクセス リストです。(正規表現の作成方法については、『Cisco IOS Dial Technologies Command Reference, Release 12.2』の付録「Regular Expressions」を参照してください)。この方法を使用するには、AS パスのアクセス リストを定義し、特定のネイバーに対して送受信されるアップデートに適用します。

BGP パス フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip as-path access-list <i>access-list-number</i> { permit deny } <i>as-regular-expressions</i>	BGP 関連アクセス リストを定義します。
ステップ 3	router bgp <i>autonomous-system</i>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor { <i>ip-address</i> <i>peer-group name</i> } filter-list { <i>access-list-number</i> <i>name</i> } { in out weight <i>weight</i> }	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip bgp neighbors [<i>paths</i> <i>regular-expression</i>]	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィックス リストの設定

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィックス リストを使用できます。プレフィックス リストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、コマンドライン インターフェイス (CLI) 設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィックス リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィックス リストに記載されたプレフィックスとルートのプレフィックスが照合されます。一致が存在する場合は、一致したルートが使用されます。プレフィックスが許可されるか、または拒否されるかは、次に示すルールに基づいて決定されます。

- 空のプレフィックス リストはすべてのプレフィックスを許可します。
- 特定のプレフィックスがプレフィックス リストのどのエン트리とも一致しなかった場合、実質的に拒否されたものと見なされます。

- 指定されたプレフィックスと一致するエントリがプレフィックス リスト内に複数存在する場合は、シーケンス番号が最小であるプレフィックス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

コンフィギュレーション エントリを削除する場合は、シーケンス番号を指定する必要はありません。**show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィックス リストを使用する場合は、あらかじめプレフィックス リストを設定しておく必要があります。プレフィックス リストを作成したり、プレフィックス リストにエントリを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip prefix-list list-name [seq seq-value] deny permit network/len [ge ge-value] [le le-value]	一致条件のために、アクセスを拒否 (deny) または許可 (permit) するプレフィックス リストを作成します。シーケンス番号を指定することもできます。少なくとも 1 つの permit コマンドまたは deny コマンドを入力する必要があります。 <ul style="list-style-type: none"> network/len は、ネットワーク番号およびネットワーク マスクの長さ (ビット単位) です。 (任意) ge および le の値は、照合するプレフィックス長の範囲を指定します。指定された ge-value および le-value は、次の条件を満たす必要があります。$len < ge-value < le-value < 32$
ステップ 3	ip prefix-list list-name seq seq-value deny permit network/len [ge ge-value] [le le-value]	(任意) プレフィックス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip prefix list [detail summary] name [network/len] [seq seq-num] [longer] [first-match]	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

プレフィックス リストまたはそのエントリをすべて削除する場合は、**no ip prefix-list list-name** グローバル コンフィギュレーション コマンドを使用します。プレフィックス リストから特定のエントリを削除する場合は、**no ip prefix-list seq seq-value** グローバル コンフィギュレーション コマンドを使用します。シーケンス番号の自動生成をディセーブルにするには **no ip prefix-list sequence number** コマンドを、自動生成を再びイネーブルにするには **ip prefix-list sequence number** コマンドを使用します。プレフィックス リスト エントリのヒット数テーブルをクリアするには、**clear ip prefix-list** 特権 EXEC コマンドを使用します。

BGP コミュニティ フィルタリングの設定

BGP コミュニティ フィルタリングは、COMMUNITIES 属性の値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。この属性によって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。各宛先は複数のコミュニティに属します。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、過渡的でグローバルなオプションの属性である、COMMUNITIES 属性（1 ~ 4294967200 の数値）によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet** : このルートをインターネット コミュニティにアドバタイズします。すべてのルータが所属します。
- **no-export** : EBGp ピアにこのルートをアドバタイズしません。
- **no-advertise** : どのピア（内部または外部）にもこのルートをアドバタイズしません。
- **local-as** : ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配信するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES 属性に、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルート マップの **match** 句で使用されるコミュニティ グループを作成できます。さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

コミュニティに基づいて COMMUNITIES 属性および **match** 句を設定するには、「[ルート マップによるルーティング情報の再配信](#)」(P.41-95) に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

デフォルトでは、COMMUNITIES 属性はネイバーに送信されません。COMMUNITIES 属性が特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

コミュニティ リストを作成、適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip community-list community-list-number {permit deny} community-number	コミュニティ リストを作成し、番号を割り当てます。 <ul style="list-style-type: none"> • community-list-number は 1 ~ 99 の整数です。この値は、コミュニティの許可または拒否グループを 1 つまたは複数識別します。 • community-number は、set community ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3	router bgp autonomous-system	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor {ip-address peer-group name} send-community	この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 5	set comm-list list-num delete	(任意) ルート マップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ属性から、コミュニティを削除します。
ステップ 6	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	ip bgp-community new-format	(任意) AA:NN の形式で、BGP コミュニティを表示、解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長形式で表示されます。シスコのデフォルトのコミュニティ形式は、NNA A です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとりま す。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。

	コマンド	目的
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show ip bgp community</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

通常、BGP ネイバーの多くは同じアップデート ポリシー (同じアウトバウンドルート マップ、配信リスト、フィルタ リスト、アップデート送信元など) を使用して設定されます。アップデート ポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは **remote-as** (設定されている場合)、**version**、**update-source**、**out-route-map**、**out-filter-list**、**out-dist-list**、**minimum-advertisement-interval**、**next-hop-self** など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対する変更を継承します。また、アウトバウンドアップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

BGP ピアを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>neighbor peer-group-name peer-group</code>	BGP ピア グループを作成します。
ステップ 4	<code>neighbor ip-address peer-group peer-group-name</code>	BGP ネイバーをピア グループのメンバーにします。
ステップ 5	<code>neighbor {ip-address peer-group-name} remote-as number</code>	BGP ネイバーを指定します。 remote-as number を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ~ 65535 です。
ステップ 6	<code>neighbor {ip-address peer-group-name} description text</code>	(任意) ネイバーに記述子を関連付けます。
ステップ 7	<code>neighbor {ip-address peer-group-name} default-originate [route-map map-name]</code>	(任意) BGP スピーカー (ローカル ルータ) にネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、このルートがデフォルトルートとして使用されるようにします。
ステップ 8	<code>neighbor {ip-address peer-group-name} send-community</code>	(任意) この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 9	<code>neighbor {ip-address peer-group-name} update-source interface</code>	(任意) IBGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。

■ BGP の設定

	コマンド	目的
ステップ 10	neighbor { <i>ip-address</i> <i>peer-group-name</i> } ebgp-multihop	(任意) ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピアアドレスへの唯一のルートがデフォルトルート (0.0.0.0) の場合、マルチホップセッションは確立されません。
ステップ 11	neighbor { <i>ip-address</i> <i>peer-group-name</i> } local-as <i>number</i>	(任意) ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ~ 65535 です。
ステップ 12	neighbor { <i>ip-address</i> <i>peer-group-name</i> } advertisement-interval <i>seconds</i>	(任意) BGP ルーティングアップデートを送信する最小インターバルを設定します。
ステップ 13	neighbor { <i>ip-address</i> <i>peer-group-name</i> } maximum-prefix <i>maximum</i> [<i>threshold</i>]	(任意) ネイバーから受信できるプレフィックス数を制御します。指定できる範囲は 1 ~ 4294967295 です。 <i>threshold</i> (任意) は、警告メッセージが生成される基準となる最大値 (パーセンテージ) です。デフォルトは 75% です。
ステップ 14	neighbor { <i>ip-address</i> <i>peer-group-name</i> } next-hop-self	(任意) ネイバー宛での BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。
ステップ 15	neighbor { <i>ip-address</i> <i>peer-group-name</i> } password <i>string</i>	(任意) TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>map-name</i> { in out }	(任意) 着信または発信ルートにルートマップを適用します。
ステップ 17	neighbor { <i>ip-address</i> <i>peer-group-name</i> } send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES 属性を指定します。
ステップ 18	neighbor { <i>ip-address</i> <i>peer-group-name</i> } timers <i>keepalive holdtime</i>	(任意) ネイバーまたはピア グループ用のタイマーを設定します。 <ul style="list-style-type: none"> <i>keepalive</i> インターバルは、キープアライブメッセージがピアに送信される間隔です。指定できる範囲は 1 ~ 4294967295 秒です。デフォルト値は 60 秒です。 <i>holdtime</i> は、キープアライブメッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲は 1 ~ 4294967295 秒です。デフォルト値は 180 秒です。
ステップ 19	neighbor { <i>ip-address</i> <i>peer-group-name</i> } weight <i>weight</i>	(任意) ネイバーからのすべてのルートに関する重みを指定します。
ステップ 20	neighbor { <i>ip-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-number</i> <i>name</i> } { in out }	(任意) アクセスリストの指定に従って、ネイバーに対して送受信される BGP ルーティングアップデートをフィルタリングします。
ステップ 21	neighbor { <i>ip-address</i> <i>peer-group-name</i> } filter-list <i>access-list-number</i> { in out weight <i>weight</i> }	(任意) BGP フィルタを確立します。
ステップ 22	neighbor { <i>ip-address</i> <i>peer-group-name</i> } version <i>value</i>	(任意) ネイバーと通信するとき使用する BGP バージョンを指定します。
ステップ 23	neighbor { <i>ip-address</i> <i>peer-group-name</i> } soft-reconfiguration inbound	(任意) 受信したアップデートのストアを開始するようにソフトウェアを設定します。
ステップ 24	end	特権 EXEC モードに戻ります。
ステップ 25	show ip bgp neighbors	設定を確認します。
ステップ 26	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存の BGP ネイバーまたはネイバー ピア グループをディセーブルにするには、**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。ディセーブル化されている既存のネイバーまたはネイバー ピア グループをイネーブルにするには、**no neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。

集約アドレスの設定

CIDR を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティング テーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング テーブル内に集約アドレスを作成するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router bgp <i>autonomous-system</i>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	aggregate-address <i>address mask</i>	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約属性が設定されます。
ステップ 4	aggregate-address <i>address mask as-set</i>	(任意) AS 設定パス情報を生成します。このコマンドは、この前のコマンドと同じルールに従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、アップデートされます。
ステップ 5	aggregate-address <i>address-mask summary-only</i>	(任意) サマリー アドレスだけをアドバタイズします。
ステップ 6	aggregate-address <i>address mask suppress-map <i>map-name</i></i>	(任意) 選択された、より具体的なルートを抑制します。
ステップ 7	aggregate-address <i>address mask advertise-map <i>map-name</i></i>	(任意) ルート マップによって指定された設定に基づいて、集約を生成します。
ステップ 8	aggregate-address <i>address mask attribute-map <i>map-name</i></i>	(任意) ルート マップで指定された属性を持つ集約を生成します。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show ip bgp neighbors [<i>advertised-routes</i>]	設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

集約エントリを削除するには、**no aggregate-address *address mask*** ルータ コンフィギュレーション コマンドを使用します。オプションをデフォルト値に戻すには、キーワードを指定してコマンドを使用します。

ルーティング ドメイン連合の設定

IBGP メッシュを削減する方法の 1 つは、AS を複数のサブ AS に分割して、単一の AS として認識される単一の連合にグループ化することです。各 AS は内部で完全にメッシュ化されていて、同じ連合内の他の AS との間には数本の接続があります。異なる AS 内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。特に、ネクスト ホップ、MED、およびローカル初期設定情報が維持されるため、すべての AS で単一の IGP を使用できます。

BGP 連合を設定するには、AS システム グループの AS 番号として機能する連合 ID を指定する必要があります。

BGP 連合を設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bgp confederation identifier autonomous-system</code>	BGP 連合 ID を設定します。
ステップ 4	<code>bgp confederation peers autonomous-system [autonomous-system ...]</code>	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp neighbor</code> <code>show ip bgp network</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートを実際の内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから学習されたルートを実際の内部ネイバーに送信しません。

ルート リフレクタを使用すると、学習されたルートを実際のネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。IBGP ピアをルート リフレクタに設定すると、その IBGP ピアは IBGP によって学習されたルートを一連の IBGP ネイバーに送信するようになります。ルート リフレクタの内部ピアには、クライアント ピアと非クライアント ピア (AS 内の他のすべてのルータ) の 2 つのグループがあります。ルート リフレクタは、これらの 2 つのグループ間でルートを実際のネイバーに送信させます。ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- EBGP スピーカーからのルートを実際のクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートを実際のクライアントにアドバタイズします。
- クライアントからのルートを実際のクライアントおよび非クライアント ピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルートリフレクタが 1 つあり、クラスタはルートリフレクタのルート ID で識別されます。冗長性を高めて、シングルポイントでの障害を回避するには、クラスタに複数のルートリフレクタを設定する必要があります。このように設定した場合は、ルートリフレクタが同じクラスタ内のルートリフレクタからのアップデートを認識できるように、クラスタ内のすべてのルートリフレクタに同じクラスタ ID (4 バイト) を設定する必要があります。クラスタを処理するすべてのルートリフレクタは完全メッシュ構造にし、一連の同一なクライアントピアおよび非クライアントピアを設定する必要があります。

ルートリフレクタおよびクライアントを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>neighbor ip-address peer-group-name route-reflector-client</code>	ローカル ルータを BGP ルートリフレクタに、指定されたネイバーをクライアントに設定します。
ステップ 4	<code>bgp cluster-id cluster-id</code>	(任意) クラスタに複数のルートリフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	<code>no bgp client-to-client reflection</code>	(任意) クライアント間のルート反映をディセーブルにします。デフォルトでは、ルートリフレクタクライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルートリフレクタはルートをクライアントに反映させる必要がありません。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip bgp</code>	設定を確認します。送信元の ID およびクラスタリスト属性を表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート ダンプニングの設定

ルートフラップ ダンプニングは、インターネットワーク内でフラッピング ルートの伝播を最小化するための BGP 機能です。ルートがフラッピングと見なされるのは、ルートが使用可能、使用不可能、使用可能、使用不可能のように、状態が継続的に変化する場合があります。ルート ダンプニングがイネーブルの場合は、フラッピングしているルートに *penalty* 値が割り当てられます。ルートの累積ペナルティが、設定された制限値に到達すると、ルートが稼働している場合であっても、BGP はルートのアドバタイズメントを抑制します。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプニングが適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

BGP ルート ダンプニングを設定するには、EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bgp dampening</code>	BGP ルート ダンプニングをイネーブルにします。

	コマンド	目的
ステップ 4	bgp dampening <i>half-life reuse suppress max-suppress [route-map map]</i>	(任意) ルート ダンプニング係数のデフォルト値を変更します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip bgp flap-statistics [<i>{regexp regexp}</i>] [<i>{filter-list list}</i>] [<i>{address mask [longer-prefix]}</i>]	(任意) フラッピングしているすべてのパスのフラップを監視します。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 7	show ip bgp dampened-paths	(任意) 抑制されるまでの時間を含めて、減衰されたルートを表示します。
ステップ 8	clear ip bgp flap-statistics [<i>{regexp regexp}</i>] [<i>{filter-list list}</i>] [<i>{address mask [longer-prefix]}</i>]	(任意) BGP フラップ統計情報を消去して、ルートが減衰される可能性を小さくします。
ステップ 9	clear ip bgp dampening	(任意) ルート ダンプニング情報を消去して、ルートの抑制を解除します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フラップ ダンプニングをディセーブルにするには、キーワードを指定しないで **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。ダンプニング係数をデフォルト値に戻すには、値を指定して **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。

BGP のモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティング パスを検出することもできます。

表 41-8 に、BGP を消去および表示するために使用する特権 EXEC コマンドを示します。表示フィールドの詳細については、Cisco.com のホーム ページにアクセスして、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References])。]

表 41-11 IP BGP の clear および show コマンド

コマンド	目的
clear ip bgp address	特定の BGP 接続をリセットします。
clear ip bgp *	すべての BGP 接続をリセットします。
clear ip bgp peer-group tag	BGP ピア グループのすべてのメンバーを削除します。
show ip bgp prefix	プレフィックスがアドバタイズされるピア グループ、またはピア グループに含まれないピアを表示します。ネクスト ホップやローカルプレフィックスなどのプレフィックス属性も表示されます。
show ip bgp cidr-only	サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
show ip bgp community [community-number] [exact]	指定されたコミュニティに属するルートを表示します。
show ip bgp community-list community-list-number [exact-match]	コミュニティ リストで許可されたルートを表示します。

表 41-11 IP BGP の clear および show コマンド (続き)

コマンド	目的
<code>show ip bgp filter-list access-list-number</code>	指定された AS パス アクセス リストによって照合されたルートを表示します。
<code>show ip bgp inconsistent-as</code>	送信元の AS と矛盾するルートを表示します。
<code>show ip bgp regexp regular-expression</code>	コマンドラインに入力された特定の正規表現と一致する AS パスを持つルートを表示します。
<code>show ip bgp</code>	BGP ルーティング テーブルの内容を表示します。
<code>show ip bgp neighbors [address]</code>	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
<code>show ip bgp neighbors [address] [advertised-routes dampened-routes flap-statistics paths regular-expression received-routes routes]</code>	特定の BGP ネイバーから取得されたルートを表示します。
<code>show ip bgp paths</code>	データベース内のすべての BGP パスを表示します。
<code>show ip bgp peer-group [tag] [summary]</code>	BGP ピア グループに関する情報を表示します。
<code>show ip bgp summary</code>	すべての BGP 接続のステータスを表示します。

また、`bgp log-neighbor changes` ルータ コンフィギュレーション コマンドを使用し、BGP ネイバーをリセット、起動、またはダウンさせるときに生成されるメッセージのログギングをイネーブルにすることもできます。

ISO CLNS ルーティングの設定

International Organization for Standardization (ISO; 国際標準化機構) Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) プロトコルとは、Open System Interconnection (OSI; オープン システム インターコネクション) モデルのネットワーク層の標準の 1 つです。ISO ネットワーク アーキテクチャ内のアドレスは、Network Service Access Point (NSAP; ネットワーク サービス アクセス ポイント) アドレスおよび Network Entity Titles (NETs) と呼ばれます。OSI ネットワークの各ノードには、1 つ以上の NETs が含まれます。さらに、各ノードには、多数の NSAP アドレスが含まれます。

スイッチ上で、`clns routing` グローバル コンフィギュレーション コマンドを使用してコネクションレス型ルーティングをイネーブルにすると、スイッチはルーティング関連の機能を果たさず、転送の決定だけを行います。ダイナミック ルーティングには、ルーティング プロトコルもイネーブルにする必要があります。スイッチは、Intermediate System-to-Intermediate System (IS-IS) ダイナミック ルーティング プロトコルをサポートします。このプロトコルは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づいています。

動的にルーティングを行う場合は、IS-IS を使用します。このルーティング プロトコルは、エリアの概念をサポートします。1 つのエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータは適切なエリアに到達する方法を認識しています。IS-IS は、ステーションルーティング (1 つのエリア内) およびエリアルーティング (エリア間) という 2 つのレベルのルーティングをサポートします。

ISO IGRP と IS-IS NSAP アドレス方式の主な違いは、エリア アドレスの定義にあります。両方ともレベル 1 ルーティング (1 つのエリア内) にはシステム ID を使用します。ただし、エリアルーティングに関してアドレスが指定される方法が異なります。ISO IGRP NSAP アドレスには、ドメイン、エリ

ア、およびシステム ID という 3 つの異なるフィールドが含まれます。IS-IS アドレスには、単一の連続的エリアフィールド（ドメインフィールドおよびエリアフィールドから成る）とシステム ID という 2 つのフィールドが含まれます。



(注)

ISO CLNS の詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.2』を参照してください。この章で使用されるコマンドの構文および使用方法の詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2』を参照するか、IOS コマンドリファレンスのマスターインデックスを使用するか、またはオンラインで検索してください。

IS-IS ダイナミック ルーティングの設定

IS-IS は、ISO ダイナミック ルーティング プロトコルの 1 つです (ISO 105890 で説明されている)。その他のルーティング プロトコルとは異なり、IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS コンフィギュレーション構文を使用することで、レイヤ 3 スイッチまたはルータごとに複数の IS-IS ルーティング プロトコルを指定できます。その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内にすべてのルータが含まれる単一のエリアとして構築されます。ネットワークの規模が大きくなるに従って、このネットワークは、すべてのエリアに属する、接続されたすべてのレベル 2 ルータのセットから構成されるバックボーン エリア内に再編成され、その後、このネットワークはローカルエリアに接続されます。1 つのローカルエリア内部では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を認識しており、バックボーン ルータは他のエリアに到達する方法を認識しています。

ルータは、ローカル エリア内でルーティングを実行するために、レベル 1 の隣接関係を確立します (ステーションルーティング)。ルータは、レベル 1 のエリア間でルーティングを実行するために、レベル 2 の隣接関係を確立します (エリアルーティング)。

1 つの Cisco ルータは、最大 29 エリアのルーティングに参加でき、バックボーンでレベル 2 ルーティングを実行できます。一般に、ルーティング プロセスごとに 1 つのエリアに対応します。デフォルトでは、ルーティング プロセスの最初のインスタンスが、レベル 1 およびレベル 2 両方のルーティングを実行するように設定されます。追加のルーティング インスタンスを設定できます。このインスタンスは、自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスの各インスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングでは、シスコの各装置に対して最大 29 個のレベル 1 エリアを定義できますが、レベル 2 ルーティングを実行するプロセスは 1 つだけ設定できます。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。同時に、このプロセスがレベル 1 ルーティングを実行するように設定することもできます。ルータ インスタンスにレベル 2 ルーティングが必要でない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 の機能を削除します。別のルータ インスタンスをレベル 2 ルータとして設定する場合にも **is-type** コマンドを使用します。



(注)

IS-IS の詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Routing Protocols」の章を参照してください。ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS IP Command Reference, Release 12.2』を参照してください。

ここでは、IS-IS ルーティングの設定方法を簡単に説明します。内容は次のとおりです。

- 「IS-IS のデフォルト設定」 (P.41-67)
- 「IS-IS ルーティングのイネーブル化」 (P.41-68)
- 「IS-IS グローバル パラメータの設定」 (P.41-70)
- 「IS-IS インターフェイス パラメータの設定」 (P.41-73)

IS-IS のデフォルト設定

表 41-12 に、IS-IS のデフォルト設定を示します。

表 41-12 IS-IS のデフォルト設定

機能	デフォルト設定
リンクステート PDU (LSP) エラーを無視	イネーブル。
IS-IS タイプ	従来型の IS-IS : ルータは、レベル 1 (ステーション) とレベル 2 (エリア) 両方のルータとして機能します。 マルチエリア IS-IS : IS-IS ルーティング プロセスの最初のインスタンスがレベル 1-2 ルータです。残りのインスタンスは、レベル 1 ルータです。
デフォルト情報送信元	ディセーブル
IS-IS 隣接関係のステート変更を記録	ディセーブル
LSP 生成スロットリング タイマー	連続で生成した 2 つの間の最大インターバル : 5 秒 初期 LSP 生成遅延 : 50 ミリ秒 1 番目と 2 番目の LSP 生成間のホールドタイム : 5000 ミリ秒
LSP 最大ライフ タイム (リフレッシュなし)	LSP パケットが削除されるまで 1200 秒 (20 分)
LSP リフレッシュ インターバル	LSP リフレッシュを 900 秒 (15 分) ごとに送信
最大 LSP パケット サイズ	1497 バイト
NSF 認識 ¹	イネーブル。レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、隣接する NSF 対応ルータからのパケットを転送し続けることができます。
Partial Route Computation (PRC; 部分ルート計算) スロットリング タイマー	最大 PRC 待機インターバル : 5 秒 トポロジの変更後の初期 PRC 計算遅延 : 2000 ミリ秒 1 番目と 2 番目の PRC 計算間のホールドタイム : 5000 ミリ秒
パーティション回避	ディセーブル
パスワード	エリアまたはドメインのパスワードが定義されておらず、認証はディセーブルになっています。
過負荷ビットの設定	ディセーブル。イネーブルの際に引数が入力されない場合、過負荷ビットがただちに設定され、 no set-overload-bit コマンドが入力されるまで設定されたままになります。
Shortest Path First (SPF) スロットリング タイマー	連続した SFP 間の最大インターバル : 10 秒 トポロジの変更後の初期 SPF 計算 : 5500 ミリ秒 1 番目と 2 番目の SPF 計算間のホールドタイム : 5500 ミリ秒
サマリー アドレス	ディセーブル

1. NSF = Nonstop Forwarding。

NSF 認識

統合型 IS-IS NSF 認識機能は IPv4 でサポートされています。この機能により、NSF を認識する顧客宅内装置 (CPE) ルータが、NSF 対応ルータによるパケットのノンストップ転送を実現します。ローカルルータでは、必ずしも NSF を実行している必要はありませんが、このルータが NSF を認識していると、スイッチオーバー プロセス時にルーティング データベースの整合性と精度、および隣接 NSF 対応ルータ上のリンクステート データベースが保持されます。

この機能は、自動的にイネーブルにされ、設定は必要ありません。この機能の詳細については、次の URL にある『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a00801541c7.s.html

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、各ルーティング プロセスに名前と NET を指定します。その後、インターフェイス上で IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

IS-IS をイネーブルにし、IS-IS ルーティング プロセスの各インターフェイスにエリアを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clns routing</code>	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	<code>router isis [area tag]</code>	指定したルーティング プロセスに対して IS-IS ルーティング プロセスをイネーブルにし、IS-IS ルーティング コンフィギュレーション モードを開始します。 (任意) <code>area tag</code> 引数を使用して、IS-IS ルータが割り当てられているエリアを特定します。複数の IS-IS エリアを設定する場合は、値を入力する必要があります。 最初に設定された IS-IS インスタンスは、デフォルトでレベル 1-2 です。後のインスタンスは、自動的にレベル 1 になります。 <code>is-type</code> グローバル コンフィギュレーション コマンドを使用してルーティングのレベルを変更できます。
ステップ 4	<code>net network-entity-title</code>	ルーティング プロセスに NET を設定します。マルチエリア IS-IS を設定する場合、各ルーティング プロセスに NET を指定します。NET およびアドレスに対して名前を指定できます。
ステップ 5	<code>is-type {level-1 level-1-2 level-2-only}</code>	(任意) ルータは、レベル 1 (ステーション) ルータ、マルチエリア ルーティング用のレベル 2 (エリア) ルータ、または両方 (デフォルト) として設定できます。 <ul style="list-style-type: none"> • level-1 : ステーション ルータとしてだけ機能 • level-1-2 : ステーションおよびエリア ルータの両方として機能 • level 2 : エリア ルータだけとして機能
ステップ 6	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 7	<code>interface interface-id</code>	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、 no switchport コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 8	<code>ip router isis [area tag]</code>	インターフェイス上の ISO CLNS に対して IS-IS ルーティング プロセスを設定し、ルーティング プロセスにエリア デジグネータを接続します。
ステップ 9	<code>clns router isis [area tag]</code>	インターフェイス上で ISO CLNS をイネーブルにします。
ステップ 10	<code>ip address ip-address-mask</code>	インターフェイスの IP アドレスを定義します。インターフェイスのいずれかが IS-IS ルーティングに設定されている場合は、イネーブルになっているエリアに含まれるすべてのインターフェイスで IP アドレスが必要です。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show isis [area tag] database detail</code>	設定を確認します。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IS-IS ルーティングをディセーブルにするには、**no router isis area-tag** ルータ コンフィギュレーション コマンドを使用します。

次に、従来型の IS-IS を IP ルーティング プロトコルとして実行するために 3 つのルータを設定する方法を示します。従来型の IS-IS では、すべてのルータはレベル 1 およびレベル 2 のルータとして機能します (デフォルト)。

ルータ A

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ B

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ C

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/1
```

```
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

IS-IS グローバルパラメータの設定

設定可能ないくつかのオプションの IS-IS グローバルパラメータを次に示します。

- ルートマップによって制御されるデフォルトルートを設定することで、デフォルトルートを IS-IS ルーティングドメイン内に強制的に設定できます。ルートマップで設定可能な、その他のフィルタリングオプションも指定できます。
- 内部チェックサムエラーとともに受信された IS-IS LSP を無視したり、破損した LSP を消去するようにルータを設定できます。これにより、LSP の発信側は、LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てられます。
- サマリーアドレスを使用して、ルーティングテーブル内に表示される集約アドレスを作成できます（経路集約）。他のルーティングプロトコルから学習したルートも集約できます。サマリーをアドバタイズするのに使用されるメトリックは、すべての個別ルートにおける最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュインターバルおよび LSP がリフレッシュなしでルータデータベース内にとどまることができる最大時間を設定できます。
- LSP 生成に対するスロットリングタイマー、最短パス優先計算、および部分ルート計算を設定できます。
- IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、スイッチがログメッセージを生成するように設定できます。
- ネットワーク内のリンクが、1500 バイト未満の Maximum Transmission Unit (MTU; 最大伝送単位) サイズの場合、それでもルーティングが行われるように LSP MTU の値を低くできます。
- パーティション回避ルータ コンフィギュレーション コマンドは、レベル 1-2 境界ルータ、隣接レベル 1 ルータ、およびエンドホスト間で完全な接続が失われた場合に、エリアがパーティション化されるのを防ぎます。

IS-IS パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clns routing</code>	スイッチ上で ISO コネクションレス型ルーティングをイネーブルに設定します。
ステップ 3	<code>router isis</code>	IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	<code>default-information originate [route-map map-name]</code>	(任意) デフォルトルートを IS-IS ルーティングドメイン内に強制的に設定します。 <code>route-map map-name</code> を入力すると、ルートマップが満たされると、ルーティングプロセスがデフォルトルートを生成します。

	コマンド	目的
ステップ 5	ignore-lsp-errors	(任意) LSP を消去する代わりに、内部チェックサムにエラーがある LSP を無視するようにルータを設定します。このコマンドは、デフォルトでイネーブルになっています (破損した LSP はドロップされます)。破損した LSP を消去するには、 no ignore-lsp-errors ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	area-password password	(任意) レベル 1 (ステーション ルータ レベル) LSP に挿入されるエリア認証パスワードを設定します。
ステップ 7	domain-password password	(任意) レベル 2 (エリア ルータ レベル) LSP に挿入されるルーティングドメイン認証パスワードを設定します。
ステップ 8	summary-address address mask [level-1 level-1-2 level-2]	(任意) 所定のレベルのアドレスのサマリーを作成します。
ステップ 9	set-overload-bit [on-startup { <i>seconds</i> wait-for-bgp }]	(任意) ルータに問題がある場合に、他のルータが Shortest Path First (SPF; 最短パス優先) 計算でこのルータを無視するように過負荷ビット (hippity ビット) を設定します。 <ul style="list-style-type: none"> • (任意) on-startup : 起動時だけ過負荷ビットを設定します。on-startup が指定されない場合、過負荷ビットが即座に設定され、no set-overload-bit コマンドを入力するまで設定されたままになります。on-startup が指定された場合、秒数または wait-for-bgp を入力する必要があります。 • seconds : on-startup キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、この秒数の間設定されたままになります。指定できる範囲は 5 ~ 86400 秒です。 • wait-for-bgp : on-startup キーワードが設定されている場合、システム起動時に過負荷ビットが設定されて、BGP が収束するまで設定されたままになります。BGP が収束されたことが IS-IS に通知されない場合、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	lsp-refresh-interval seconds	(任意) LSP リフレッシュ インターバル (秒) を設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルトでは、LSP リフレッシュを 900 秒 (15 分) ごとに送信します。
ステップ 11	max-lsp-lifetime seconds	(任意) LSP パケットがリフレッシュされずにルータ データベース内に継続する最大時間を設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は 1200 秒 (20 分) です。指定されたタイム インターバルのあと、LSP パケットは削除されます。
ステップ 12	lsp-gen-interval [level-1 level-2] <i>lsp-max-wait</i> [<i>lsp-initial-wait</i> <i>lsp-second-wait</i>]	(任意) IS-IS 生成スロットリング タイマーを設定します。 <ul style="list-style-type: none"> • <i>lsp-max-wait</i> : 2 つの連続する LSP 生成間の最大インターバル (秒)。指定できる範囲は 1 ~ 120 秒です。デフォルト値は 5 秒です。 • <i>lsp-initial-wait</i> : 最初の LSP 生成遅延 (ミリ秒)。指定できる範囲は 1 ~ 10000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • <i>lsp-second-wait</i> : 最初と 2 番目の LSP 生成間 (ミリ秒) のホールドタイム。指定できる範囲は 1 ~ 10000 ミリ秒です。デフォルト値は 5000 ミリ秒です。

	コマンド	目的
ステップ 13	spf-interval [level-1 level-2] <i>spf-max-wait</i> [<i>spf-initial-wait</i> <i>spf-second-wait</i>]	(任意) IS-IS SPF スロットリング タイマーを設定します。 <ul style="list-style-type: none"> <i>spf-max-wait</i> : 連続する SFP 間 (秒) の最大インターバル。指定できる範囲は 1 ~ 120 で、デフォルトは 10 です。 <i>spf-initial-wait</i> : トポロジ変更後の最初の SFP 計算 (ミリ秒)。指定できる範囲は 1 ~ 10000 で、デフォルトは 5500 です。 <i>spf-second-wait</i> : 最初と 2 番めの SFP 計算間 (ミリ秒) のホールドタイム。指定できる範囲は 1 ~ 10000 で、デフォルトは 5500 です。
ステップ 14	prc-interval <i>prc-max-wait</i> [<i>prc-initial-wait</i> <i>prc-second-wait</i>]	(任意) IS-IS PRC スロットリング タイマーを設定します。 <ul style="list-style-type: none"> <i>prc-max-wait</i> : 2 つの連続する PRC 計算間の最大インターバル (秒)。指定できる範囲は 1 ~ 120 秒です。デフォルト値は 5 秒です。 <i>prc-initial-wait</i> : トポロジ変更後の最初の PRC 計算遅延 (ミリ秒)。指定できる範囲は 1 ~ 10,000 ミリ秒です。デフォルト値は 2000 ミリ秒です。 <i>prc-second-wait</i> : 最初と 2 番めの PRC 計算間 (ミリ秒) のホールドタイム。指定できる範囲は 1 ~ 10,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
ステップ 15	log-adjacency-changes [all]	(任意) IS-IS 隣接ステート変更をログするようルータを設定します。End System-to-Intermediate System PDU および Link State Packet (LSP; リンクステート パケット) など、IS-IS Hello に関連しないイベントにより生成されたすべての変更をログに含めるには、 all を入力します。
ステップ 16	lsp-mtu size	(任意) 最大 LSP パケット サイズ (バイト) を指定します。指定できる範囲は 128 ~ 4352 バイトです。デフォルト値は 1497 バイトです。 (注) ネットワーク内の任意のリンクで MTU サイズが縮小された場合、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17	partition avoidance	(任意) 境界ルータ、すべての隣接レベル 1 ルータ、およびエンド ホスト間で、フル接続が切断された場合、IS-IS レベル 1-2 境界ルータがレベル 1 エリア プレフィックスをレベル 2 バックボーンにアダプタイズしないようにします。
ステップ 18	end	特権 EXEC モードに戻ります。
ステップ 19	show clns	設定を確認します。
ステップ 20	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ルート生成をディセーブルにするには、**no default-information originate** ルータ コンフィギュレーション コマンドを使用します。**no area-password** または **no domain-password** ルータ コンフィギュレーション コマンドを使用して、パスワードをディセーブルにします。LSP MTU 設定をディセーブルにするには、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレス指定、LSP リフレッシュ インターバル、LSP ライフタイム、LSP タイマー、SPF タイマー、および PRC タイマーをデフォルト状態に戻すには、コマンドの **no** 形式を使用します。**no partition avoidance** ルータ コンフィギュレーション コマンドを使用して、出力形式をディセーブルにします。

IS-IS インターフェイス パラメータの設定

任意で、特定のインターフェイス固有の IS-IS パラメータを、付加されている他のルータとは別に設定できます。ただし、一部の値（乗数およびタイム インターバルなど）をデフォルトから変更する場合、複数のルータおよびインターフェイス上でもこれを変更する必要があります。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、またはその両方で設定できます。

次に、設定可能なインターフェイス レベル パラメータの一部を示します。

- インターフェイスのデフォルト メトリック：QoS ルーティングが実行されない場合に、IS-IS メトリックの値として使用され、割り当てられます。
- hello インターバル（インターフェイスから送信される hello パケットの間隔）またはデフォルトの hello パケット乗数：インターフェイス上で使用されて、IS-IS hello パケットで送信されるホールドタイムを決定します。ホールドタイムは、ネイバーがダウンしていると宣言するまでに、別の hello パケットを待機する時間を決定します。これにより、障害リンクまたはネイバーが検出される速さも決定し、ルートを再計算できるようになります。hello パケットが頻繁に損失され、IS-IS 隣接で不要に障害が発生する場合は、hello 乗数を変更します。hello 乗数を大きくし、それに対応して hello インターバルを小さくすると、リンク障害を検出するのに必要な時間を増やすことなく、hello プロトコルの信頼性を高めることができます。
- その他のタイム インターバル：
 - Complete Sequence Number PDU (CSNP) インターバル CSNP は、指定ルータにより送信され、データベースの同期を維持します。
 - 再送信インターバル。これは、ポイントツーポイントリンクの IS-IS LSP の再送信間隔です。
 - IS-IS LSP 再送信スロットル インターバル。これは、IS-IS LSP がポイントツーポイントリンクで再送信される最大レート（パケット間のミリ秒数）です。このインターバルは、同じ LSP が連続する再送信間隔である再送信インターバルとは異なります。
- 指定ルータの選択プライオリティ：マルチアクセス ネットワークに必要な隣接数を削減し、その代わりに、ルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズを削減できます。
- インターフェイス回線タイプ：指定されたインターフェイス上のネイバーに必要な隣接タイプです。
- インターフェイスのパスワード認証

IS-IS インターフェイス パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがまだレイヤ 3 インターフェイスとして設定されていない場合は、 no switchport コマンドを入力し、インターフェイスをレイヤ 3 モードにします。
ステップ 3	<code>isis metric default-metric [level-1 level-2]</code>	(任意) 指定したインターフェイスにメトリック（またはコスト）を設定します。指定できる範囲は 0 ~ 63 です。デフォルトは 10 です。レベルが入力されない場合は、レベル 1 およびレベル 2 ルータの両方にデフォルト値が適用されます。

コマンド	目的
ステップ 4 isis hello-interval { <i>seconds</i> minimal } [level-1 level-2]	(任意) スイッチが hello パケットを送信する間隔を指定します。デフォルトでは、 hello インターバル <i>seconds</i> の 3 倍の値が、送信される hello パケットの <i>holdtime</i> としてアドバタイズされます。 hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティングトラフィック量は増大します。 <ul style="list-style-type: none"> • minimal : ホールドタイムが 1 秒になるように、システムが hello 乗数に基づいて hello インターバルを計算するようにします。 • <i>seconds</i> : 指定できる範囲は、1 ~ 65,535 秒です。デフォルトは 10 秒です。
ステップ 5 isis hello-multiplier <i>multiplier</i> [level-1 level-2]	(任意) ルータが隣接装置のダウンを宣言するまでに、ネイバーが損失する IS-IS hello パケット数を指定します。指定できる範囲は 3 ~ 1000 です。デフォルトは 3 です。 hello 乗数を小さくすると、高速コンバージェンスとなりますが、ルーティングが不安定になる場合があります。
ステップ 6 isis csnp-interval <i>seconds</i> [level-1 level-2]	(任意) インターフェイスに IS-IS CSNP を設定します。指定できる範囲は 0 ~ 65535 です。デフォルト値は 10 秒です。
ステップ 7 isis retransmit-interval <i>seconds</i>	(任意) ポイントツーポイントリンクの IS-IS LSP の再送信間隔 (秒) を設定します。指定する値は、ネットワーク上の任意の 2 つのルータ間の予測ラウンドトリップ遅延よりも大きい整数である必要があります。指定できる範囲は 0 ~ 65535 です。デフォルトは 5 秒です。
ステップ 8 isis retransmit-throttle-interval <i>milliseconds</i>	(任意) IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイントリンク上で再送信される最大レート (パケット間のミリ秒数) です。指定できる範囲は 0 ~ 65535 です。デフォルト値は、 isis lsp-interval コマンドにより決定します。
ステップ 9 isis priority <i>value</i> [level-1 level-2]	(任意) 指定ルータ選択で使用するプライオリティを設定します。指定できる範囲は 0 ~ 127 です。デフォルトは 64 です。
ステップ 10 isis circuit-type { level-1 level-1-2 level-2-only }	(任意) 指定されたインターフェイス上のネイバーに必要な隣接タイプを設定します (インターフェイスの回線タイプを指定します)。 <ul style="list-style-type: none"> • level-1 : このノードとネイバーの両方に共通のエリアアドレスが少なくとも 1 つある場合、レベル 1 隣接関係が確立されます。 • level-1-2 : ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、少なくとも 1 つの共通のエリアがある場合、レベル 1 およびレベル 2 隣接関係が確立されます。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルトです。 • level 2 : レベル 2 隣接関係が確立されます。隣接ルータがレベル 1 ルータである場合、隣接関係は確立されません。
ステップ 11 isis password <i>password</i> [level-1 level-2]	(任意) インターフェイスの認証パスワードを設定します。デフォルトでは、認証はディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれレベル 1 またはレベル 2 ルーティング用のパスワードだけがイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 およびレベル 2 です。
ステップ 12 end	特権 EXEC モードに戻ります。
ステップ 13 show clns interface <i>interface-id</i>	設定を確認します。
ステップ 14 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルト設定に戻るには、コマンドの **no** 形式を使用します。

ISO IGRP と IS-IS のモニタリングおよびメンテナンス

CLNS キャッシュのすべての内容または特定のネイバーまたはルートの情報を削除できます。ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の CLNS または IS-IS の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーに関する情報も表示できます。

表 41-13 に、ISO CLNS および IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。表示されるフィールドの詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2』を参照するか、Cisco IOS コマンドリファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

表 41-13 ISO CLNS と IS-IS の clear および show コマンド

コマンド	目的
<code>clear clns cache</code>	CLNS ルーティング キャッシュを消去して、再初期化します。
<code>clear clns es-neighbors</code>	隣接データベースから End System (ES) ネイバー情報を削除します。
<code>clear clns is-neighbors</code>	隣接データベースから Intermediate System (IS) ネイバー情報を削除します。
<code>clear clns neighbors</code>	隣接データベースから CLNS ネイバー情報を削除します。
<code>clear clns route</code>	ダイナミックに取得された CLNS ルーティング情報を削除します。
<code>show clns</code>	CLNS ネットワークについての情報を表示します。
<code>show clns cache</code>	CLNS ルーティング キャッシュのエントリを表示します。
<code>show clns es-neighbors</code>	関連するエリアを含む、ES ネイバー エントリを表示します。
<code>show clns filter-expr</code>	フィルタ式を表示します。
<code>show clns filter-set</code>	フィルタ セットを表示します。
<code>show clns interface [interface-id]</code>	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。
<code>show clns neighbor</code>	IS-IS ネイバーについての情報を表示します。
<code>show clns protocol</code>	このルータの IS-IS または ISO IGRP ルーティング プロセスごとにプロトコル固有の情報を表示します。
<code>show clns route</code>	このルータが認識している CLNS パケットのルーティング方法について、その宛先をすべて表示します。
<code>show clns traffic</code>	このルータが認識している CLNS パケットの情報を表示します。
<code>show ip route isis</code>	ISIS IP ルーティング テーブルの現在のステータスを表示します。
<code>show isis database</code>	IS-IS リンクステータス データベースを表示します。
<code>show isis routes</code>	IS-IS レベル 1 ルーティング テーブルを表示します。
<code>show isis spf-log</code>	IS-IS の SPF 計算履歴を表示します。
<code>show isis topology</code>	すべてのエリア内の接続されたルータすべてのリストを表示します。
<code>show route-map</code>	設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
<code>trace clns destination</code>	ネットワークのパケットが指定された宛先までに経由するパスを検出します。
<code>which-route {nsap-address clns-name}</code>	指定された CLNS 宛先が検出されたルーティング テーブルを表示します。

Multi-VRF CE の設定

Virtual Private Network (VPN; バーチャルプライベートネットワーク) は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。VPN は、共通ルーティングテーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VRF テーブルと呼ばれる VPN ルーティングテーブルと各インターフェイスを関連付けます。

IE 3000 スイッチは、IP サービス イメージを稼働している場合、カスタマー エッジ (CE) 装置の複数の VPN ルーティング/フォワーディング (multi-VRF) インスタンスをサポートします (multi-VRF CE)。サービス プロバイダーは、Multi-VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。



(注)

スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング (MPLS) が使用されません。MPLS VRF の詳細については、Cisco.com のホームページにアクセスして、『Cisco IOS Switching Services Configuration Guide, Release 12.2』を参照してください ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References])。

- 「Multi-VRF CE の概要」 (P.41-76)
- 「Multi-VRF CE のデフォルト設定」 (P.41-78)
- 「マルチ VRF CE の設定時の注意事項」 (P.41-78)
- 「VRF の設定」 (P.41-80)
- 「VRF 認識サービスの設定」 (P.41-81)
- 「VPN ルーティングセッションの設定」 (P.41-85)
- 「BGP PE/CE ルーティングセッションの設定」 (P.41-85)
- 「Multi-VRF CE の設定例」 (P.41-86)
- 「Multi-VRF CE ステータスの表示」 (P.41-90)

Multi-VRF CE の概要

Multi-VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。Multi-VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネットポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF に属することはできません。



(注)

Multi-VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

Multi-VRF CE には、次のデバイスが含まれます。

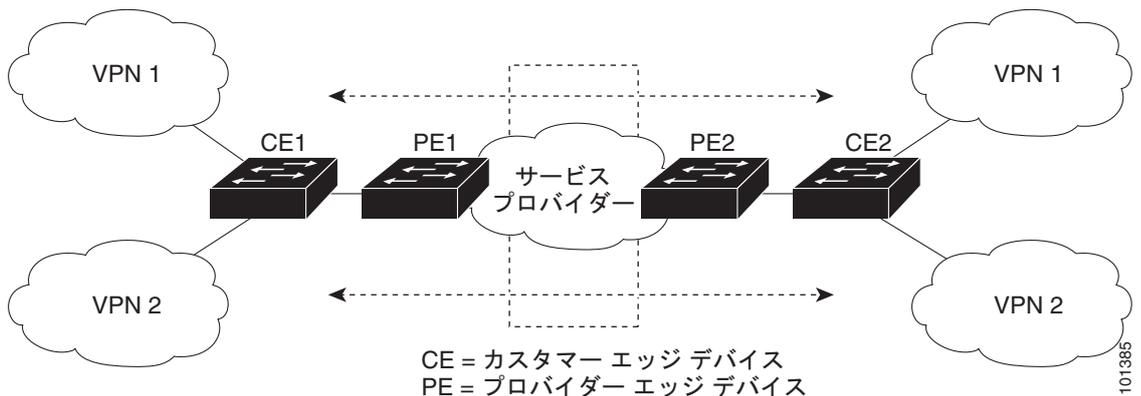
- お客様は、CE デバイスにより、1 つまたは複数のプロバイダー エッジ (PE) ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカルルートをルータにアドバタイズし、リモート VPN ルートをそこから学習します。IE 3000 スイッチは、CE に設定することができます。

- PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE では、直接接続している VPN の VPN ルートだけを維持すればよく、すべてのサービス プロバイダー VPN ルートを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイスに接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

Multi-VRF CE では、複数のお客様が 1 つの CE を共有でき、CE と PE の間で 1 つの物理リンクだけが使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。Multi-VRF CE は、制限付きの PE 機能を CE デバイスに拡張して、別々の VRF テーブルを維持し、VPN のプライバシーおよびセキュリティをブランチ オフィスに拡張します。

図 41-6 に、IE3000 スイッチを複数の仮想 CE として使用した構成例を示します。このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。この場合、IE3000 スイッチには multi-VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

図 41-6 複数の仮想 CE として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、Multi-VRF CE 関連のデータ構造で VLAN ID と Policy Label (PL) の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

Multi-VRF CE を設定すると、レイヤ 3 フォワーディング テーブルは、次の 2 つのセクションに概念的に分割されます。

- Multi-VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID はさまざまな PL にマッピングされ、処理中に VRF を区別するために使用されます。レイヤ 3 設定機能では、学習した新しい VPN ルートごとに、入力ポートの VLAN ID を使用して PL を取得し、Multi-VRF CE ルーティング セクションに PL および新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポート内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されます。

Multi-VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力 PL 番号に基づいてルーティング テーブルを検索します。ルートが見つかり、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかり、ルートは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかり、パケットを正しい隣接デバイスに転送します。
- CE は、出力 PE からパケットを受信すると、入力 PL を使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかり、パケットを VPN 内で転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が優先ルーティング プロトコルです。

Multi-VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ : VPN コミュニティのその他すべてのメンバーのリスト。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング : VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送 : VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

Multi-VRF CE のデフォルト設定

表 41-14 に、VRF のデフォルト設定を示します。

表 41-14 VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ : 8000 ギガビット イーサネット スイッチ : 12000
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

マルチ VRF CE の設定時の注意事項



(注) マルチ VRF CE を使用するには、IP サービス イメージをスイッチにインストールする必要があります。

ネットワークに VRF を設定する場合は、次の内容に注意してください。

- Multi-VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。
- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- マルチ VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。それぞれのお客様には独自の VLAN があります。
- Multi-VRF CE ではサポートされない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、Multi-VRF CE の使用と複数の CE の使用に違いはありません。図 41-6 では、複数の仮想レイヤ 3 インターフェイスが Multi-VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- IE3000 スイッチは、1 つのグローバル ネットワークと最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル (BGP、OSPF、RIP、およびスタティック ルーティング) を使用できます。ただし、次の理由から External BGP (EBGP) を使用することを推奨します。
 - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
 - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
 - BGP では、ルートの属性を CE に簡単に渡すことができます。
- Multi-VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- マルチ VRF CE 内のラインレート マルチキャスト転送をサポートしています。
- マルチキャスト VRF は、同一インターフェイス上でプライベート VLAN と共存することができません。
- 最大 1000 のマルチキャスト ルータがサポートされていて、すべての VRF で共有可能です。
- VRF を設定しない場合は、105 のポリシーを設定できます。
- VRF を 1 つでも設定する場合は、41 のポリシーを設定できます。
- 41 より多いポリシーを設定する場合は、VRF を設定できません。
- VRF とプライベート VLAN は相互に排他的です。プライベート VLAN では VRF をイネーブルにできません。同じように、VLAN インターフェイスで VRF が設定されている VLAN では、プライベート VLAN をイネーブルにできません。
- VRF とポリシーベース ルーティング (PBR) は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、PBR をイネーブルにはできません。

- VRF と Web Cache Communication Protocol (WCCP) は、スイッチ インターフェイス上で相互に排他的です。インターフェイスで WCCP がイネーブルになっているときは、VRF をイネーブルにはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、WCCP をイネーブルにはできません。

VRF の設定

1 つまたは複数の VRF を設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティングをイネーブルにします
ステップ 3	ip vrf vrf-name	VRF に名前を付けて VRF コンフィギュレーション モードを開始します。
ステップ 4	rd route-distinguisher	ルート識別子を指定し、VRF テーブルを作成します。AS 番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。
ステップ 5	route-target {export import both} route-target-ext-community	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルートターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。 <i>route-target-ext-community</i> は、ステップ 4 で入力した <i>route-distinguisher</i> と同一にする必要があります。
ステップ 6	import map route-map	(任意) ルート マップを VRF に関連付けます。
ステップ 7	interface interface-id	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッドポートまたは SVI に設定できます。
ステップ 8	ip vrf forwarding vrf-name	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show ip vrf [brief detail interfaces] [vrf-name]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf vrf-name** グローバル コンフィギュレーション コマンドを使用します。VRF からあるインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

マルチキャスト VRF の設定

VRF テーブル内でマルチキャストを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティング モードをイネーブルにします
ステップ 3	ip vrf vrf-name	VRF に名前を付けて VRF コンフィギュレーション モードを開始します。
ステップ 4	rd route-distinguisher	ルート識別子を指定し、VRF テーブルを作成します。AS 番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。
ステップ 5	route-target {export import both} route-target-ext-community	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。 route-target-ext-community は、ステップ 4 で入力した route-distinguisher と同一にする必要があります。
ステップ 6	import map route-map	(任意) ルート マップを VRF に関連付けます。
ステップ 7	ip multicast-routing vrf vrf-name distributed	(任意) VRF テーブルのグローバルなマルチキャスト ルーティングをイネーブルにします。
ステップ 8	interface interface-id	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 9	ip vrf forwarding vrf-name	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 10	ip address ip-address mask	レイヤ 3 インターフェイスに IP アドレスを設定します。
ステップ 11	ip pim sparse-dense mode	VRF に関連付けられたレイヤ 3 インターフェイスで PIM をイネーブルにします。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ip vrf [brief detail interfaces] [vrf-name]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『Cisco IOS IP Multicast Configuration Guide, Release 12.4』を参照してください。

VRF 認識サービスの設定

IP サービスはグローバル インターフェイスに設定可能で、グローバル ルーティング インスタンスで稼働します。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームに依存しないモジュールに実装されます。VRF とは、Cisco IOS 内の複数のルーティング インスタンスを意味します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。

- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

次のサービスは、VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル (SNMP)
- ホットスタンバイ ルータ プロトコル (HSRP)
- Syslog
- traceroute
- FTP および TFTP



(注) VRF 認識サービスは、ユニキャスト RPF (uRPF) またはネットワーク タイム プロトコル (NTP) ではサポートされません。

ARP のユーザ インターフェイス

ARP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

コマンド	目的
<code>show ip arp vrf vrf-name</code>	指定された VRF 内の ARP テーブルを表示します。

ping のユーザ インターフェイス

ping の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

コマンド	目的
<code>ping vrf vrf-name ip-host</code>	指定された VRF 内の ARP テーブルを表示します。

SNMP のユーザ インターフェイス

SNMP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server trap authentication vrf</code>	VRF 上のパケットの SNMP トラップをイネーブルにします。
ステップ 3	<code>snmp-server engineID remote <host> vrf <vpn instance> <engine-id string></code>	スイッチ上のリモート SNMP エンジンの名前を設定します。

	コマンド	目的
ステップ4	snmp-server host <host> vrf <vpn instance> traps <community>	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ5	snmp-server host <host> vrf <vpn instance> informs <community>	SNMP 情報動作の受信側を指定して、SNMP 情報の送信に使用される VRF テーブルを指定します。
ステップ6	snmp-server user <user> <group> remote <host> vrf <vpn instance> <security model>	SNMP アクセス用に、VRF 上にあるリモートホストの SNMP グループにユーザを追加します。
ステップ7	end	特権 EXEC モードに戻ります。

HSRP のユーザ インターフェイス

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが、確実に適切な IP ルーティング テーブルに追加されます。

HSRP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ3	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。
ステップ4	ip vrf forwarding <vrf-name>	インターフェイス上に VRF を設定します。
ステップ5	ip address ip address	インターフェイスの IP アドレスを入力します。
ステップ6	standby 1 ip ip address	HSRP をイネーブルにして、仮想 IP アドレスを設定します。
ステップ7	end	特権 EXEC モードに戻ります。

Syslog のユーザ インターフェイス

Syslog の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	logging on	ストレージルータ イベント メッセージのロギングをイネーブルにする、または一時的にディセーブルにします。
ステップ3	logging host ip address vrf vrf name	ロギングメッセージが送信される Syslog サーバのホストアドレスを指定します。
ステップ4	logging buffered logging buffered size debugging	内部バッファへのメッセージを記録します。
ステップ5	logging trap debugging	Syslog サーバに送信されるロギングメッセージを制限します。

	コマンド	目的
ステップ 6	<code>logging facility facility</code>	システム ロギング メッセージをロギング ファシリティに送信します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。

traceroute のユーザ インターフェイス

traceroute の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

	コマンド	目的
	<code>traceroute vrf vrf-name ipaddress</code>	VPN VRF 内の宛先アドレスを検索するため、その名前を指定します。

FTP および TFTP のユーザ インターフェイス

FTP および TFTP を VRF 認識とするには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイスに付加される VRF テーブルを使用する場合、E1/0 であれば、CLI `ip [t]ftp source-interface E1/0` を設定して、特定のルーティング テーブルを使用するよう [t]ftp に通知する必要があります。この例では、VRF テーブルが宛先 IP アドレスを検索するのに使用されます。これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。つまり、VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

FTP 接続の送信元 IP アドレスを指定するには、`ip ftp source-interface show` モード コマンドを使用します。接続が確立されているインターフェイスのアドレスを使用するには、`no` 形式のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip ftp source-interface interface-type interface-number</code>	FTP 接続の送信元 IP アドレスを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

TFTP 接続の送信元アドレスとして特定のインターフェイスの IP アドレスを指定するには、`ip tftp source-interface show` モード コマンドを使用します。デフォルトに戻るには、`no` 形式のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip tftp source-interface interface-type interface-number</code>	TFTP 接続の送信元 IP アドレスを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル (RIP、OSPF、EIGRP、BGP)、またはスタティック ルーティングで設定できます。ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。



(注) VRF インスタンス内部で EIGRP ルーティング プロセスが実行されるように設定するには、**autonomous-system autonomous-system-number** アドレス ファミリ コンフィギュレーション モード コマンドを入力して、自律システム番号を設定する必要があります。

VPN 内で OSPF を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id vrf vrf-name	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	log-adjacency-changes	(任意) 隣接状態の変更をログします。これがデフォルトの状態になります。
ステップ 4	redistribute bgp autonomous-system-number subnets	BGP ネットワークから OSPF ネットワークに情報を再配信するようにスイッチを設定します。
ステップ 5	network network-number area area-id	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip ospf process-id	OSPF ネットワークの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf process-id vrf vrf-name** グローバル コンフィギュレーション コマンドを使用します。

BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router bgp autonomous-system-number	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	network network-number mask network-mask	ネットワークとマスクを指定し、BGP の使用を宣言します。
ステップ 4	redistribute ospf process-id match internal	OSPF 内部ルートを再配信するようにスイッチを設定します。
ステップ 5	network network-number area area-id	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。

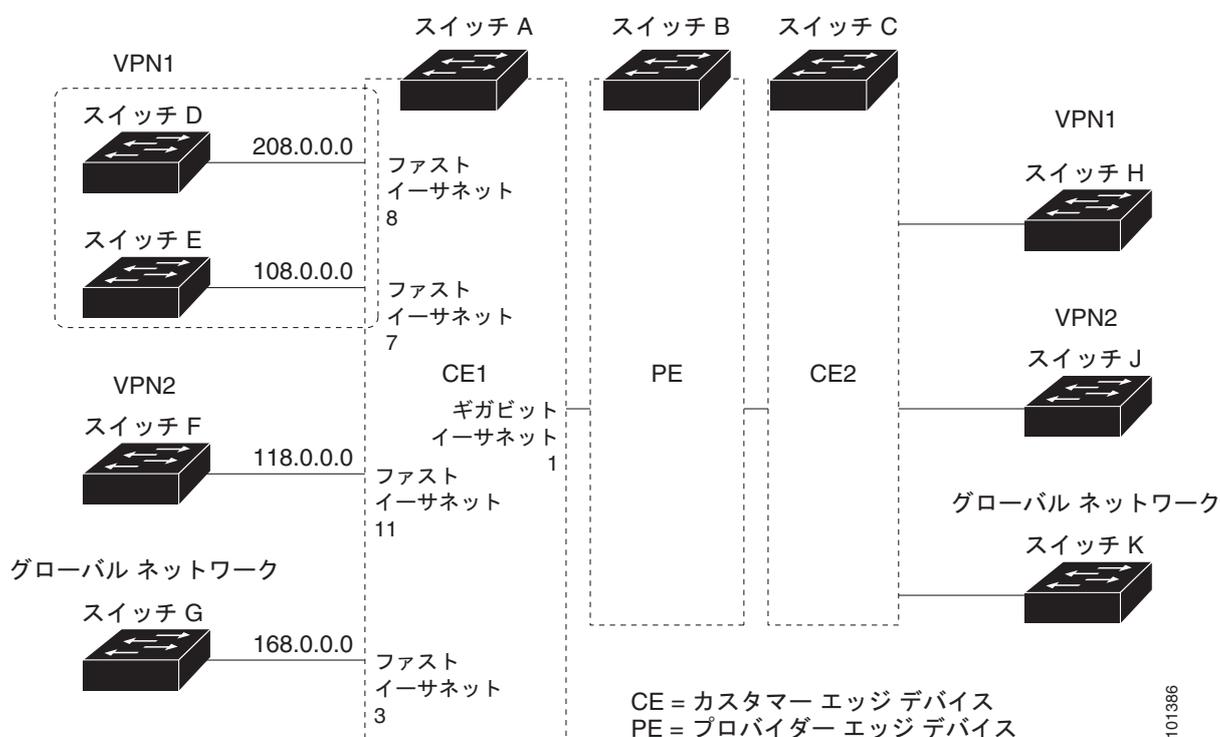
	コマンド	目的
ステップ 6	<code>address-family ipv4 vrf vrf-name</code>	PE/CE ルーティングセッションの BGP パラメータを定義し、VRF アドレスファミリモードを開始します。
ステップ 7	<code>neighbor address remote-as as-number</code>	PE と CE ルータ間の BGP セッションを定義します。
ステップ 8	<code>neighbor address activate</code>	IPv4 アドレスファミリのアドバタイズメントをアクティブにします。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show ip bgp [ipv4] [neighbors]</code>	BGP 設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

BGP ルーティングプロセスを削除するには、`no router bgp autonomous-system-number` グローバルコンフィギュレーションコマンドを使用します。ルーティング特性を削除するには、コマンドにキーワードを指定してこのコマンドを使用します。

Multi-VRF CE の設定例

図 41-7 は、図 41-6 と同じネットワークの物理接続を単純化した例です。VPN1、VPN2、およびグローバルネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。図のあとには、IE3000 スイッチを CE スイッチ A として設定し、カスタマー スイッチ D および F に対して VRF を設定する例を示します。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同じです。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 41-7 Multi-VRF CE の設定例



101386

スイッチ A の設定

スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビットイーサネットポート 1 は PE へのトランク接続です。ファストイーサネットポート 8 と 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet1/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config)# interface fastethernet1/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf v11
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf v12
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf v12
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D の設定

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ F の設定

スイッチ F は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

```
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ B の設定

このコマンドをスイッチ B (PE ルータ) で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitEthernet1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitEthernet1/0.10
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
```

```
Router(config-router-af)# end
```

Multi-VRF CE ステータスの表示

マルチ VRF CE の設定とステータスに関する情報を表示するには、表 41-15 の特権 EXEC コマンドを使用します。

表 41-15 マルチ VRF CE 情報を表示するコマンド

コマンド	目的
<code>show ip protocols vrf vrf-name</code>	VRF に関するルーティング プロトコル情報を表示します。
<code>show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]</code>	VRF に関する IP ルーティング テーブル情報を表示します。
<code>show ip vrf [brief detail interfaces] [vrf-name]</code>	定義した VRF インスタンスに関する情報を表示します。

表示される情報の詳細については、『Cisco IOS Switching Services Command Reference, Release 12.2』を参照してください。

プロトコル独立機能の設定

ここでは、IP ルーティング プロトコルに依存しない機能の設定方法について説明します。この章に記載されている IP ルーティング プロトコル独立コマンドの詳細については、Cisco.com のホームページにアクセスして、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2』の「IP Routing Protocol-Independent Commands」を参照してください（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）。

ここでは、次の設定について説明します。

- 「CEF の設定」 (P.41-90)
- 「等コスト ルーティング パスの個数の設定」 (P.41-92)
- 「スタティック ユニキャスト ルートの設定」 (P.41-92)
- 「デフォルトのルートおよびネットワークの指定」 (P.41-94)
- 「ルート マップによるルーティング情報の再配信」 (P.41-95)
- 「ポリシーベース ルーティングの設定」 (P.41-98)
- 「ルーティング情報のフィルタリング」 (P.41-102)
- 「認証キーの管理」 (P.41-105)

CEF の設定

Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に割り当てることができます。動的なネットワークでは、ルーティング

の変更によって、高速スイッチング キャッシュ エントリが頻繁に無効となります。それにより、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スwitching されることがあります。CEF は転送情報ベース (FIB) 検索テーブルを使用して、宛先ベースの IP パケット スwitching を実行します。

CEF の 2 つの主要な構成要素は、分散 FIB と分散隣接関係テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラーイメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクストホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクストホップのアドレスが保持されます。

スイッチは、ギガビット速度の回線レート IP トラフィックを達成するため Application Specific Integrated Circuit (ASIC; 特定用途向け IC) を使用しているので、CEF 転送はソフトウェア転送パス (CPU により転送されるトラフィック) にだけ適用されます。

デフォルトで、CEF はグローバルにイネーブルに設定されています。何らかの理由でディセーブルになっている場合は、**ip cef** グローバル コンフィギュレーション コマンドを使用して再度イネーブルにできます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで CEF がイネーブルです。 **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。



注意

CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で CEF をディセーブルにしないでください。

ディセーブルである CEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにしたりするには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip cef	CEF の動作をイネーブルにします。
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	ip route-cache cef	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip cef	すべてのインターフェイスの CEF ステータスを表示します。

	コマンド	目的
ステップ 7	<code>show cef linecard [detail]</code>	CEF に関連するインターフェイス情報を表示します。
ステップ 8	<code>show cef interface [interface-id]</code>	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 9	<code>show adjacency</code>	CEF の隣接テーブル情報を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

等コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティング テーブルに複数の等コスト ルートが含まれる場合は、これらを **パラレルパス**と呼ぶこともあります。ネットワークへの等コストパスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレルパスを使用すると、パスに障害が発生した場合に冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。

等コスト ルートはルータによって自動的に取得、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレルパスの最大数は制御可能です。スイッチ ソフトウェアでは最大 32 の等コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

ルーティング テーブルに格納されるパラレルパスのデフォルトの最大数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>maximum-paths maximum</code>	プロトコル ルーティング テーブルのパラレルパスの最大数を設定します。指定できる範囲は 1 ~ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合だけ 1 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip protocols</code>	<i>Maximum path</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、**no maximum-paths** ルータ コンフィギュレーション コマンドを使用します。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

LAN ベース イメージを実行するスイッチは、SVI で最大 16 のユーザ設定のスタティック ルートをサポートします。スタティック ルーティングの設定は、LAN ベース ルーティング SDM テンプレートだけを使用した LAN ベース イメージ、および SVI インターフェイスだけでサポートされます。ルーティング プロトコルはサポートされません。

スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip route prefix mask {address interface} [distance]</code>	スタティック ルートを確立します。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ip route</code>	設定を確認するため、ルーティング テーブルの現在のステートを表示します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スタティック ルートを削除するには、`no ip route prefix mask {address | interface}` グローバル コンフィギュレーション コマンドを使用します。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、アドミニストレーティブ ディスタンスの値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています (表 41-16 を参照)。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのアドミニストレーティブ ディスタンスよりも大きな値になるように設定します。

表 41-16 ダイナミック ルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルト距離
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
EBGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IBGP	200
Unknown	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。`redistribute` スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。ただし、`network` コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに `redistribute` スタティック コマンドを指定しないかぎり、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティックルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

デフォルトのルートおよびネットワークの指定

ルータは、他のすべてのネットワークへのルートを学習できません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛てに指定します（スマート ルータには、インターネット全体ルーティング テーブル情報が格納されます）。これらのデフォルト ルートは動的に取得されるか、ルータごとに設定されます。ほとんどのダイナミックな内部ルーティング プロトコルには、スマート ルータを使用してデフォルト情報を動的に生成し、他のルータに転送するメカニズムがあります。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ネットワークへのスタティック ルートをスタティック デフォルト ルートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip default-network <i>network number</i>	デフォルト ネットワークを指定します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip route	最終ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルートを削除するには、**no ip default-network *network number*** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、特に設定する必要はありません。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合があります。Cisco ルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、アドミニストレーティブ ディスタンスおよびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

ルート マップによるルーティング情報の再配信

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信できます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部を定義します。**match** コマンドは、条件が一致する必要があることを指定しています。**set** コマンドは、ルーティング アップデートが **match** コマンドで定義した条件を満たす場合に行われる処理を指定します。再配信はプロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものであります。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理はすべて実行されません。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。



(注) **set** ルート マップ コンフィギュレーション コマンドを使用しないルート マップは、CPU に送信されるので、CPU の使用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャネルを通じて送り返されます (宛先ベース ルーティング)、ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに **set** コマンドが適用されます。一致基準を満たさないパケットは、通常のルーティング チャネルを通じて転送されます。

BGP ルート マップ **continue** 句を使用して、エントリが無事に一致して句が設定された後、ルート マップの追加のエントリを実行できます。**continue** 句を使用すれば、同じルート マップ内で特定のポリシー コンフィギュレーションを繰り返す必要がないように、より多くのモジュラ ポリシー定義を設定および編成できます。スイッチで発信ポリシーに **continue** コマンドを使用できるようになりました。ルート マップ **continue** コマンドの使用の詳細については、次の URL で、『BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guides_list.html



(注) 次に示すステップ 3 ~ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

再配信用のルート マップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>route-map map-tag [permit deny] [sequence number]</code>	再配信を制御するために使用するルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。 <i>map-tag</i> : ルート マップ用のわかりやすい名前を指定します。 redistribute ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 (任意) permit が指定され、このルート マップの一致条件が満たされている場合は、 set アクションの制御に従ってルートが再配信されます。 deny が指定されている場合、ルートは再配信されません。 <i>sequence number</i> (任意) : 同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を指定する番号です。
ステップ 3	<code>match as-path path-list-number</code>	BGP AS パス アクセス リストと一致させます。
ステップ 4	<code>match community-list community-list-number [exact]</code>	BGP コミュニティ リストと一致させます。
ステップ 5	<code>match ip address {access-list-number access-list-name} [...access-list-number ...access-list-name]</code>	名前または番号を指定し、標準アクセス リストと一致させます。1 ~ 199 の整数を指定できます。
ステップ 6	<code>match metric metric-value</code>	指定されたルート メトリックと一致させます。 <i>metric-value</i> には、0 ~ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。
ステップ 7	<code>match ip next-hop {access-list-number access-list-name} [...access-list-number ...access-list-name]</code>	指定されたアクセス リスト (番号 1 ~ 199) のいずれかで送信される、ネクストホップのルータ アドレスと一致させます。
ステップ 8	<code>match tag tag value [...tag-value]</code>	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ~ 4294967295 の整数を指定できます。
ステップ 9	<code>match interface type number [...type number]</code>	指定されたインターフェイスの 1 つから、指定されたネクスト ホップへのルートと一致させます。
ステップ 10	<code>match ip route-source {access-list-number access-list-name} [...access-list-number ...access-list-name]</code>	指定されたアドバタイズ済みアクセス リストによって指定されるアドレスと一致させます。
ステップ 11	<code>match route-type {local internal external [type-1 type-2]}</code>	指定された route-type と一致させます。 <ul style="list-style-type: none"> • local : ローカルに生成された BGP ルート • internal : OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート • external : OSPF 外部ルート (タイプ 1 またはタイプ 2) または EIGRP 外部ルート

	コマンド	目的
ステップ 12	<code>set dampening halflife reuse suppress max-suppress-time</code>	BGP ルート ダンプニング係数を設定します。
ステップ 13	<code>set local-preference value</code>	ローカル BGP パスに値を割り当てます。
ステップ 14	<code>set origin {igp egp as incomplete}</code>	BGP の送信元コードを設定します。
ステップ 15	<code>set as-path {tag prepend as-path-string}</code>	BGP AS パスを変更します。
ステップ 16	<code>set level {level-1 level-2 level-1-2 stub-area backbone}</code>	ルーティング ドメインの指定エリアにアダプタイズされるルートのレベルを設定します。 stub-area および backbone は、OSPF NSSA およびバックボーン エリアです。
ステップ 17	<code>set metric metric value</code>	再配信されるルートに指定するメトリック値を設定します (EIGRP 専用)。 <i>metric value</i> は -294967295 ~ 294967295 の整数です。
ステップ 18	<code>set metric bandwidth delay reliability loading mtu</code>	再配信されるルートに指定するメトリック値を設定します (EIGRP 専用)。 <ul style="list-style-type: none"> • <i>bandwidth</i> : 0 ~ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅 (キロビット/秒単位)。 • <i>delay</i> : 0 ~ 4294967295 の範囲のルート遅延 (10 マイクロ秒単位)。 • <i>reliability</i> : 0 ~ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • <i>loading</i> : 0 ~ 255 の数値で表されるルートの有効帯域幅 (255 は 100% の負荷)。 • <i>mtu</i> : ルートの MTU の最小サイズ (バイト単位)。範囲は 0 ~ 4294967295 です。
ステップ 19	<code>set metric-type {type-1 type-2}</code>	再配信されるルートに OSPF 外部メトリック タイプを設定します。
ステップ 20	<code>set metric-type internal</code>	ネクスト ホップの IGP メトリックと一致するように、EBGP ネイバーにアダプタイズされるプレフィックスの multi-exit discriminator (MED) 値を設定します。
ステップ 21	<code>set weight</code>	ルーティング テーブルの BGP 重みを設定します。指定できる値は 1 ~ 65535 です。
ステップ 22	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 23	<code>show route-map</code>	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 24	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、`no route-map map tag` グローバル コンフィギュレーション コマンド、または `no match` や `no set` ルート マップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを送信したり、ルート再配信を制御できます。

ルート再配信を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは前述の手順で定義されたキーワードと同じです。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>redistribute protocol [process-id] {level-1 level-1-2 level-2} [metric metric-value] [metric-type type-value] [match internal external type-value] [tag tag-value] [route-map map-tag] [weight weight] [subnets]</code>	ルーティング プロトコル間でルートを再配信します。 <code>route-map</code> を指定しないと、すべてのルートが再配信されます。キーワード <code>route-map</code> に <code>map-tag</code> を指定しないと、ルートは配信されません。
ステップ 4	<code>default-metric number</code>	現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します (BGP、RIP、OSPF)。
ステップ 5	<code>default-metric bandwidth delay reliability loading mtu</code>	EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show route-map</code>	設定を確認するため、設定されたすべてのルートマップ、または指定されたルート マップだけを表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

再配信をディセーブルにするには、そのコマンドの `no` 形式を使用します。

ルーティング プロトコルのメトリックを、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは 5 つの特性の組み合わせです。このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。ルーティング情報を制御せずにさまざまなルーティング プロトコル間で交換するとルーティング グループが発生し、ネットワーク動作が著しく低下することがあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することがあります。

- RIP はスタティック ルートを自動的に再配信できます。スタティック ルートにはメトリック 1 (直接接続) が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

ポリシーベース ルーティングの設定

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- アプリケーション
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、インタラクティブ対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は高帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーションデータは低帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、**Access Control List (ACL)** (アクセス コントロール リスト) を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクストホップに転送 (ルーティング) されます。

- パケットがルート マップ ステートメントと一致しない場合は、すべての **set** 句が適用されます。
- ステートメントが許可としてマークされている場合、どのルートマップ ステートメントとも一致しないパケットは通常の転送チャネルを通じて送信され、宛先ベースのルーティングが実行されません。
- PBR では、拒否としてマークされているルートマップ ステートメントはサポートされません。

ルート マップの設定の詳細については、「[ルート マップによるルーティング情報の再配信 \(P.41-95\)](#)」を参照してください。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンドステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定できます。一致が見つかるまで、ルート マップにこのプロセスが行われます。一致が見つからない場合、通常の宛先ベース ルーティングが行われます。**match** ステートメントリストの末尾には、暗黙の拒否ステートメントがあります。

match 句が満たされた場合は、**set** 句を使用して、パス内のネクストホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*』を参照してください。表示されているにもかかわらずスイッチでサポートされない PBR コマンドについては、[付録 B 「Cisco IOS Release 15.0\(1\)SE でサポートされていないコマンド」](#) を参照してください。



(注)

このソフトウェア リリースは、IPv4 および IPv6 トラフィック処理時に PBR をサポートしません。

PBR 設定時の注意事項

PBR の設定を開始する前に、次の点に注意してください。

- PBR を使用するには、スイッチ上で IP サービス イメージが稼働している必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- PBR には、**route-map deny** ステートメントはサポートされません。
- レイヤ 3 モードの EtherChannel ポートチャネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチには最大 246 個の IP ポリシー ルート マップを定義できます。
- スイッチには、PBR 用として最大 512 個のアクセス コントロール エントリ (ACE) を定義できます。

- ルート マップに一致基準を設定する場合は、次の注意事項に従ってください。
 - ローカル アドレス宛でのパケットを許可する ACL と照合させないでください。PBR はこれらのパケットを転送しますが、ping や Telnet 障害またはルート プロトコル フラッピングが発生する可能性があります。
 - 拒否 ACE を含む ACL と照合させないでください。拒否 ACE と一致するパケットが CPU に送られるため、CPU の利用率が高くなる可能性があります。
- PBR を使用するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用して、まずルーティング テンプレートをイネーブルにする必要があります。VLAN またはデフォルト テンプレートでは、PBR がサポートされません。SDM テンプレートの詳細については、第 10 章「SDM テンプレートの設定」を参照してください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにはできません。その反対の場合も同じで、VRF がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- WCCP と PBR は、スイッチ インターフェイスで相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、WCCP をイネーブルにできません。その反対の場合も同じで、WCCP がインターフェイスでイネーブルになっているときは、PBR をイネーブルにできません。
- PBR で使用される Ternary CAM (TCAM; 3 値連想メモリ) エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- パケット長、Type of Service (ToS; タイプ オブ サービス)、set interface、set default next hop、または set default interface に基づく PBR は、サポートされていません。有効な set アクションがないか、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされていません。
- スイッチは PBR ルート マップでの Quality of Service (QoS) DSCP および IP precedence の一致をサポートしていて、次のような制限事項があります。
 - DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用できません。
 - DSCP 透過性と PBR DSCP ルート マップを同じスイッチ上に設定できません。
 - QoS DSCP を含む PBR を設定する場合、QoS がイネーブル (**mls qos** グローバル コンフィギュレーション コマンドを使用) またはディセーブル (**no mls qos** コマンドを使用) になるように設定できます。QoS がイネーブルの場合、トラフィックの DSCP 値が変更されないようにするには、**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを入力して、スイッチの入力トラフィック ポートで DSCP 信頼状態を設定します。信頼状態が DSCP でない場合、デフォルトですべての信頼されないトラフィックは DSCP 値が 0 としてマークされることとなります。

PBR のイネーブル化

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準およびすべての match 句と一致した場合の動作を指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、match 句と一致したものはすべて PBR の対象になります。

PBR は、スイッチの速度低下を引き起こさない速度で、高速転送したり実装したりできます。高速スウィッチングされた PBR では、ほとんどの match および set コマンドを使用できます。PBR の高速スウィッチングをイネーブルにするには、事前に PBR をイネーブルにする必要があります。PBR の高速スウィッチングは、デフォルトでディセーブルです。

スイッチで生成されたパケットまたはローカルパケットは、通常どおりにポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。ローカル PBR は、デフォルトでディセーブルに設定されています。

PBR を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	route-map map-tag [permit] [sequence number]	<p>パケットの出力場所を制御するために使用するルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> map-tag : ルート マップ用のわかりやすい名前を指定します。 ip policy route-map インターフェイス コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 (任意) permit が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートがポリシー ルーティングされます。 <p>(注) route-map deny ステートメントは、インターフェイスに適用する PBR ルート マップではサポートされません。</p> <ul style="list-style-type: none"> sequence number (任意) : 同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を示す番号です。
ステップ 3	match ip address {access-list-number access-list-name} [...access-list-number ...access-list-name]	<p>1 つまたは複数の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。</p> <p>(注) 拒否 ACE を含む ACL またはローカル アドレス宛てのパケットを許可する ACL は入力しないでください。</p> <p>match コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。</p>
ステップ 4	set ip next-hop ip-address [...ip-address]	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します (ネクスト ホップは隣接していなければなりません)。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 7	<code>ip policy route-map map-tag</code>	レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを識別します。1 つのインターフェイスに設定できるルート マップは、1 つだけです。ただし、異なるシーケンス番号を持つ複数のルート マップ エントリを設定できます。これらのエントリは、最初的一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。 (注) IP ポリシー ルート マップに deny ステートメントが含まれていると、その設定は失敗します。
ステップ 8	<code>ip route-cache policy</code>	(任意) PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	<code>ip local policy route-map map-tag</code>	(任意) ローカル PBR をイネーブルにして、スイッチから送信されるパケットに PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show route-map [map-name]</code>	(任意) 設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 13	<code>show ip policy</code>	(任意) インターフェイスに付加されたポリシー ルート マップを表示します。
ステップ 14	<code>show ip local policy</code>	(任意) ローカル PBR がイネーブルであるかどうか、およびイネーブルである場合は使用されているルート マップを表示します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、**no route-map map-tag** グローバル コンフィギュレーション コマンド、または **no match** または **no set** ルート マップ コンフィギュレーション コマンドを使用します。インターフェイス上で PBR をディセーブルにするには、**no ip policy route-map map-tag** インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されるパケットに対して PBR をディセーブルにするには、**ip local policy route-map map-tag** グローバル コンフィギュレーション コマンドを使用します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、以下の作業を実行します。



(注) OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

受動インターフェイスの設定

ローカル ネットワーク上の他のルータが動的にルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用し、ルーティング アップデート メッセージがルータ インターフェイスから送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたルータ インターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を回避するには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用し、すべてのインターフェイスをデフォルトでパッシブになるように設定します。このあとで、隣接関係が必要なインターフェイスを手動で設定します。

受動インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router {bgp rip ospf eigrp}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	passive-interface interface-id	指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	passive-interface default	(任意) すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	no passive-interface interface type	(任意) 隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	network network-address	(任意) ルーティング プロセス用のネットワーク リストを指定します。 <i>network-address</i> は IP アドレスです。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、**show ip ospf interface** などのネットワーク モニタリング用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、**show ip interface** 特権 EXEC コマンドを使用します。

ルーティング アップデートの送信を再度イネーブルにするには、**no passive-interface interface-id** ルータ コンフィギュレーション コマンドを使用します。**default** キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。次に、**no passive-interface** ルータ コンフィギュレーション コマンドを使用し、隣接関係を必要とする各インターフェイスを個別に設定します。**default** キーワードは、ほとんどの配信ルータに 200 を超えるインターフェイスが備わっているインターネット サービス プロバイダーや大規模な企業ネットワークの場合に役立ちます。

ルーティング アップデートのアドバタイズおよび処理の制御

ACL と **distribute-list** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズを抑制し、他のルータが 1 つまたは複数のルートを取得しないようにできます。この機能を OSPF で使用した場合は外部ルートにだけ適用されるため、インターフェイス名を指定できません。

distribute-list ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルートを処理しないようにすることもできます (OSPF にこの機能は適用されません)。

ルーティング アップデートのアドバタイズまたは処理を制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>distribute-list {access-list-number access-list-name} out [interface-name routing process autonomous-system-number]</code>	アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズを許可または拒否します。
ステップ 4	<code>distribute-list {access-list-number access-list-name} in [type-number]</code>	アップデートにリストされたルートの処理を抑制します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを変更またはキャンセルするには、**no distribute-list in** ルータ コンフィギュレーション コマンドを使用します。アップデート中のネットワーク アドバタイズメントの抑制をキャンセルするには、**no distribute-list out** ルータ コンフィギュレーション コマンドを使用します。

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「アドミニストレーティブ ディスタンス」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティング プロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。アドミニストレーティブ ディスタンスの値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルのアドミニストレーティブ ディスタンスが最短（値が最小）であるルートが選択されます。表 41-16 (P.41-93) に、さまざまなルーティング情報送信元のデフォルトのアドミニストレーティブ ディスタンスを示します。

各ネットワークには独自の要件があるため、アドミニストレーティブ ディスタンスを割り当てる一般的な注意事項はありません。

ルーティング情報の送信元をフィルタリングするには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	distance <i>weight</i> { <i>ip-address</i> { <i>ip-address mask</i> }} [<i>ip access list</i>]	アドミニストレーティブ ディスタンスを定義します。 <i>weight</i> : アドミニストレーティブ ディスタンスは 10 ~ 255 の整数です。単独で使用した場合、 <i>weight</i> はデフォルトのアドミニストレーティブ ディスタンスを指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。 (任意) <i>ip access list</i> : 着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip protocols	指定されたルーティング プロセス用のデフォルトのアドミニストレーティブ ディスタンスを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アドミニストレーティブ ディスタンスを削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

認証キーの管理

キー管理を使用すると、ルーティング プロトコルで使用される認証キーを制御できます。一部のプロトコルでは、キー管理を使用できません。認証キーは EIGRP および RIP バージョン 2 で使用できます。

認証キーを管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証キーを管理するには、キー チェーンを定義してそのキー チェーンに属するキーを識別し、各キーの有効期間を指定します。各キーには、ローカルにストアされる独自のキー ID (**key number** キー チェーン コンフィギュレーション コマンドで指定) があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5 (MD5) 認証キーが一意に識別されます。

有効期間が指定された複数のキーを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは 1 つだけです。キー番号は小さい方から大きい方へソフトウェアによって順に調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

認証キーを管理するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	key chain <i>name-of-chain</i>	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。
ステップ 3	key number	キー番号を識別します。指定できる範囲は 0 ~ 2147483647 です。

	コマンド	目的
ステップ 4	<code>key-string text</code>	キー スtring を識別します。String には 1 ~ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定できません。
ステップ 5	<code>accept-lifetime start-time {infinite end-time duration seconds}</code>	(任意) キーを受信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および <i>duration</i> は infinite です。
ステップ 6	<code>send-lifetime start-time {infinite end-time duration seconds}</code>	(任意) キーを送信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトは、デフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および <i>duration</i> は infinite です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show key chain</code>	認証キー情報を表示します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

キー チェーンを削除するには、`no key chain name-of-chain` グローバル コンフィギュレーション コマンドを使用します。

IP ネットワークのモニタリングおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを削除したり、ステータスを表示するには、表 41-17 に示す特権 EXEC コマンドを使用します。

表 41-17 IP ルートの削除またはルート ステータスの表示を行うコマンド

コマンド	目的
<code>clear ip route {network [mask *]}</code>	IP ルーティング テーブルから 1 つまたは複数のルートをクリアします。
<code>show ip protocols</code>	アクティブなルーティング プロトコル プロセスのパラメータおよびステータスを表示します。
<code>show ip route [address [mask] [longer-prefixes]] [protocol [process-id]]</code>	ルーティング テーブルの現在のステータスを表示します。
<code>show ip route summary</code>	ルーティング テーブルの現在のステータスをサマリー形式で表示します。
<code>show ip route supernets-only</code>	スーパーネットを表示します。

表 41-17 IP ルートの削除またはルート ステータスの表示を行うコマンド (続き)

コマンド	目的
<code>show ip cache</code>	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
<code>show route-map [map-name]</code>	設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。



CHAPTER 42

IPv6 ユニキャスト ルーティングの設定

この章では、IE 3000 スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、第 44 章「IPv6 MLD スヌーピングの設定」を参照してください。IPv6 アクセス コントロール リスト (ACL) の設定については、第 45 章「IPv6 ACL の設定」を参照してください。IPv4 ユニキャスト ルーティングの設定については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

この機能を使用するには、スイッチ上で IP サービス イメージが稼働している必要があります。

IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートを使用するようにスイッチを設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」(P.42-5) を参照してください。



(注)

この章で説明するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマニュアルを参照してください。

この章の内容は、次のとおりです。

- 「IPv6 の概要」(P.42-1)
- 「IPv6 の設定」(P.42-10)
- 「IPv6 の表示」(P.42-28)

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service (QoS)、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータでネットワーク アドレス変換 (NAT) 処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 次の URL にある『Cisco IOS IPv6 Configuration Library』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- Cisco IOS ソフトウェア マニュアルを検索するには、検索フィールドを使用します。たとえば、スタティック ルートに関する情報を取得する場合は、検索フィールドに「Implementing Static Routes for IPv6」と入力してスタティック ルートに関する資料を取得します。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ここでは、スイッチへの IPv6 の実装について説明します。内容は次のとおりです。

- 「IPv6 アドレス」 (P.42-2)
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」 (P.42-2)
- 「サポートされていない IPv6 ユニキャスト ルーティング機能」 (P.42-9)
- 「制限事項」 (P.42-10)

IPv6 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。スイッチはサイトローカルなユニキャスト アドレス、エニキャスト アドレス、またはマルチキャスト アドレスをサポートしません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド (n:n:n:n:n:n:n:n. の形式) で表されます。次に、IPv6 アドレスの例を示します。

```
2031:0000:130F:0000:0000:09C0:080F:130B
```

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

```
2031:0:130F:0:0:9C0:80F:130B
```

2 つのコロン (::) を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

```
2031:0:130F::09C0:080F:130B
```

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章では、次の項が IE 3000 スイッチに該当します。

- 「IPv6 Address Formats」
- 「IPv6 Address Type: Unicast」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

- 「128 ビット幅のユニキャスト アドレス」 (P.42-3)
- 「IPv6 の DNS」 (P.42-4)
- 「IPv6 ユニキャストのパス MTU ディスカバリ」 (P.42-4)
- 「ICMPv6」 (P.42-4)
- 「ネイバー探索」 (P.42-4)
- 「DRP」 (P.42-4)

- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.42-5)
- 「IPv6 アプリケーション」 (P.42-5)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.42-5)
- 「DHCP for IPv6 アドレスの割り当て」 (P.42-6)
- 「IPv6 のスタティック ルート」 (P.42-7)
- 「IPv6 の RIP」 (P.42-7)
- 「IPv6 の OSPF の設定」 (P.42-7)
- 「EIGRP IPv6」 (P.42-8)
- 「IPv6 の HSRP」 (P.42-8)
- 「IPv6 上の SNMP および Syslog」 (P.42-8)
- 「IPv6 による HTTP (S)」 (P.42-9)

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001 (2000::/3) で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3 (001) ~ E000::/3 (111) のアドレスには、Extended Unique Identifier (EUI) 64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィックス FE80::/10 (1111 1110 10) およびインターフェイス ID を使用します。Neighbor Discovery Protocol (NDP; ネイバー探索プロトコル) およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意的なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の DNS

IPv6 は、Domain Name System (DNS; ドメイン ネーム システム) のレコードタイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコードタイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv6 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチはシステム Maximum Transmission Unit (MTU; 最大伝送単位) の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合わせて調整できます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケットサイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャストパケットのパス MTU ディスカバリをサポートしません。

ICMPv6

IPv6 のインターネット制御メッセージプロトコル (ICMP) は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 NDP は ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク (ローカルリンク) 上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Preference (DRP) をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option (RFC 4191) をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDP は、到達可能または到達可能な可能性があるルータとして、常に同じルータを選択

するか、またはルータ リストから繰り返し使用できます。DRP を使用することにより、IPv6 ホストが、両方もが到達可能または到達可能な可能性がある 2 台のルータを差別化するように設定できます。

IPv6 の DRP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアダプタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、Traceroute、Telnet、および Trivial File Transfer Protocol (TFTP)
- IPv6 トランスポートによる Secure Shell (SSH; セキュア シェル)
- IPv6 トランスポートによる HTTP サーバアクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol (CDP) サポート

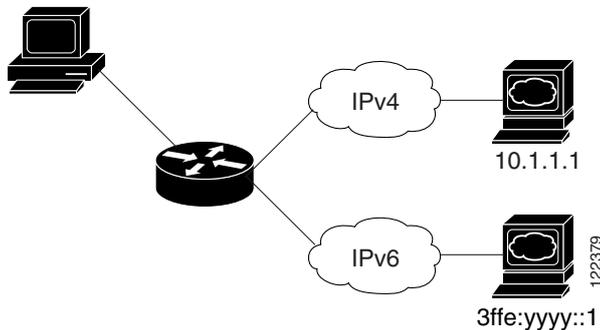
これらのアプリケーションの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方に Ternary Content Addressable Memory (TCAM; 3 値連想メモリ) の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 42-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 42-1 インターフェイス上での IPv4/IPv6 のデュアル サポート



IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 スイッチング データベース管理 (SDM) テンプレートを使用します。デュアル IPv4/IPv6 SDM テンプレートについての詳細は、第 10 章「SDM テンプレートの設定」を参照してください。

デュアル IPv4 および IPv6 テンプレートを使用すると、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 専用環境のスイッチは、IPv4 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境のスイッチは、IPv4 および IPv6 パケットをルーティングし、IPv4 QoS をハードウェアで適用します。
- IPv6 QoS はサポートされません。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4/IPv6 プロトコル スタックについての詳細は、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 により、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能により、ホストが接続されているネットワークに基づいた適切なプレフィックスで重複のないアドレス割り当てが行われます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよび DNS ネームサーバアドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

Cisco IOS Release 12.2(58)SE 以降のスイッチでは、次の機能がサポートされます。

- DHCPv6 Bulk Lease クエリー

DHCPv6 バルクリース クエリーでは、クライアントが、DHCPv6 バインディングに関する情報を要求できます。この機能により、新しいクエリー タイプが追加され、TCP を使用した DHCPv6 バインディング データのバルク転送が可能になります。再起動後、リレー サーバが DHCP サーバからバインディング情報を取得するために自動的にバルク リース クエリーを生成するため、DHCPv6 バインディング データのバルク転送は、リレー サーバスイッチがリブートされ、リレー サーバがすべてのバインディング情報を失った場合に役立ちます。

- DHCPv6 リレー ソース設定

DHCPv6 サーバは、DHCP リレー エージェントの送信元アドレスに対して応答します。通常、DHCPv6 リレー エージェントからのメッセージには、それらの送信元インターフェイスが送信元アドレスとして示されます。ただし、一部のネットワークでは、より安定したアドレス（ループバック インターフェイスなど）をリレー エージェントからのメッセージの送信元アドレスとして設定することが望ましい場合があります。DHCPv6 リレー送信元設定機能には、この機能が用意されています。

これらの機能の詳細および設定方法については、『[Cisco IOS IPv6 Configuration Guide, Release 12.4](#)』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーク デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 の RIP

IPv6 の Routing Information Protocol (RIP) は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 の OSPF の設定

IP サービス イメージが稼働するスイッチは IP のリンクステート プロトコルの IPv6 Open Shortest Path First (OSPF) をサポートしています。詳細については、Cisco.com で『[Cisco IOS IPv6 Configuration Library](#)』の「Implementing OSPF for IPv6」の章を参照してください。

OSPFv3 グレースフル リスタート

Cisco IOS Release 12.2(58)SE 以降のリリースでは、IP サービス フィーチャ セットを実行するスイッチは OSPFv3 のグレースフル リスタート機能をサポートします。この機能により、OSPFv3 ルーティング プロトコル情報が復元されている間も、既知のルート上でノンストップのデータの転送が可能になります。スイッチは、再起動モード（グレースフル リスタート対応スイッチなど）か、ヘルパーモード（グレースフル リスタート認識スイッチなど）のいずれかで、グレースフル リスタートに参加できます。

グレースフル リスタート機能を実行するには、スイッチがハイ アベイラビリティ (HA) ステートフル スイッチオーバー (SSO) モード (つまり、デュアル RP) になっている必要があります。グレースフル リスタートが可能なスイッチは、これらの障害が発生すると、グレースフル リスタートの機能を実行します。

- ルート プロセッサ (RP) 障害が発生し、スタンバイ RP へのスイッチオーバーが行われた場合
- スタンバイ RP への計画的な RP スイッチオーバーが行われた場合

グレースフル リスタート機能では、隣接スイッチがグレースフル リスタート認識である必要があります。

詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

EIGRP IPv6

IP サービス イメージを実行するスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol (EIGRP) をサポートします。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼働するため、使用可能な IPv4 ルータ ID がない場合があります。

IPv6 の EIGRP の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の HSRP

IP サービス イメージが稼働するスイッチは、IPv6 対応のホットスタンバイ ルータ プロトコル (HSRP) をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカルアドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカルアドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

IPv6 の HSRP の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 上の SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート

- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル (UDP) SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 に関連する SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP (S)

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカードアドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続が確立するためには、基本ネットワーク接続 (ping) がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 ポリシーベース ルーティング
- IPv6 バーチャル プライベート ネットワーク (VPN) Routing And Forwarding (VRF; VPN ルーティングおよび転送) テーブルのサポート
- Multiprotocol ボーダー ゲートウェイ プロトコル (BGP)、および Intermediate System-to-Intermediate System (IS-IS) ルーティングの IPv6 ルーティング プロトコルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ

- IPv6 ユニキャスト Reverse-Path Forwarding
- IPv6 の汎用プレフィックス

制限事項

IPv6 はスイッチのハードウェアに実装されるため、TCAM 内の IPv6 圧縮アドレスによるいくつかの制限があります。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- ICMPv6 リダイレクト機能は、IPv6 ホスト ルート（特定のホストに到達するのに使用されるルート）、またはマスク長が 64 ビットを超える IPv6 ルートではサポートされません。スイッチは、ホスト ルートまたはマスク長が 64 ビットを超えるルートを介して到達可能な特定の宛先へのより最適なファーストホップ ルータに、ホストをリダイレクトできません。
- マスク長が 64 ビットを超える IPv6 ホスト ルートまたは IPv6 ルートでは、等価コストおよび不等価コスト ルートを使用するロード バランシングはサポートされません。
- スイッチは、SNAP カプセル化 IPv6 パケットを転送できません。



(注) IPv4 SNAP カプセル化パケットにも同様の制限がありますが、パケットはスイッチでドロップされ、転送されません。

- スイッチは、IPv6/IPv4 および IPv4/IPv6 パケットをハードウェアでルーティングしますが、スイッチを IPv6/IPv4 または IPv4/IPv6 トンネル エンドポイントにはできません。
- ホップバイホップの拡張ヘッダーを持つブリッジング済みの IPv6 パケットは、ソフトウェアで転送されます。IPv4 の場合、これらのパケットはソフトウェアでルーティングされ、ハードウェアでブリッジングされます。
- ソフトウェア コンフィギュレーション ガイドで定義された標準の SPAN および RSPAN 制限のほかに、次のような IPv6 パケット固有の制限事項があります。
 - RSPAN IPv6 ルーテッドパケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスが不正である場合があります。
 - RSPAN IPv6 ルーテッドパケットを送信した場合、宛先 MAC アドレスが不正である場合があります。標準トラフィックは影響を受けません。
- スイッチはソースルート IPv6 パケットに関する QoS 分類または PBR をハードウェアで適用できません。
- スイッチはマルチキャスト パケットに対して ICMPv6 *Packet Too Big* メッセージを生成できません。

IPv6 の設定

ここでは、次の IPv6 転送の設定情報について説明します。

- 「IPv6 のデフォルト設定」(P.42-11)
- 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」(P.42-11)
- 「DRP の設定」(P.42-14)
- 「IPv4 および IPv6 プロトコル スタックの設定」(P.42-15)

- 「DHCP for IPv6 アドレス割り当ての設定」 (P.42-16)
- 「IPv6 ICMP レート制限の設定」 (P.42-19)
- 「IPv6 の CEF の設定」 (P.42-20)
- 「IPv6 のスタティック ルートの設定」 (P.42-20)
- 「IPv6 RIP の設定」 (P.42-22)
- 「IPv6 OSPF の設定」 (P.42-23)
- 「IPv6 の EIGRP の設定」 (P.42-25)
- 「IPv6 の HSRP の設定」 (P.42-25)

IPv6 のデフォルト設定

表 42-1 に IPv6 のデフォルト設定を示します。

表 42-1 IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	ディセーブル (IPv4 CEF および dCEF はデフォルトでイネーブル) (注) IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- この章で説明されている機能の中には、IP サービス イメージを実行する IE 3000 スイッチでサポートされていないものがあります。「サポートされていない IPv6 ユニキャスト ルーティング機能」 (P.42-9) を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで指定した *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数 (スラッシュ (/) で始まる) は、プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:1:ff00::/104 (このアドレスはネイバー探索プロセスで使用される)
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>sdm prefer dual-ipv4-and-ipv6 {default routing}</code>	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 <ul style="list-style-type: none"> • default : スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • routing : IPv4 PBR などの IPv4 および IPv6 ルーティングをサポートするためにスイッチをルーティング テンプレートに設定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>reload</code>	オペレーティング システムをリロードします。
ステップ 5	<code>configure terminal</code>	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	<code>no switchport</code>	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。

	コマンド	目的
ステップ 8	<code>ipv6 address ipv6-prefix/prefix length eui-64</code> または <code>ipv6 address ipv6-address/prefix length</code> または <code>ipv6 address ipv6-address link-local</code> または <code>ipv6 enable</code>	IPv6 アドレスの下位 64 ビットの Extended Unique Identifier (EUI; 拡張固有識別子) を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスの IPv6 アドレスを手動で設定します。 インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	<code>ip routing</code>	スイッチ上で IP ルーティングをイネーブルに設定します。
ステップ 11	<code>ipv6 unicast-routing</code>	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ipv6 interface interface-id</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface EXEC** コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID (20B:46FF:FE2F:D940) を付加する方法を示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/1
GigabitEthernet1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
```

```

Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

```

DRP の設定

Router Advertisement (RA; ルータ アドバタイズメント) メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	ipv6 nd router-preference {high medium low}	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 DRP をディセーブルにするには、**no ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end

```

IPv6 の DRP の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv4 および IPv6 プロトコル スタックの設定

IPv6 ルーティングを設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選擇する必要があります。まだ設定していない場合、**sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan} [desktop]** グローバル コンフィギュレーション コマンドを使用して IPv6 をサポートするテンプレートを設定します。新規テンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	スイッチ上でルーティングをイネーブルに設定します。
ステップ 3	ipv6 unicast-routing	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。
ステップ 6	ip address ip-address mask [secondary]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	グローバルな IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクローカルなアドレスでなく、インターフェイス上の特定の、リンクローカルなアドレスを使用するように指定します。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show interface interface-id show ip interface interface-id show ipv6 interface interface-id	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv4 ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。IPv6 ルーティングをディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。インターフェイスから IPv4 アドレスを削除するには、**no ip address ip-address mask** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6**

address インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

DHCP for IPv6 アドレス割り当ての設定

ここでは、IPv6 DHCP (DHCPv6) アドレス割り当ての設定方法について説明します。

- 「DHCPv6 アドレス割り当てのデフォルト設定」 (P.42-16)
- 「DHCPv6 アドレス割り当ての設定時の注意事項」 (P.42-16)
- 「DHCPv6 サーバ機能のイネーブル化」 (P.42-17)
- 「DHCPv6 クライアント機能のイネーブル化」 (P.42-19)

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
 - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
 - SVI : **interface vlan vlan_id** コマンドを使用して作成された VLAN インターフェイスです。
 - レイヤ 3 モードの EtherChannel ポート チャンネル : **interface port-channel port-channel-number** コマンドを使用して作成されたポートチャンネル論理インターフェイス。
- DHCPv6 を設定する場合は、事前に IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 dhcp pool <i>poolname</i></code>	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。
ステップ3	<code>address prefix <i>IPv6-prefix</i> lifetime {<i>tl tl</i> infinite}</code>	(任意) アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 lifetime <i>tl tl</i> : IPv6 アドレス プレフィックスが有効ステートを維持するタイム インターバル (秒) を指定します。指定できる範囲は 5 ~ 4294967295 秒です。間隔を指定しない場合は、 infinite を指定します。
ステップ4	<code>link-address <i>IPv6-prefix</i></code>	(任意) リンクアドレスの IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
ステップ5	<code>vendor-specific <i>vendor-id</i></code>	(任意) ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を入力します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ~ 4294967295 です。
ステップ6	<code>suboption number {address <i>IPv6-address</i> ascii <i>ASCII-string</i> hex <i>hex-string</i>}</code>	(任意) ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ~ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプションパラメータで定義されているように入力します。
ステップ7	<code>exit</code>	DHCP プール コンフィギュレーション モードに戻ります。
ステップ8	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ9	<code>interface <i>interface-id</i></code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

	コマンド	目的
ステップ 10	ipv6 dhcp server [<i>poolname</i> automatic] [rapid-commit] [<i>preference value</i>] [allow-hint]	<p>インターフェイスで DHCPv6 サーバ機能をイネーブルにします。</p> <ul style="list-style-type: none"> • poolname : (任意) IPv6 DHCP プールのユーザ定義の名前。プール名には象徴的な文字列 (Engineering など) または整数 (0 など) を使用できます。 • automatic : (任意) システムが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • rapid-commit : (任意) 2 つのメッセージの交換方法を許可します。 • preference value : (任意) サーバによって送信されるアドバタイズメントメッセージ内のプリファレンス オプションで指定されるプリファレンス値。有効な範囲は 0 ~ 255 です。デフォルトのプリファレンス値は 0 です。 • allow-hint : (任意) サーバが、SOLICIT メッセージ内のクライアントからの指示を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show ipv6 dhcp pool または show ipv6 dhcp interface	<p>DHCPv6 プール設定を確認します。</p> <p>DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。</p>
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool poolname** グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次の例では、350 というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで DHCPv6 クライアント機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ3	ipv6 address dhcp [rapid-commit]	インターフェイスで、DHCPv6 サーバから IPv6 アドレスを取得するようにします。 rapid-commit : (任意) アドレス割り当てで、2 つのメッセージの交換方法を許可します。
ステップ4	ipv6 dhcp client request [vendor-specific]	(任意) インターフェイスでベンダー固有のオプションを要求するようにします。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show ipv6 dhcp interface	DHCPv6 クライアント機能がインターフェイス上でイネーブルであることを確認します。

DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除するには、**no ipv6 address dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ (バケットに格納される最大トークン数) は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 icmp error-interval interval [bucketsize]</code>	IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定します。 <ul style="list-style-type: none"> <code>interval</code> : バケットに追加されるトークンの間隔 (ミリ秒)。指定できる範囲は 0 ~ 2147483647 ミリ秒です。 <code>bucketsize</code> : (任意) バケットに格納される最大トークン数。指定できる範囲は 1 ~ 200 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 interface [interface-id]</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ipv6 icmp error-interval` グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 の CEF の設定

Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) は、ネットワーク パフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。IPv6 CEF はデフォルトでディセーブルになっていますが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、最初に `ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケット フォワーディングをグローバルに設定する必要があります。そして、`ipv6 address` インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

IPv6 CEF をディセーブルにするには、`no ipv6 cef` グローバル コンフィギュレーション コマンドを使用します。IPv6 CEF または dCEF をディセーブルにした後に再びイネーブルにするには、`ipv6 cef` グローバル コンフィギュレーション コマンドを使用します。IPv6 ステータスを確認するには、`show ipv6 cef` 特権 EXEC コマンドを入力します。

CEF および dCEF の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルートの設定

スタティック IPv6 ルートを設定する前に、`ip routing` グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、`ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 route ipv6-prefix/prefix length {ipv6-address interface-id [ipv6-address]} [administrative distance]</code>	<p>スタティック IPv6 ルートを設定します。</p> <ul style="list-style-type: none"> • <i>ipv6-prefix</i> : スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • <i>/prefix length</i> : IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 • <i>ipv6-address</i> : 指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 • <i>interface-id</i> : Point-To-Point (ポイントツーポイント) インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 <p>(注) リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、<i>interface-id</i> を指定する必要があります (リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります)。</p> <ul style="list-style-type: none"> • <i>administrative distance</i> : (任意) アドミニストレーティブ ディスタンス。指定できる範囲は 1 ~ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルートタイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 4 show ipv6 static [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>] [interface <i>interface-id</i>] [recursive] [detail] または show ipv6 route static [<i>updated</i>]	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 <ul style="list-style-type: none"> • interface interface-id : (任意) 出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。 • recursive : (任意) 再帰スタティック ルートのみを表示します。 recursive キーワードは interface キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。 • detail : (任意) 次に示す追加情報を表示します。 <ul style="list-style-type: none"> – 有効な再帰ルートの場合、出力パス セットおよび最大分解深度 – 無効なルートの場合、ルートが無効な理由
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたスタティック ルートを削除するには、**no ipv6 route ipv6-prefix/prefix length {ipv6-address | interface-id [ipv6-address]} [administrative distance]** グローバル コンフィギュレーション コマンドを使用します。

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 RIP の設定

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ipv6 router rip name	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーション モードを開始します。
ステップ 3 maximum-paths number-paths	(任意) IPv6 RIP がサポートできる等コストルートの最大数を定義します。指定できる範囲は 1 ~ 64 で、デフォルトは 4 ルートです。
ステップ 4 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5 interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6 ipv6 rip name enable	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。

	コマンド	目的
ステップ7	<code>ipv6 rip name default-information {only originate}</code>	<p>(任意) IPv6 デフォルト ルート (:::0) を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。</p> <p>(注) 任意のインターフェイスから IPv6 デフォルト ルート (:::0) を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。</p> <ul style="list-style-type: none"> • only : デフォルト ルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • originate : デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ9	<code>show ipv6 rip [name] [interface interface-id] [database] [next-hops]</code> または <code>show ipv6 route rip [updated]</code>	IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをディセーブルにするには、**no ipv6 router rip name** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して RIP ルーティング プロセスをディセーブルにするには、**no ipv6 rip name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス `cisco` をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF の設定

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- スイッチ上で IP サービス イメージが稼働している必要があります。
- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須手順または任意の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 router ospf process-id	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ~ 65535 の正の整数を指定できます。
ステップ 3	area area-id range {ipv6-prefix/prefix length} [advertise not-advertise] [cost cost]	<p>(任意) エリア境界でルートを統合し、サマライズします。</p> <ul style="list-style-type: none"> • area-id : ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィックスのどちらかを指定できます。 • ipv6-prefix/prefix length : 宛先 IPv6 ネットワーク、およびプレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ (/) を付加する必要があります。 • advertise : (任意) Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • not-advertise : (任意) アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • cost cost : (任意) 現在のサマリー ルートのメトリックまたはコスト。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ~ 16777215 です。
ステップ 4	maximum paths number-paths	(任意) IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ~ 64 で、デフォルトは 16 です。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	ipv6 ospf process-id area area-id [instance instance-id]	<p>インターフェイス上で IPv6 OSPF をイネーブルにします。</p> <p>instance instance-id : (任意) インスタンス ID</p>
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ9	show ipv6 ospf [<i>process-id</i>] [<i>area-id</i>] interface [<i>interface-id</i>] または show ipv6 ospf [<i>process-id</i>] [<i>area-id</i>]	OSPF インターフェイスの情報を表示します。 OSPF ルーティング プロセスに関する一般的な情報を表示します。
ステップ10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf process-id area area-id** インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 の EIGRP の設定

EIGRP IPv6 をイネーブルにするには、インターフェイスで **ipv6 router eigrp as-number** コマンドおよび **ipv6 eigrp as-number** コマンドを設定します。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**eigrp router-id ip-address** コマンドを使用します。

スイッチ上で IP サービス イメージが稼働している必要があります。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv4 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface default** コマンドを使用して、すべてのインターフェイスをパッシブに設定してから、選択されたインターフェイスで **no passive-interface** コマンドを使用し、これらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の HSRP の設定

IPv6 の HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。

スイッチで IPv6 の HSRP がイネーブルである場合、IPv6 ホストは IPv6 ネイバー探索ルータのアドバタイズメント メッセージから使用可能な IPv6 ルータを学習します。HSRP IPv6 グループには、HSRP グループ番号に基づいて作成される仮想 MAC アドレスがあります。グループには、デフォルトで、HSRP 仮想 MAC アドレスに基づいて作成される仮想 IPv6 リンクローカル アドレスがあります。HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。

スイッチ上で IP サービス イメージが稼働している必要があります。

IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2 (HSRPv2) をイネーブルにする必要があります。

HSRPv1 および HSRPv2 を使用して IPv6 の HSRP を設定する場合の設定に関する注意事項については、「[HSRP HSRP 設定時の注意事項](#)」(P.46-6) および「[HSRP のトラブルシューティング](#)」(P.46-12) を参照してください。

IPv6 の HSRP および HSRPv2 の詳細については、[第 46 章「HSRP および VRRP の設定」](#) を参照してください。



(注) IPv6 の HSRP グループを設定する前に、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 の HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

レイヤ 3 インターフェイス上で HSRPv2 をイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始して、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	standby version {1 2}	HSRP バージョンを変更するには、 2 を入力します。デフォルトは 1 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show standby	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 の HSRP グループのイネーブル化

レイヤ 3 インターフェイス上で IPv6 の HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、IPv6 の HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。

コマンド	目的
ステップ3 <code>standby [group-number] ipv6 {link-local-address autoconfig}</code>	IPv6 の HSRP グループを作成、(またはイネーブルに) する <ul style="list-style-type: none"> • (任意) group-number : HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 4095 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • ホットスタンバイ ルータ インターフェイスのリンクローカルアドレスを入力するか、リンクローカルプレフィックスおよび変更された EUI-64 形式のインターフェイス ID から自動的に生成されるリンクローカルアドレスをイネーブルにします。この場合、EUI-64 インターフェイス ID は、関連する HSRP 仮想 MAC アドレスから作成されません。
ステップ4 <code>standby [group-number] preempt [delay {minimum seconds reload seconds sync seconds}]</code>	ルータを preempt に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。 <ul style="list-style-type: none"> • (任意) group-number : コマンドが適用されるグループ番号です。 • (任意) delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 秒です (1 時間)。デフォルトは 0 です (引き継ぐまで遅延がない)。 • (任意) reload : リロード後のプリエンブション遅延 (秒) を設定します。遅延時間は、ルータのリロード後の最初のインターフェイスアップ イベントに対してだけ適用されます。 • (任意) sync : IP 冗長クライアントの最大同期化時間 (秒) を設定します。 デフォルト値に戻すには、このコマンドの no 形式を使用します。
ステップ5 <code>standby [group-number] priority priority</code>	アクティブ ルータを選択するときに使用される priority 値を設定します。指定できる範囲は 1 ~ 255 です。デフォルトプライオリティは 100 です。最大の値が、最高のプライオリティを表します。 デフォルト値に戻すには、このコマンドの no 形式を使用します。
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ7 <code>show standby [interface-id [group-number]]</code>	設定を確認します。
ステップ8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 の HSRP をディセーブルにするには、`no standby [group-number] ipv6` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのグループ 1 で IPv6 の HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、IPv6 の HSRP を使用して学習されます。



(注) これは、IPv6 の HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

IPv6 の HSRP の設定の詳細については、Cisco.com で『Cisco IOS IPv6 Configuration Library』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンドリファレンスを参照してください。

表 42-2 に、スイッチ上で IPv6 をモニタするための特権 EXEC コマンドを示します。

表 42-2 IPv6 のモニタリング用コマンド

コマンド	目的
show ipv6 access-list	アクセスリストのサマリーを表示します。
show ipv6 cef	IPv6 CEF を表示します。
show ipv6 interface interface-id	IPv6 インターフェイスのステータスおよび設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 42-3 に、EIGRP IPv6 情報を表示するための特権 EXEC コマンドを示します。

表 42-3 EIGRP IPv6 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [as-number] interface	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [as-number] neighbor	EIGRP IPv6 で検出されたネイバーを表示します。

表 42-3 EIGRP IPv6 情報を表示するためのコマンド (続き)

コマンド	目的
<code>show ipv6 eigrp [as-number] traffic</code>	送受信される EIGRP IPv6 パケット数を表示します。
<code>show ipv6 eigrp topology [as-number ipv6-address] [active all-links detail-links pending summary zero-successors]</code>	IPv6 トポロジテーブルの EIGRP エントリを表示します。

表 42-4 に、IPv4 および IPv6 のアドレス タイプに関する情報を表示するための特権 EXEC コマンドを示します。

表 42-4 IPv4 および IPv6 のアドレス タイプの表示用コマンド

コマンド	目的
<code>show ip http server history</code>	アクセスした IP アドレス、接続が終了したときの時間を含む、最近 20 回の HTTP サーバへの接続を表示します。
<code>show ip http server connection</code>	アクセスしているローカルおよびリモート IP アドレスを含む、HTTP サーバへの現在の接続を表示します。
<code>show ip http client connection</code>	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
<code>show ip http client history</code>	サーバに対して HTTP クライアントが行った最後の 20 回の要求のリストを表示します。

次に、`show ipv6 interface` 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
  3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
<output truncated>
```

次に、`show ipv6 cef` 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
```

```

3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to FastEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to FastEthernet2/0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
  attached to Loopback10
3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<output truncated>

```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
    FastEthernet0/4
    FastEthernet0/11
    FastEthernet0/12
    FastEthernet1/4
    FastEthernet1/6
    FastEthernet1/7
  Redistribution:
    None

```

次に、**show ipv6 rip** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
  Redistribution:
    None

```

次に、**show ipv6 static** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1

```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
3FFE:C000:0:7::777                         - 0007.0007.0007 REACH V17
3FFE:C101:113:1::33                        - 0000.0000.0033 REACH Fa1/0/13

```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L   FF00::/8 [0/0]
    via Null0, receive
```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd: 1 total, 1 local destination
        0 source-routed, 0 truncated
        0 format errors, 0 hop count exceeded
        0 bad header, 0 unknown option, 0 bad source
        0 unknown protocol, 0 not a router
        0 fragments, 0 total reassembled
        0 reassembly timeouts, 0 reassembly failures
  Sent: 36861 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
        0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```




CHAPTER 43

IPv6 マルチキャストの実装

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6 マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

ここでは、IPv6 マルチキャストを設定する方法について説明します。コマンドリファレンスについては、『[Cisco IOS IPv6 Command Reference](#)』を参照してください。

IPv6 マルチキャストの実装に関する情報

- 「IPv6 マルチキャストの概要」 (P.43-1)
- 「IPv6 マルチキャスト ルーティングの実装」 (P.43-2)
- 「プロトコル独立マルチキャスト」 (P.43-5)
- 「スタティック mroute」 (P.43-11)
- 「MRIB」 (P.43-11)
- 「MFIB」 (P.43-11)
- 「IPv6 マルチキャスト VRF Lite」 (P.43-12)
- 「IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング」 (P.43-12)
- 「IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP」 (P.43-13)
- 「IPv6 マルチキャストでの NSF と SSO のサポート」 (P.43-14)
- 「IPv6 マルチキャストの帯域幅ベースの CAC」 (P.43-14)

IPv6 マルチキャストの概要

IPv6 マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLD プロトコルを使用して行われます。

スイッチは、MLD プロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。ネットワークでは、各サブネットでマルチキャスト データのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。マルチキャスト パケットは、IPv6 ユニキャスト パケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャスト アドレスがマルチキャスト グループの受信先として選択されます。送信者は、データ グラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバを含むグループにアクティビティがない場合もあります。



(注)

IPv6 マルチキャスト ルーティングは、IP ベース イメージでのみサポートされます。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル (IGMP) for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります (RFC 2710 で規定)。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。
- PIM in Source Specific Multicast (PIM-SSM) は PIM-SM と類似していますが、IP マルチキャスト アドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

マルチキャスト リスナー ディスカバリ プロトコル for IPv6

キャンパス ネットワークでマルチキャストの実装を開始するには、ユーザは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLD プロトコルは、直接接続されているリンク上のマルチキャストリスナー（たとえば、マルチキャスト パケットを受信するノード）の存在を検出するため、およびこれらのネイバー ノードを対象にしている特定のマルチキャスト アドレスを検出するために、IPv6 スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループメ

メンバーシップの検出に使用されます。MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアおよびホストの違いは次のとおりです。

- クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。
- ホストは、レポート メッセージを送信して、クエリアにホスト メンバーシップを通知する受信側（スイッチを含む）です。

同じ送信元からのマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャスト グループに対する加入および脱退を行ったり、グループ トラフィックの受信を開始したりします。

MLD では、メッセージの伝送にインターネット制御メッセージ プロトコル (ICMP) が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチ アラート オプションが設定されています。スイッチ アラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD では、次の 3 種類のメッセージが使用されます。

- クエリー：一般、グループ固有、およびマルチキャスト アドレス固有。MLD から一般クエリーが送信されると、マルチキャスト アドレス フィールドは 0 に設定されます。一般クエリーでは、接続されているリンク上にリスナーが存在するマルチキャスト アドレスを学習します。

グループ固有のクエリーとマルチキャスト アドレス固有のクエリーはどちらも、マルチキャスト アドレス フィールドをクエリーされているアドレスに設定します。グループ アドレスはマルチキャスト アドレスです。

- レポート：レポート メッセージでは、マルチキャスト アドレス フィールドは、送信側がリッスンしている特定の IPv6 マルチキャスト アドレスのフィールドになります。
- Done : Done メッセージでは、マルチキャスト アドレス フィールドは、MLD メッセージの送信元がすでにリッスンしていない特定の IPv6 マルチキャスト アドレスのフィールドになります。



(注)

MLD バージョン 2 には、Done メッセージはありません。

MLD レポートの送信には、有効な IPv6 リンクローカル送信元アドレスを使用するか、または送信側 インターフェイスが有効なリンクローカル アドレスをまだ取得していない場合は未指定アドレス (::) を使用する必要があります。未指定アドレスでのレポートの送信は、ネイバー探索プロトコルでの IPv6 マルチキャストの使用をサポートできます。

ステートレス自動設定で Duplicate Address Detection (DAD; 重複アドレス検出) を実行するためには、ノードは複数の IPv6 マルチキャスト グループに加入する必要があります。DAD を実行する前は、インターフェイスの送信用にレポート ノードが使用するアドレスは一時的なアドレスのみであり、通信には使用できません。そのため、未指定アドレスを使用する必要があります。

MLD バージョン 2 または MLD バージョン 1 のメンバーシップ レポートから生成される MLD ステータスは、グローバルに、またはインターフェイス単位で制限できます。MLD グループ制限機能は、MLD パケットによって生じる Denial of Service (DoS; サービス拒絶) 攻撃に対する保護を提供します。設定されている制限を超過するメンバーシップ レポートは MLD キャッシュには格納されず、これらの超過メンバーシップ レポートのトラフィックは転送されません。

MLD では、送信元フィルタリングがサポートされています。送信元フィルタリングにより、特定の送信元アドレスからのパケット (SSM をサポートするのに必要)、または特定の送信元アドレスを除くすべてのアドレスから特定のマルチキャスト アドレスに送信されたパケットをリッスンする対象をノードがレポートできるようになります。

MLD を使用するホストが **Leave** メッセージを送信した場合、スイッチはクエリー メッセージを送信することによって、このホストがグループに加入した最後のホストであることを再確認する必要があります。再確認後、トラフィックの転送を停止できます。この処理には約 2 秒かかります。この「脱退遅延」は、IPv4 マルチキャスト対応 IGMP バージョン 2 にも存在します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

IPv6 マルチキャスト ユーザ認証およびプロファイル サポート

IPv6 マルチキャストは、ネットワーク内の任意のホストがマルチキャスト グループの受信側または送信元になれる設計になっています。したがって、ネットワークのマルチキャスト トラフィックを制御するには、マルチキャスト アクセス コントロールが必要です。アクセス コントロール機能は、主に、送信元のアクセス コントロールとアカウントティング、受信側のアクセス コントロールとアカウントティング、およびこのアクセス コントロール メカニズムのプロビジョニングで構成されます。

マルチキャスト アクセス コントロールは、マルチキャストと認証、認可、アカウントティング (AAA) 間のインターフェイスを提供し、ラストホップ スイッチ、マルチキャストにおける受信側アクセス コントロール機能、およびマルチキャストにおけるグループまたはチャネル ディセーブル化機能でのプロビジョニング、認可、およびアカウントティングを実現します。

新しいマルチキャスト サービス環境を展開する場合、ユーザ認証を追加し、インターフェイス単位でユーザ プロファイルのダウンロードを行う必要があります。AAA と IPv6 マルチキャストを使用すると、マルチキャスト環境でのユーザ認証とユーザ プロファイルのダウンロードがサポートされます。

RADIUS サーバからアクセス スイッチへのマルチキャスト アクセス コントロール プロファイルのダウンロードをトリガーするイベントは、アクセス スイッチへの MLD join の着信です。このイベントが発生すると、ユーザは認可キャッシュのタイムアウトが発生させて定期的なダウンロードを要求するか、または適切な **multicast clear** コマンドを使用してプロファイルが変更された場合に新規ダウンロードをトリガーできます。

アカウントティングは RADIUS アカウントティングを使用して行われます。開始および停止アカウントティング レコードは、アクセス スイッチから RADIUS サーバに送信されます。リソースの消費をストリーム単位で追跡できるように、これらのアカウントティング レコードには、マルチキャスト送信元およびグループに関する情報が含まれています。ラストホップ スイッチが新しい MLD レポートを受信すると、開始レコードが送信され、MLD leave を受信するか、何らかの理由によりグループまたはチャネルが削除されると、停止レコードが送信されます。

IPv6 MLD プロキシ

MLD プロキシ機能は、スイッチのアップストリーム インターフェイス上で、スイッチがすべての (*, G) および (S, G) エントリに対して MLD メンバーシップ レポートを生成するか、またはこれらのエントリのユーザ定義サブセットを生成するメカニズムを提供します。MLD プロキシ機能により、デバイスは、プロキシグループ メンバーシップ情報を学習し、その情報に基づいてマルチキャスト パケットを転送できるようになります。

スイッチが mroute プロキシ エントリの RP として動作する場合、これらのエントリの MLD メンバーシップ レポートを、ユーザが指定したプロキシ インターフェイス上で生成できます。

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト (PIM) は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding (RPF) チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャスト ルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー (SPT) の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをブルーニング (削除) 送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステータスは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ (DR) は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの (*, G) マルチ

キャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

指定スイッチ

Cisco スイッチは、LAN セグメント上に複数のスイッチが存在する場合、PIM-SM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って指定スイッチを選択します。

指定スイッチは、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、アクティブな送信元およびホスト グループ メンバーシップに関する情報を通知します。

LAN 上に複数の PIM-SM スイッチが存在する場合は、指定スイッチを選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。 `ipv6 pim dr-priority` コマンドを使用して DR の選択を強制することを選択しない限り、最も大きい IPv6 アドレスの PIM スイッチが LAN の DR になります。このコマンドでは、LAN セグメント上の各スイッチの DR プライオリティ (デフォルトのプライオリティ = 1) を指定して、最もプライオリティの高いスイッチが DR として選択されるようにすることができます。LAN セグメント上のすべてのスイッチのプライオリティが同じ場合にも、最上位 IPv6 アドレスを持つスイッチが使用されます。

DR で障害が発生した場合、PIM-SM はスイッチ A の障害を検出し、フェールオーバー DR を選択する手段を提供します。DR (スイッチ A) が動作不能になった場合、スイッチ A とネイバーとの隣接関係がタイムアウトすると、スイッチ B はその状況を検出します。スイッチ B はホスト A から MLD メンバーシップ レポートを受けているため、このインターフェイスでグループ A の MLD ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。この段階で、スイッチ B を経由する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。また、ホスト A がトラフィックを送信していた場合、スイッチ B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。このアクションがトリガーとなって、RP は、スイッチ B を経由する新しいブランチを介して、ホスト A への SPT に加入します。



(注)

- 2 つの PIM スイッチが直接接続されている場合、これらのスイッチはネイバーになります。PIM ネイバーを表示するには、`show ipv6 pim neighbor` 特権 EXEC コマンドを使用します。
- DR 選択プロセスは、マルチアクセス LAN のみで必要です。

Rendezvous Point

IPv6 PIM では、組み込み RP がサポートされています。組み込み RP サポートを利用すると、スイッチは、スタティックに設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。スイッチが RP である場合、RP としてスタティックに設定する必要があります。

スイッチは、MLD レポート内、または PIM メッセージおよびデータ パケット内の組み込み RP グループアドレスを検索します。このようなアドレスが見つかったら、スイッチはアドレス自体からグループの RP を学習します。この学習された RP は、グループのすべてのプロトコル アクティビティに使用されます。スイッチが RP である場合、組み込み RP を RP として設定する必要があり、スイッチはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセス リストに設定する必要があります。PIM がスパス モードで設定されている場合は、RP として動作する 1 つ以上のスイッチを選択する必要もあります。RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップ スイッチによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパース モードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに、ファーストホップ スイッチによって PIM register メッセージを送信するために使用されます。また、RP アドレスは、ラストホップ スイッチによって PIM join および prune メッセージを RP に送信してグループ メンバーシップについて通知するためにも使用されます。すべてのスイッチ (RP スイッチを含む) で RP アドレスを設定する必要があります。

1 つの PIM スイッチを複数のグループの RP にすることができます。特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセス リストで指定されている条件によって、スイッチがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。ユーザは、アクセス リストを照合するか、または登録されている送信元の AS パスとルート マップに指定されている AS パスを比較できます。

PIMv6 エニーキャスト RP ソリューションの概要

IPv6 PIM のエニーキャスト RP ソリューションは、IPv6 ネットワークによる PIM-SM RP のエニーキャスト サービスのサポートを可能にします。これにより、PIM のみを実行するドメイン内でエニーキャスト RP を使用できるようになります。この機能は、ドメイン間接続が不要な場合に便利です。エニーキャスト RP は、IPv4 および IPv6 で使用できますが、IPv4 だけで動作する Multicast Source Discovery Protocol (MSDP) には依存しません。

エニーキャスト RP は、PIM RP のデバイスに障害が発生した場合に、高速コンバージェンスを取得するために ISP ベースのバックボーンが使用するメカニズムです。受信側および送信元が最も近くの RP にランデブーできるようにするには、送信元からのパケットがすべての RP に到達して、加入している受信側を検出する必要があります。

ユニキャスト IP アドレスは RP アドレスとして選択されます。このアドレスは、静的に設定されるか、またはダイナミック プロトコルを使用して、ドメイン全体のすべての PIM デバイスに配信されます。ドメイン内の一連のデバイスが、この RP アドレスの RP として動作するように選択されます。これらのデバイスは、エニーキャスト RP セットと呼ばれます。エニーキャスト RP セット内の各デバイスは、RP アドレスを使用してループバック インターフェイスで設定されます。また、エニーキャスト RP セット内の各デバイスには、RP 間の通信に使用する別の物理 IP アドレスも必要です。

RP アドレス、または RP アドレスに対応するプレフィックスは、ドメイン内部のユニキャストルーティング システムに挿入されます。エニーキャスト RP セット内の各デバイスは、エニーキャスト RP セット内のその他すべてのデバイスのアドレスで設定されます。また、この設定は、セット内のすべての RP で一致している必要があります。

IPv6 BSR : RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。PIM スイッチは、(*, G) join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G (グループ) がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、(*, G) ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ (C-BSR) として設定され、単一の BSR がそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補 RP (C-RP) として設定されます。通常、これらのスイッチは、C-BSR として設定されているものと同じスイッチです。候補 RP は、Candidate-RP-Advertisement (C-RP-Adv; 候補 RP アドバタイズメント) メッセージをそのドメインの BSR に定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。BSR は、定期的に発信する Bootstrap Message (BSM; ブートストラップ メッセージ) にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM 送信元固有マルチキャスト

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM-SM から派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。この情報は、MLD メンバーシップ レポートによってラストホップ スイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは (S, G) チャネルに基づいて配信されます。1 つの (S, G) チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、(S, G) チャネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は (S, G) チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

IPv6 用の SSM マッピング

IPv6 用の SSM マッピングでは、MLD バージョン 1 の受信側用にスタティックとダイナミックの両方のドメイン ネーム システム (DNS) マッピングがサポートされています。この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。

SSM マッピングにより、スイッチは実行コンフィギュレーションまたは DNS サーバのいずれかでマルチキャスト MLD バージョン 1 レポートの送信元を検索できるようになります。そのあと、スイッチは送信元に対する (S, G) join を開始できます。

PIM 共有ツリーおよび送信元ツリー (最短パス ツリー)

デフォルトでは、グループのメンバは、RP をルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。このタイプの配布ツリーは、共有ツリーまたはランデブーポイント ツリー (RPT) と呼ばれます (下の図を参照)。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループメンバに配布されます。

データしきい値で保証される場合、共有ツリー上のリーフスイッチは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。このタイプの配布ツリーは、最短パス ツリーまたは送信元ツリーと呼ばれます。デフォルトでは、Cisco IOS ソフトウェアは、送信元から最初のデータパケットを受信した時点で、送信元ツリーへの切り替えを行います。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフスイッチ C が RP に join メッセージを送信します。
2. RP がスイッチ C へのリンクを発信インターフェイスリストに登録します。
3. 送信元がデータを送信します。スイッチ A が register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のスイッチ C にデータを転送し、送信元に join メッセージを送信します。この時点で、データはスイッチ C に 2 回 (カプセル化された状態で 1 回、ネイティブの状態でも 1 回) 着信する可能性があります。
5. データがネイティブの (カプセル化されていない) 状態で RP に着信すると、RP はスイッチ A に register-stop メッセージを送信します。
6. デフォルトでは、最初のデータパケット受信時に、スイッチ C が Join メッセージを送信元に送信するよう要求します。
7. スイッチ C は、(S, G) でデータを受信すると、共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が (S, G) の発信インターフェイスからスイッチ C へのリンクを削除します。
9. RP が送信元への prune メッセージをトリガーします。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM スイッチで処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定スイッチによって送信され、グループの RP によって受信されます。

Reverse Path Forwarding

Reverse Path Forwarding は、マルチキャストデータグラムの転送に使用されます。これは、次のように機能します。

- スイッチで、送信元へのユニキャストパケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、スイッチは、マルチキャストルーティングテーブルエントリの発信インターフェイスリストに存在するインターフェイスにパケットを転送します。
- パケットが RPF インターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM スイッチが送信元ツリー ステートである場合（つまり、(S, G) エントリがマルチキャストルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM スイッチが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバがグループに加入している場合は既知である）RP のアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。(S, G) join（送信元ツリー ステート）は送信元に向けて送信されます。(*, G) join（共有ツリー ステート）は RP に向けて送信されます。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクストホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

双方向 PIM

双方向 PIM により、マルチキャスト スイッチは、PIM-SM の単方向共有ツリーと比較して、保持するステート情報を減らすことができます。双方向共有ツリーは、データを送信元からランデブー ポイント アドレス (RPA) に伝送し、それらを RPA から受信側に配布します。PIM-SM とは異なり、双方向 PIM は送信元ツリーへの切り替えは実行しません。また、送信元から RP へのデータの登録カプセル化は行われません。

指定された単一のフォワーダ (DF) が、双方向 PIM ドメイン内のすべてのリンク（マルチアクセスおよびポイントツーポイント リンクを含む）の各 RPA 用に存在しています。唯一の例外は、DF が存在しない RPL です。DF は、MRIB が提供するメトリックとの比較で決定される、RPA への最適なルートを持つリンク上のスイッチです。指定された RPA の DF は、リンクにダウンストリーム トラフィックを転送し、リンクからのアップストリーム トラフィックをランデブー ポイント リンク (RPL) に転送します。DF は、RPA にマップするすべての双方向グループに対してこの機能を実行します。また、

リンク上の DF は、リンク上のダウンストリーム スイッチからの Join メッセージを処理するとともに、MLD などのローカル メンバシップ メカニズムによって検出されたローカル受信者にパケットが転送されることを保証します。

双方向 PIM は、中レートまたは低レートの送信元が多数存在する場合に役立ちます。ただし、双方向共有ツリーの遅延特性は、PIM-SM で構築された送信元ツリーよりもさらに劣る可能性があります (トポロジに依存)。

IPv6 では、双方向 RP のスタティック設定だけがサポートされています。

スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

Multicast Routing Information Base (MRIB; マルチキャスト ルーティング情報ベース) は、マルチキャスト ルーティング プロトコル (ルーティング クライアント) によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティング プロトコルと Multicast Forwarding Information Base (MFIB; マルチキャスト転送情報ベース) 間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。MRIB では、ルーティング クライアント以外に、転送クライアント (MFIB インスタンス) や特別なクライアント (MLD など) も扱われます。MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブルエ

ントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチングパスに関連付けられているルート キャッシュ管理の必要がなくなります。

分散型 MFIB

Distributed MFIB (dMFIB; 分散型 MFIB) は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。また、dMFIB には、ラインカード間での複製に関するプラットフォーム固有の情報も含まれることがあります。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

dMFIB は、次の機能を実装します。

- ラインカードに MFIB のコピーを配布します。
- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- MFIB プラットフォーム アプリケーション プログラム インターフェイス (API) を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり (パケットがデータ駆動型イベントのトリガーとなっている場合に必要)、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。
- RP に存在するクライアントがオンデマンドでトラフィックの統計情報を読み取れるようにするフックを提供します (dMFIB はこれらの統計情報を RP に定期的にアップロードすることはありません)。

また、dMFIB および MRIB サブシステムを組み合わせると、スイッチが各ラインカードで MFIB データベースの「カスタマイズ」コピーを保有したり、MFIB 関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6 マルチキャスト VRF Lite

IPv6 マルチキャスト VRF Lite 機能は、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) コンテキストに対する IPv6 マルチキャスト サポートを提供します。これらの VRF のスコープは、VRF が定義されているスイッチに制限されています。

この機能により、別の VRF に属するデバイス間の通信は、明示的に設定されていない限り許可されないため、より高いレベルのセキュリティでのルーティングと転送の切り分けができます。IPv6 マルチキャスト VRF Lite 機能は、特定の VRF に属するトラフィックの管理とトラブルシューティングを容易にします。

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。プロセス スイッチングでは、ルート プロセッサが各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システム メモリにコピーされます。次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、RP は、巡回冗長検査 (CRC) も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。(ARP などを使用して) 隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクスト ホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロード バランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報 (NLRI)、および IPv6 アドレスを使用するネクスト ホップ (宛先へのパス内の次のスイッチ) 属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ (IPv6 アドレス ファミリなど) および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPv6 は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier (SAFI) では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ (IPv6 ユニキャストとマルチキャストなど) を設定するために、個別の BGP ルーティング テーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストでの NSF と SSO のサポート

IPv6 マルチキャストでは、Nonstop Forwarding (NSF; ノンストップ フォワーディング) およびステートフル スイッチオーバー (SSO) がサポートされています。

IPv6 マルチキャストの帯域幅ベースの CAC

IPv6 マルチキャストの帯域幅ベースのコール アドミッション制御 (CAC) 機能は、コスト乗数を使用してインターフェイス単位の mroute ステートリミッタをカウントする手段を実装します。この機能を使用すると、マルチキャストフローで異なる量の帯域幅が使用されるネットワーク環境で、インターフェイス単位の帯域幅ベースの CAC を提供できます。

この機能では、IPv6 マルチキャスト ステートを詳細に制限および考慮します。この機能を設定すると、IPv6 マルチキャスト PIM トポロジの着信インターフェイスまたは発信インターフェイスとして使用できる回数にインターフェイスを制限できます。

この機能を使用すると、スイッチ管理者はアクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定して、インターフェイス制限に対してこのようなステートを考慮するときに使用するコスト乗数を指定できます。この機能では、異なる帯域幅要件に応じてコスト乗数を適切に調整することによって、帯域幅ベースのローカル CAC ポリシーを柔軟に実装できます。

IPv6 マルチキャストの実装

- 「IPv6 マルチキャストルーティングのイネーブル化」(P.43-14)
- 「MLD プロトコルのカスタマイズおよび確認」(P.43-15)
- 「PIM の設定」(P.43-21)
- 「BSR の設定」(P.43-25)
- 「SSM マッピングの設定」(P.43-27)
- 「スタティック mroute の設定」(P.43-28)
- 「IPv6 マルチキャストでの MFIB の使用」(P.43-29)

IPv6 マルチキャスト ルーティングのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 multicast-routing [vrf vrf-name]</code> 例： Switch(config)# <code>ipv6 multicast-routing</code>	すべての IPv6 対応インターフェイスでマルチキャストルーティングをイネーブルにし、イネーブルになっているすべてのスイッチインターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 3	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

- 「インターフェイスでの MLD のカスタマイズおよび確認」 (P.43-15)
- 「MLD グループ制限の実装」 (P.43-16)
- 「受信側の明示的トラッキングによってホストの動作を追跡するための設定」 (P.43-17)
- 「マルチキャスト ユーザ認証およびプロファイル サポートの設定」 (P.43-18)
- 「IPv6 での MLD プロキシのイネーブル化」 (P.43-19)
- 「MLD トラフィック カウンタのリセット」 (P.43-20)
- 「MLD インターフェイス カウンタのクリア」 (P.43-21)

インターフェイスでの MLD のカスタマイズおよび確認

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ3	ipv6 mld join-group [group-address] [include exclude] {source-address source-list [acl]} 例： Switch(config-if)# ipv6 mld join-group FF04::10	指定したグループおよび送信元に対して MLD レポートを設定します。
ステップ4	ipv6 mld access-group access-list-name 例： Switch(config-if)# ipv6 access-list acc-grp-1	ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。
ステップ5	ipv6 mld static-group group-address] [include exclude] {source-address source-list [acl]} 例： Switch(config-if)# ipv6 mld static-group ff04::10 include 100::1	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ6	ipv6 mld query-max-response-time seconds 例： Switch(config-if)# ipv6 mld query-max-response-time 20	MLD キューにアドバタイズされる最大応答時間を設定します。
ステップ7	ipv6 mld query-timeout seconds 例： Switch(config-if)# ipv6 mld query-timeout 130	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。

	コマンド	目的
ステップ 8	exit 例： Switch(config-if)# exit	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	show ipv6 mld [vrf vrf-name] groups [link-local] [group-name group-address] [interface-type interface-number] [detail explicit] 例： Switch# show ipv6 mld groups FastEthernet 2/1	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 10	show ipv6 mld groups summary 例： Switch# show ipv6 mld groups summary	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。
ステップ 11	show ipv6 mld [vrf vrf-name] interface [type number] 例： Switch# show ipv6 mld interface FastEthernet 2/1	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	debug ipv6 mld [group-name group-address interface-type] 例： Switch# debug ipv6 mld	MLD プロトコル アクティビティに対するデバッグをイネーブにします。
ステップ 13	debug ipv6 mld explicit [group-name group-address] 例： Switch# debug ipv6 mld explicit	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD 制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 mld [vrf vrf-name] state-limit number 例： Switch(config)# ipv6 mld state-limit 300	MLD ステートの数をグローバルに制限します。
ステップ3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ3	ipv6 mld limit number [except access-list] 例： Switch(config-if)# ipv6 mld limit 100	MLD ステートの数をインターフェイス単位で制限します。
ステップ4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ3	ipv6 mld explicit-tracking access-list-name 例： Switch(config-if)# ipv6 mld explicit-tracking list1	ホストの明示的トラッキングをイネーブルにします。
ステップ4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ユーザ認証およびプロファイル サポートの設定

マルチキャスト ユーザ認証およびプロファイル サポートを設定する前に、次の制約事項を認識しておく必要があります。

- ポート、インターフェイス、VC、または VLAN ID がユーザまたは加入者アイデンティティになります。ホスト名、ユーザ ID、またはパスワードを使用したユーザ アイデンティティはサポートされていません。
- IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化
- 方式リストの指定およびマルチキャスト アカウンティングのイネーブル化
- スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化
- MLD インターフェイスでの認可ステータスのリセット

IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model 例： Switch(config)# aaa new-model	AAA アクセス コントロール システムをイネーブルにします。
ステップ 3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

方式リストの指定およびマルチキャスト アカウンティングのイネーブル化

次の作業では、AAA 認およびアカウンティングに使用される方式リストを指定する方法、およびインターフェイス上の指定したグループまたはチャンネルでマルチキャスト アカウンティングをイネーブルにする方法を示します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization multicast default [method3 method4] 例： Switch(config)# aaa authorization multicast default	AAA 認可をイネーブルにし、IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 3	aaa accounting multicast default [start-stop stop-only] [broadcast] [method1] [method2] [method3] [method4] 例： Switch(config)# aaa accounting multicast default	課金、または RADIUS を使用する際のセキュリティのために、IPv6 マルチキャスト サービスの AAA アカウンティングをイネーブルにします。

	コマンド	目的
ステップ4	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ5	ipv6 multicast aaa account receive access-list-name [throttle throttle-number] 例： Switch(config-if)# ipv6 multicast aaa account receive list1	指定したグループまたはチャンネルで AAA アカウンティングをイネーブルにします。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化

状況によっては、アクセス コントロール プロファイルに従って加入者の認証とチャンネルの認可が行われていないかぎり、マルチキャスト トラフィックの受信を防止することが必要となる場合があります。つまり、アクセス コントロール プロファイルで特に指定がなければ、トラフィックを完全になくす必要があります。

未認証グループまたは未認可チャンネルからマルチキャスト トラフィックをスイッチが受信しないようにするには、次の作業を実行します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 multicast [vrf vrf-name] group-range[access-list-name] 例： Switch(config)# ipv6 multicast group-range	スイッチのすべてのインターフェイスで未認可グループまたはチャンネルのマルチキャスト プロトコル アクションおよびトラフィック転送をディセーブルにします。
ステップ3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 での MLD プロキシのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 mld host-proxy [group-acl] 例： Switch(config)# ipv6 mld host-proxy proxy-group	MLD プロキシ機能をイネーブルにします。
ステップ3	ipv6 mld host-proxy interface [group-acl] 例： Switch(config)# ipv6 mld host-proxy interface Ethernet 0/0	RP 上の指定したインターフェイス上で MLD プロキシ機能をイネーブルにします。

■ IPv6 マルチキャストの実装

	コマンド	目的
ステップ 4	show ipv6 mld host-proxy [<i>interface-type interface-number</i>] group [<i>group-address</i>]] 例： Switch(config)# show ipv6 mld host-proxy Ethernet0/0	IPv6 MLD ホスト プロキシ情報を表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイスでの認可ステータスのリセット

インターフェイスを指定しない場合は、すべての MLD インターフェイスで認可がリセットされます。
特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	clear ipv6 multicast aaa authorization [<i>interface-type interface-number</i>] 例： Switch# clear ipv6 multicast aaa authorization FastEthernet 1/0	IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータをクリアします。
ステップ 2	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	clear ipv6 mld [<i>vrf vrf-name</i>] traffic 例： Switch# clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。
ステップ 2	show ipv6 mld [<i>vrf vrf-name</i>] traffic 例： Switch# show ipv6 mld traffic	MLD トラフィック カウンタを表示します。
ステップ 3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ4	clear ipv6 mld [vrf vrf-name] counters interface-type 例： Switch# clear ipv6 mld counters Ethernet1/0	MLD インターフェイス カウンタをクリアします。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir] 例： Switch(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ3	exit 例： Switch(config)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します
ステップ4	show ipv6 pim [vrf vrf-name] interface [state-on] [state-off] [type number] 例： Switch# show ipv6 pim interface	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ5	show ipv6 pim [vrf vrf-name] group-map [group-name group-address] [group-range group-mask] [info-source {bsr default embedded-rp static}] 例： Switch# show ipv6 pim group-map	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ6	show ipv6 pim [vrf vrf-name] neighbor [detail] [interface-type interface-number count] 例： Switch# show ipv6 pim neighbor	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。

	コマンド	目的
ステップ 7	show ipv6 pim [vrf vrf-name] range-list [config] [rp-address rp-name] 例： Switch# show ipv6 pim range-list	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 8	show ipv6 pim [vrf vrf-name] tunnel [interface-type interface-number] 例： Switch# show ipv6 pim tunnel	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 9	debug ipv6 pim [group-name group-address interface interface-type bsr group mvpn neighbor] 例： Switch# debug ipv6 pim	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM オプションの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim [vrf vrf-name] spt-threshold infinity [group-list access-list-name] 例： Switch(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 3	ipv6 pim [vrf vrf-name] accept-register { list access-list route-map map-name} 例： Switch(config)# ipv6 pim accept-register route-map reg-filter	RP のレジスタを許可または拒否します。
ステップ 4	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	ipv6 pim dr-priority value 例： Switch(config-if)# ipv6 pim dr-priority 3	PIM スイッチの DR プライオリティを設定します。
ステップ 6	ipv6 pim hello-interval seconds 例： Switch(config-if)# ipv6 pim hello-interval 45	インターフェイスにおける PIM hello メッセージの頻度を設定します。

	コマンド	目的
ステップ7	ipv6 pim join-prune-interval <i>seconds</i> 例： Switch(config-if)# ipv6 pim join-prune-interval 75	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ8	exit 例： Switch(config-if)# exit	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ9	show ipv6 pim [vrf vrf-name] join-prune statistic [<i>interface-type</i>] 例： Switch# show ipv6 pim join-prune statistic	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

双方向 PIM の設定および双方向 PIM 情報の表示

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 pim [vrf vrf-name] rp-address <i>ipv6-address</i> [<i>group-access-list</i>] [bidir] 例： Switch(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir	特定のグループ範囲の PIM RP のアドレスを設定します。 bidir キーワードを使用すると、そのグループ範囲が双方向共有ツリー転送に使用されるようになります。
ステップ3	exit 例： Switch(config-if)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ4	show ipv6 pim [vrf vrf-name] df [<i>interface-type interface-number</i>] [<i>rp-address</i>] 例： Switch# show ipv6 pim df	RP の各インターフェイスの指定フォワーダ (DF) 選択ステータスを表示します。
ステップ5	show ipv6 pim [vrf vrf-name] df winner [<i>interface-type interface-number</i>] [<i>rp-address</i>] 例： Switch# show ipv6 pim df winner ethernet 1/0 200::1	各 RP の各インターフェイスの DF 選択ウィナーを表示します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリアされたら、ユーザは **show ipv6 pim traffic** コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	clear ipv6 pim [vrf vrf-name] traffic 例： Switch# clear ipv6 pim traffic	PIM トラフィック カウンタをリセットします。
ステップ 2	show ipv6 pim [vrf vrf-name] traffic 例： Switch# show ipv6 pim traffic	PIM トラフィック カウンタを表示します。
ステップ 3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	clear ipv6 pim [vrf vrf-name] topology [group-name group-address] 例： Switch# clear ipv6 pim topology FF04::10	PIM トポロジ テーブルをクリアします。
ステップ 2	show ipv6 mrib [vrf vrf-name] client [filter] [name {client-name client-name : client-id}] 例： Switch# show ipv6 mrib client	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 3	show ipv6 mrib [vrf vrf-name] route [link-local] summary [sourceaddress-or-name *] [groupname-or-address [prefix-length]] 例： Switch# show ipv6 mrib route	MRIB ルート情報を表示します。
ステップ 4	show ipv6 pim [vrf vrf-name] topology [groupname-or-address [sourcename-or-address]] link-local route-count [detail] 例： Switch# show ipv6 pim topology	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。

	コマンド	目的
ステップ5	debug ipv6 mrib [vrf vrf-name] client 例： Switch# debug ipv6 mrib client	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ6	debug ipv6 mrib [vrf vrf-name] io 例： Switch# debug ipv6 mrib io	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ7	debug ipv6 mrib proxy 例： Switch# debug ipv6 mrib proxy	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシアクティビティに対するデバッグをイネーブルにします。
ステップ8	debug ipv6 mrib [vrf vrf-name] route [group-name group-address] 例： Switch# debug ipv6 mrib route	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ9	debug ipv6 mrib [vrf vrf-name] table 例： Switch# debug ipv6 mrib table	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address[hash-mask-length] [priority priority-value] 例： Switch(config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10	候補 BSR になるようにスイッチを設定します。
ステップ3	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ4	ipv6 pim bsr border 例： Switch(config-if)# ipv6 pim bsr border	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。

	コマンド	目的
ステップ 5	exit 例： Switch(config-if)# exit	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	show ipv6 pim [vrf vrf-name] bsr {election rp-cache candidate-rp} 例： Switch# show ipv6 pim bsr election	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir] 例： Switch(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0	BSR に PIM RP アドバタイズメントを送信します。
ステップ 3	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 4	ipv6 pim bsr border 例： Switch(config-if)# ipv6 pim bsr border	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 pim [vrf vrf-name] bsr candidate bsr ipv6-address [hash-mask-length] [priority priority-value] 例： Switch(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4	候補 BSR になるようにスイッチを設定します。

	コマンド	目的
ステップ3	ipv6 pim [vrf vrf-name] bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] [scope scope-value] [bidir] 例： Switch(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ4	interface type number 例： Switch(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ5	ipv6 multicast boundary scope scope-value 例： Switch(config-if)# ipv6 multicast boundary scope 6	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 pim [vrf vrf-name] bsr announced rp ipv6-address [group-list access-list-name] [priority priority-value] [bidir] [scope scope-value] 例： Switch(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ3	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセスリストの送信元アドレスが使用されるようになります。



(注) DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバに直接接続される可能性があります。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld [vrf vrf-name] ssm-map enable 例： Switch(config)# ipv6 mld ssm-map enable	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 3	no ipv6 mld [vrf vrf-name] ssm-map query dns 例： Switch(config)# no ipv6 mld ssm-map query dns	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 4	ipv6 mld [vrf vrf-name] ssm-map static access-list source-address 例： Switch(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1	スタティック SSM マッピングを設定します。
ステップ 5	exit 例： Switch(config-if)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 6	show ipv6 mld [vrf vrf-name] ssm-map [source-address] 例： Switch# show ipv6 mld ssm-map	SSM マッピング情報を表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート (mroute) は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ipv6 route <i>ipv6-prefix / prefix-length ipv6-address</i> <i>interface-type interface-number ipv6-address</i> }} [<i>administrative-distance</i>] [<i>administrative-multicast-distance</i> unicast] multicast] [tag tag 例 : Switch(config)# ipv6 route 2001:DB8::/64 6::6 100	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ3	exit 例 : Switch(config-if)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ4	show ipv6 mroute [<i>vrf vrf-name</i>] [<i>link-local</i> [<i>group-name</i> <i>group-address</i> [<i>source-address</i> <i>source-name</i>]]] [summary] [count] 例 : Switch# show ipv6 mroute ff07::1	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ5	show ipv6 mroute [<i>vrf vrf-name</i>] [link-local <i>group-name</i> <i>group-address</i>] active [<i>kpbs</i>] 例 : Switch# show ipv6 mroute active	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ6	show ipv6 rpf [<i>vrf vrf-name</i>] <i>ipv6-prefix</i> 例 : Switch# show ipv6 rpf 2001:DB8::1:1:2	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show ipv6 mfib [<i>vrf vrf-name</i>] [<i>link-local</i> <i>verbose</i> <i>group-address-name</i> <i>ipv6-prefix / prefix-length</i> <i>source-address-name</i>] active count interface status summary 例： Switch# show ipv6 mfib	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 2	show ipv6 mfib [<i>vrf vrf-name</i>] [<i>link-local</i> <i>group-name</i> <i>group-address</i>] active [<i>kbps</i>] 例： Switch# show ipv6 mfib active	アクティブな送信元からマルチキャストグループへの送信レートを表示します。
ステップ 3	show ipv6 mfib [<i>vrf vrf-name</i>] [<i>all</i> <i>linkscope</i> <i>group-name</i> <i>group-address</i> [<i>source-name</i> <i>source-address</i>]] count 例： Switch# show ipv6 mfib count	MFIB からのグループおよび送信元に関するサマリートラフィック統計情報を表示します。
ステップ 4	show ipv6 mfib interface 例： Switch# show ipv6 mfib interface	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 5	show ipv6 mfib status 例： Switch# show ipv6 mfib status	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 6	show ipv6 mfib [<i>vrf vrf-name</i>] summary 例： Switch# show ipv6 mfib summary	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 7	debug ipv6 mfib [<i>vrf vrf-name</i>] [<i>group-name</i> <i>group-address</i>] [<i>adjacency</i> <i>db</i> <i>fs</i> <i>init</i> <i>interface</i> <i>mrrib</i> [<i>detail</i>] <i>nat</i> <i>pak</i> <i>platform</i> <i>ppr</i> <i>ps</i> <i>signal</i> <i>table</i>] 例： Switch# debug ipv6 mfib FF04::10 pak	IPv6 MFIB に対するデバッグ出力をイネーブルにします。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MFIB トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	clear ipv6 mfib [<i>vrf vrf-name</i>] counters [<i>group-name</i> group-address [<i>source-address</i> <i>source-name</i>]] 例： Switch# clear ipv6 mfib counters FF04::10	アクティブなすべての MFIB トラフィック カウンタをリセット します。
ステップ2	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



CHAPTER 44

IPv6 MLD スヌーピングの設定



(注)

Multicast Listener Discovery (MLD) スヌーピングを使用すると、IE 3000 スイッチ上で、スイッチドネットワーク内のクライアントやルータに IP Version 6 (IPv6) マルチキャスト データを効率的に配信することができます。IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理 (SDM) テンプレートがスイッチに設定されている必要があります。**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力して、テンプレートを選択します。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、[第 10 章「SDM テンプレートの設定」](#)を参照してください。
- スイッチの IPv6 については、[第 42 章「IPv6 ユニキャスト ルーティングの設定」](#)を参照してください。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- [「MLD スヌーピングの概要」 \(P.44-1\)](#)
- [「IPv6 MLD スヌーピングの設定」 \(P.44-5\)](#)
- [「MLD スヌーピング情報の表示」 \(P.44-12\)](#)

MLD スヌーピングの概要

IP バージョン 4 (IPv4) では、レイヤ 2 スイッチはインターネット グループ管理プロトコル (IGMP) スヌーピングを使用して、ダイナミックにレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッドを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN (仮想 LAN) 内のすべてのポートにフラッドされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、直接接続されたリンク上のマルチキャストリスナー (IPv6 マルチキャスト パケットを受信するノード) の存在、およびネイバー ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1 (MLDv1) は IGMPv2 と、MLD バージョン 2 (MLDv2) は IGMPv3 とそれぞれ同等です。MLD は ICMP バージョン 6 (ICMPv6) のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング : MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 Basic Snooping (MBSS; MLDv2 基本スヌーピング) : MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。



(注)

スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 Enhanced Snooping (MESS; MLDv2 拡張スヌーピング) をサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できません。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレス テーブルはソフトウェアで構築され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャスト アドレスに基づくブリッジングを実行します。

次に、IPv6 MLD スヌーピングの一部のパラメータについて説明します。

- 「MLD メッセージ」(P.44-2)
- 「MLD クエリー」(P.44-3)
- 「マルチキャスト クライアント エージングの堅牢性」(P.44-3)
- 「マルチキャスト ルータ検出」(P.44-3)
- 「MLD レポート」(P.44-4)
- 「MLD Done メッセージおよび即時脱退」(P.44-4)
- 「TCN 処理」(P.44-5)

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query : IGMPv2 クエリーと同等で、General Query または Multicast-Address-Specific Query (MASQ) のいずれかになります。
- Multicast Listener Report : IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ : IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに回答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。



(注)

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN (範囲 1006 ~ 4094) を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに回答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ (IGMP Leave メッセージと同等) を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ (直前にルータ制御パケットを送信したルータ) を追跡します。

- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポートもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、`ipv6 mld snooping last-listener-query count` グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応

答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping ten query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知 (TCN) 送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping ten flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定

次に、IPv6 MLD スヌーピングの設定方法について説明します。

- 「MLD スヌーピングのデフォルト設定」 (P.44-5)
- 「MLD スヌーピング設定時の注意事項」 (P.44-6)
- 「MLD スヌーピングのイネーブル化またはディセーブル化」 (P.44-6)
- 「スタティックなマルチキャスト グループの設定」 (P.44-8)
- 「マルチキャスト ルータ ポートの設定」 (P.44-8)
- 「MLD 即時脱退のイネーブル化」 (P.44-9)
- 「MLD スヌーピング クエリの設定」 (P.44-10)
- 「MLD リスナー メッセージ抑制のディセーブル化」 (P.44-11)

MLD スヌーピングのデフォルト設定

表 44-1 に、MLD スヌーピングのデフォルト設定を示します。

表 44-1 MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング (グローバル)	無効です。
MLD スヌーピング (VLAN 単位)	有効です。VLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	無効です。

表 44-1 MLD スヌーピングのデフォルト設定 (続き)

機能	デフォルト設定
MLD スヌーピングの堅牢性変数	グローバル : 2、VLAN 単位 : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル : 2、VLAN 単位 : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル : 1000 (1 秒)、VLAN : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	無効です。
TCN クエリー カウント	2
MLD リスナー抑制	有効です。

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN (範囲 1006 ~ 4094) を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチで保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチで保持可能なアドレス エントリの最大数は 1000 です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート (イネーブル) の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 mld snooping</code>	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ5	<code>reload</code>	OS (オペレーティング システム) をリロードします。

スイッチで MLD スヌーピングをグローバルにディセーブルにするには、`no ipv6 mld snooping` グローバル コンフィギュレーション コマンドを使用します。

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。



(注)

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN (範囲 1006 ~ 4094) を使用している場合は、IE 3000 スイッチが拡張 VLAN 上でクエリーを受信できるように、Catalyst 6500 スイッチ上で拡張 VLAN に対する IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 mld snooping</code>	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ3	<code>ipv6 mld snooping vlan <i>vlan-id</i></code>	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定した VLAN 番号に対して `no ipv6 mld snooping vlan vlan-id` グローバル コンフィギュレーション コマンドを使用します。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよびメンバ ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping vlan <i>vlan-id</i> static ipv6_multicast_address interface interface-id</code>	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループをスタティックに設定します。 <ul style="list-style-type: none"> <code>vlan-id</code> は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 <code>ipv6_multicast_address</code> は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 <code>interface-id</code> は、メンバ ポートです。物理インターフェイスまたはポート チャネル (1 ~ 48) に設定できます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 mld snooping multicast-address user</code> または <code>show ipv6 mld snooping multicast-address vlan vlan-id user</code>	スタティックなメンバ ポートおよび IPv6 アドレスを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、`no ipv6 mld snooping vlan vlan-id static mac-address interface interface-id` グローバル コンフィギュレーション コマンドを使用します。グループからすべてのメンバ ポートが削除された場合、このグループは削除されます。

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

MLD スヌーピングでは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習しますが、コマンドライン インターフェイス (CLI) を使用しても VLAN にマルチキャスト ルータ ポートを追加できます。マルチキャスト ルータ ポートを追加する (マルチキャスト ルータにスタティック接続を追加する) には、スイッチで `ipv6 mld snooping vlan mrouter` グローバル コンフィギュレーション コマンドを使用します。



(注)

マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></code>	マルチキャスト ルータの VLAN ID、およびマルチキャスト ルータにインターフェイスを指定します。 <ul style="list-style-type: none"> 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 48 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>]</code>	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ipv6 mld snooping vlan *vlan-id* mrouter interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにはなりません。

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave</code>	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show ipv6 mld snooping vlan <i>vlan-id</i></code>	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN で MLD 即時脱退をディセーブルにするには、**no ipv6 mld snooping vlan *vlan-id* immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピング クエリーの設定

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping robustness-variable value	(任意) スイッチが一般クエリーに回答しないリスナー (ポート) を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ~ 3 です。デフォルトは 2 です。
ステップ 3	ipv6 mld snooping vlan <i>vlan-id</i> robustness-variable value	(任意) VLAN 単位で堅牢性変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージングアウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ~ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	ipv6 mld snooping last-listener-query-count count	(任意) MLD クライアントがエージングアウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ~ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。
ステップ 5	ipv6 mld snooping vlan <i>vlan-id</i> last-listener-query-count count	(任意) VLAN 単位で最後のリスナー クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ~ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1 秒後に送信されます。
ステップ 6	ipv6 mld snooping last-listener-query-interval interval	(任意) スイッチが MASQ を送信した後、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ~ 32,768 ミリ秒です。デフォルト値は 1000 (1 秒) です。
ステップ 7	ipv6 mld snooping vlan <i>vlan-id</i> last-listener-query-interval interval	(任意) VLAN 単位で最後のリスナー クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ~ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	ipv6 mld snooping tcn query solicit	(任意) TCN 送信請求をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッドイングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	ipv6 mld snooping tcn flood query count count	(任意) TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ~ 10 で、デフォルトは 2 です。
ステップ 10	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	show ipv6 mld snooping querier [vlan vlan-id]	(任意) スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル (最大応答時間) を 2000 (2 秒) に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no ipv6 mld snooping listener-message-suppression	MLD メッセージ抑制をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD メッセージ抑制を再びイネーブルにするには、`ipv6 mld snooping listener-message-suppression` グローバル コンフィギュレーション コマンドを使用します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには、表 44-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 44-2 MLD スヌーピング情報表示用のコマンド

コマンド	目的
<code>show ipv6 mld snooping [vlan vlan-id]</code>	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 (任意) 個々の VLAN に関する情報を表示するには、 <code>vlan vlan-id</code> を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show ipv6 mld snooping mrouter [vlan vlan-id]</code>	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 (任意) 個々の VLAN に関する情報を表示するには、 <code>vlan vlan-id</code> を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show ipv6 mld snooping querier [vlan vlan-id]</code>	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレス および着信ポートに関する情報を表示します。 (任意) <code>vlan vlan-id</code> を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show ipv6 mld snooping multicast-address [vlan vlan-id] [count dynamic user]</code>	スイッチまたは VLAN のすべてあるいは特定の IPv6 マルチキャスト アドレス情報を表示します。 <ul style="list-style-type: none"> <code>count</code> を入力して、スイッチまたは VLAN のグループ数を表示します。 <code>dynamic</code> を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 <code>user</code> を入力して、スイッチまたは VLAN の MLD スヌーピングユーザ設定グループ情報を表示します。
<code>show ipv6 mld snooping multicast-address vlan vlan-id [ipv6-multicast-address]</code>	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。



CHAPTER 45

IPv6 ACL の設定

この章では、IE3000 スイッチに IPv6 ACL を設定する方法について説明します。IP バージョン 6 (IPv6) Access Control List (ACL; アクセス コントロール リスト) を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP バージョン 4 (IPv4) の名前付き ACL を作成し、適用する方法と同じです。レイヤ 3 管理トラフィックをフィルタリングするために、入力ルータ ACL を作成し、適用することもできます。



(注) IPv6 を使用するには、デュアル IPv4 および IPv6 Switching Database Management (SDM; スイッチング データベース管理) テンプレートがスイッチに設定されている必要があります。テンプレートの選択は、`sdm prefer {default | dual-ipv4-and-ipv6}` グローバル コンフィギュレーション コマンドで行います。IPv6 の ACL をサポートするのは、IP サービス イメージが稼働しているスイッチだけです。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、[第 10 章「SDM テンプレートの設定」](#)を参照してください。
- IP Version 4 (IPv4) 用の IP ACLS の詳細については、[第 38 章「ACL によるネットワーク セキュリティの設定」](#)を参照してください。



(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「IPv6 ACL の概要」(P.45-1)
- 「IPv6 ACL の設定」(P.45-3)
- 「IPv6 ACL の表示」(P.45-8)

IPv6 ACL の概要

スイッチ イメージは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL
 - ルーテッド ポート、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、またはレイヤ 3 EtherChannel などのレイヤ 3 インターフェイスの発信トラフィックまたは着信トラフィックでサポートされます。
 - 経路選択済みの IPv6 パケットだけに適用されます。

- IPv6 ポート ACL
 - レイヤ 2 インターフェイスのインバウンドトラフィックだけでサポートされます。
 - インターフェイスに届くすべての IPv6 パケットに適用されます。



(注)

サポートされない IPv6 ACL を設定した場合、エラーメッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN (VLAN) ACL (VLAN マップ) をサポートしません。



(注)

スイッチでの ACL サポートの詳細については、第 38 章「ACL によるネットワークセキュリティの設定」を参照してください。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。

IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。



(注)

いずれかのポート ACL (IPv4、IPv6、または MAC) がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

ここでは、スイッチの IPv6 ACL の特性の一部について説明します。

- 「サポートされる ACL 機能」(P.45-2)
- 「IPv6 ACL の制限事項」(P.45-3)

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム (IPv4 では **fragments** キーワード) がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スwitchの Ternary CAM (TCAM) スペースが不足している場合、ACL ラベルに対応付けられたパケットは CPU に転送され、ACL はソフトウェアで適用されます。
- ホップバイホップ オプションがあるルーテッドパケットまたはブリッジドパケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ログギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

IPv6 ACL の制限事項

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- IPv6 送信元および宛先アドレス：ACL 照合は、Extended Universal Identifier (EUI) -64 形式の /0 ~ /64 のプレフィックスおよびホスト アドレス (/128) だけでサポートされます。スイッチは、情報損失のない次のホスト アドレスだけをサポートします。
 - 集約グローバルユニキャスト アドレス
 - リンクに対してローカルなアドレス
- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL (**reflect** キーワード) をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL (VLAN マップ) はサポートしていません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- スイッチは出力ポート ACL をサポートしません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、スイッチだけでサポートされます。スイッチは、コントロールプレーン (着信) IPv6 ACL だけをサポートします。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス (物理ポートまたは SVI) に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうかを判断します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つ Access Control Entry (ACE; アクセス コントロール エントリ) を追加しようとする場合、スイッチは現在インターフェイスに接続されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL の設定

IPv6 ACL を設定する場合は、事前にデュアル IPv4/IPv6 SDM テンプレートのいずれかを選択する必要があります。

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

-
- ステップ 1** IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
 - ステップ 2** IPv6 ACL が、トラフィックをブロックする (拒否) または通過させる (許可) よう設定します。
 - ステップ 3** インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。
-

ここでは、IPv6 ACL の設定および適用方法について説明します。

- 「IPv6 ACL のデフォルト設定」(P.45-4)

- 「他の機能との相互作用」 (P.45-4)
- 「IPv6 ACL の作成」 (P.45-4)
- 「インターフェイスへの IPv6 ACL の適用」 (P.45-7)

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能との相互作用

IPv6 ACL の設定には、他の機能またはスイッチ特性と次の相互作用があります。

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはドロップされます。パケットのコピーがインターネット制御メッセージプロトコル (ICMP) キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジドフレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチに作成したり、同一インターフェイスに適用したりできます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラーメッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると (たとえば、IPv6 ACL の付加に IPv4 コマンドを使用するなど)、エラーメッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- TCAM が満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 access-list <i>access-list-name</i></code>	IPv6 アクセス リスト名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3a deny permit <i>protocol</i> { <i>source-ipv6-prefix/prefix-length</i> any host <i>source-ipv6-address</i> } [<i>operator</i> [<i>port-number</i>]] { <i>destination-ipv6-prefix/</i> <i>prefix-length</i> any host <i>destination-ipv6-address</i> } [<i>operator</i> [<i>port-number</i>]] [dscp <i>value</i>] [fragments] [log] [log-input] [<i>sequence value</i>] [time-range <i>name</i>]	<p>条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。</p> <ul style="list-style-type: none"> <i>protocol</i> には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ~ 255 の整数を使用できます。ICMP、TCP、および UDP の具体的なパラメータについては、ステップ 3b ~ 3d を参照してください。 <i>source-ipv6-prefix/prefix-length</i> または <i>destination-ipv6-prefix/prefix-length</i> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、16 ビット値を使用したコロン区切りの 16 進形式で指定されます (RFC 2373 を参照)。 <p>(注) CLI (コマンドライン インターフェイス) ヘルプでは、/0 ~ /128 の範囲のプレフィックス長が表示されますが、スイッチは、集約可能なグローバルユニキャストアドレスとリンクに対してローカルなホストアドレスの /0 ~ /64 の範囲のプレフィックス、および EUI ベースの /128 プレフィックスに対する IPv6 アドレス照合だけをサポートします。</p> <ul style="list-style-type: none"> IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 host <i>source-ipv6-address</i> または <i>destination-ipv6-address</i> には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 (任意) <i>operator</i> には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、range (包含範囲) があります。 <p><i>source-ipv6-prefix/prefix-length</i> 引数のあとの <i>operator</i> は、送信元ポートに一致する必要があります。<i>destination-ipv6-prefix/prefix-length</i> 引数のあとの <i>operator</i> は、宛先ポートに一致する必要があります。</p> <ul style="list-style-type: none"> (任意) <i>port-number</i> は、TCP または UDP のフィルタリングで、それぞれ 0 ~ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 (任意) dscp <i>value</i> を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ~ 63 です。 (任意) fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 (任意) log を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 (任意) sequence <i>value</i> を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 (任意) time-range <i>name</i> を入力して、ステートメントの時間の範囲を指定します。

	コマンド	目的
ステップ 3b	<pre>deny permit tcp {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6- prefix/prefix-length any host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port protocol}] [psh] [range {port protocol}] [rst] [sequence value] [syn] [time-range name] [urg]</pre>	<p>(任意) TCP アクセス リストおよびアクセス条件を定義します。</p> <p>TCP の場合は tcp を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。</p> <ul style="list-style-type: none"> • ack : acknowledgment (ACK; 確認応答) ビットセット • established : 確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin : 終了ビットセット。送信元からのデータはそれ以上ありません。 • neq {port protocol} : 所定のポート番号上にないパケットだけを照合します。 • psh : プッシュ機能ビットセット • range {port protocol} : ポート番号の範囲内のパケットだけを照合します。 • rst : リセットビットセット • syn : 同期ビットセット • urg : 緊急ポインタ ビットセット
ステップ 3c	<pre>deny permit udp {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-le ngth any host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port protocol}] [range {port protocol}] [sequence value] [time-range name]</pre>	<p>(任意) UDP アクセス リストおよびアクセス条件を定義します。</p> <p>ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前であればなりません。UDP の場合、established パラメータは無効です。</p>
ステップ 3d	<pre>deny permit icmp {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-le ngth any host destination-ipv6-address} [operator [port-number]] [icmp-type [icmp-code] icmp-message] [dscp value] [log] [log-input] [sequence value] [time-range name]</pre>	<p>(任意) ICMP アクセス リストおよびアクセス条件を定義します。</p> <p>インターネット制御メッセージ プロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • icmp-type : ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 • icmp-code : ICMP パケットを ICMP メッセージ コードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 • icmp-message : ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定のアクセス リストから拒否または許可条件を削除するには、キーワードを指定して **no deny** | **permit IPv6** アクセス リスト コンフィギュレーション コマンドを使用します。

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番目の拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番目の拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番目の許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番目の許可エントリは必要です。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。レイヤ 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	アクセス リストを適用するレイヤ 2 インターフェイス (ポート ACL 用) またはレイヤ 3 インターフェイス (ルータ ACL 用) を特定して、インターフェイス コンフィギュレーション モードを開始します。 (注) IP ベース イメージが稼働しているスイッチは、ポート ACL をサポートしません。
ステップ 3	no switchport	ルータ ACL を適用する場合は、インターフェイスをレイヤ 2 モード (デフォルト) からレイヤ 3 モードに変更します。
ステップ 4	ipv6 address ipv6-address	レイヤ 3 インターフェイス (ルータ ACL 用) で IPv6 アドレスを設定します。 このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。
ステップ 5	ipv6 traffic-filter access-list-name {in out}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 out キーワードはレイヤ 2 インターフェイス (ポート ACL) ではサポートされません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	アクセス リストの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスからアクセス リストを削除するには、**no ipv6 traffic-filter access-list-name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト *Cisco* を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

表 45-1 に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

表 45-1 IPv6 アクセス リスト情報を表示するコマンド

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [<i>access-list-name</i>]	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチに設定済みのすべてのアクセス リストが表示されます。

```
Switch# show access-lists
Extended IP access list hello
  10 permit ip any any
IPv6 access list ipv6
  permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30

IPv6 access list outbound
  deny udp any any sequence 10
  deny tcp any any eq telnet sequence 20
```



CHAPTER 46

HSRP および VRRP の設定

この章では、IE 3000 スイッチでホットスタンバイ ルータ プロトコル (HSRP) を使用方法について説明します。HSRP は、IP トラフィック ルーティングに冗長性を提供し、特定のルータの可用性に依存しないルーティングを実現します。IPv4 用 HSRP は、IP サービス イメージが稼働しているスイッチでサポートされます。IPv6 HSRP を使用するには、第 42 章「IPv6 ユニキャストルーティングの設定」を参照してください。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンドスイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンドスイッチを設定することもできます。クラスタリングの詳細については、第 6 章「スイッチのクラスタ化」、および Cisco.com で利用できる『*Getting Started with Cisco Network Assistant*』を参照してください。

この章で使用するコマンドの構文および使用方法の詳細については、次のマニュアルを参照してください。

- このリリースのスイッチ コマンドリファレンス
- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』 (次の URL から入手可能)
http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
- 『*Hot Standby Router Protocol Version 2*』 フィーチャ モジュール (次の URL から入手可能)
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthsrpv2.html

この章で説明する内容は、次のとおりです。

- 「HSRP の概要」 (P.46-1)
- 「HSRP の設定」 (P.46-4)
- 「HSRP 設定の表示」 (P.46-13)
- 「VRRP の設定」 (P.46-13)

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークの可用性を高めるシスコの標準方式です。HSRP を使用すると、特定のルータの可用性に依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC (メディア アクセス コントロール) アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになり HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。相互にバックアップ機能を提供するように設定され

ている複数のルータに、共通のターゲットを表すルータです。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイルータとして選択されます。スタンバイルータは、指定されたアクティブルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。



(注)

HSRP グループのルータには、IE 3000 のルーテッドポートやスイッチ仮想インターフェイス (SVI) など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークの可用性を高めます。アクティブルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイルータは、アクティブルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

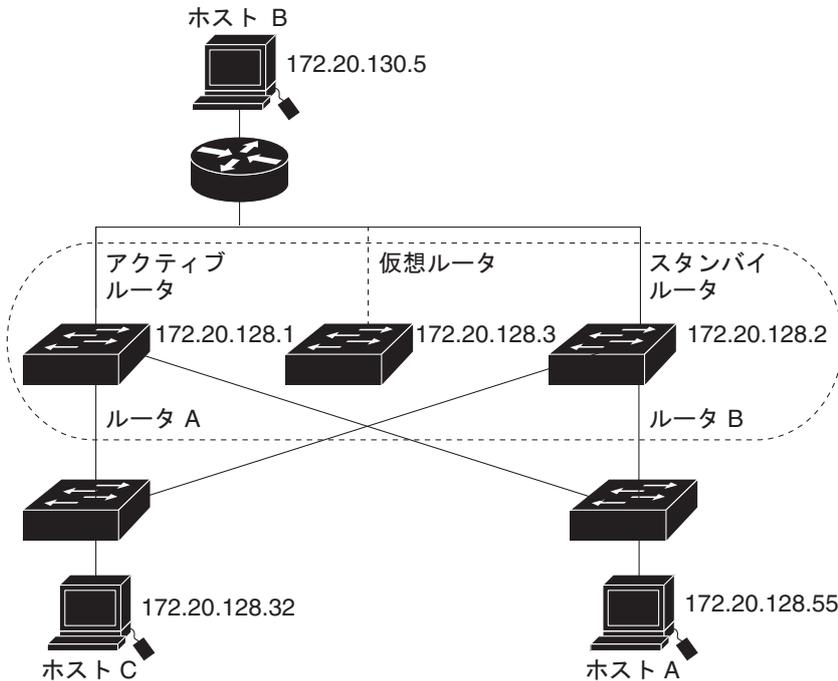
HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。 n 台のルータで HSRP が稼働している場合、 $n + 1$ 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブルータの故障を HSRP が検出すると、選択されているスタンバイルータがホットスタンバイグループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイルータも選択されます。HSRP が稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブルータおよびスタンバイルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル (ICMP) のリダイレクトメッセージがデフォルトでディセーブルとなっています。

レイヤ 3 で動作する IE 3000 スイッチ間で複数のホットスタンバイグループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンドグループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブルータ、スイッチ 2 のインターフェイスをスタンバイルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブルータ、スイッチ 1 の別のインターフェイスをスタンバイルータとして設定することもできます。

図 46-1 に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルトルータとして仮想ルータの IP アドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの転送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブルータとなり、アクティブルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 46-1 HSRP の一般的な構成



204345

HSRP のバージョン

スイッチは、次の Hot Standby Redundancy Protocol (HSRP; ホットスタンバイ ルータ プロトコル) をサポートします。

- HSRPv1 : HSRP のバージョン 1 で、デフォルトのバージョンです。次の機能があります。
 - HSRP グループ番号は 0 ~ 255 まで使用できます。
 - HSRPv1 は 224.0.0.2 のマルチキャストアドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol (CGMP) の脱退処理と競合します。HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。
- HSRPv2 : HSRP のバージョン 2 です。このバージョンには次のような特長があります。
 - HSRP グループ番号とサブインターフェイスの VLAN ID を照合させるために、HSRPv2 では 0 ~ 4095 のグループ番号と 0000.0C9F.F000 ~ 0000.0C9F.FFFF の MAC アドレスを使用できます。
 - HSRPv2 は 224.0.0.102 のマルチキャストアドレスを使用して hello パケットを送信します。HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
 - HSRPv2 のパケット形式は、HSRPv1 とは異なります。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value (TLV) 形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプフィールドは無視されます。

MHSRP

スイッチは、Multiple HSRP (MHSRP) をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロードシェアリングが可能です。ホストネットワークからサーバネットワークまで、ロードバランシングを実現して複数のスタンバイグループ（およびパス）を使用するために、MHSRP を設定できます。図 46-2 では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立しています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブルータになり、ルータ B がスタンバイルータとなります。グループ 2 では、ルータ B に最高のプライオリティが割り当てられているので、ルータ B がデフォルトのアクティブルータになり、ルータ A がスタンバイルータとなります。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータの packets 転送機能を引き継ぎます。

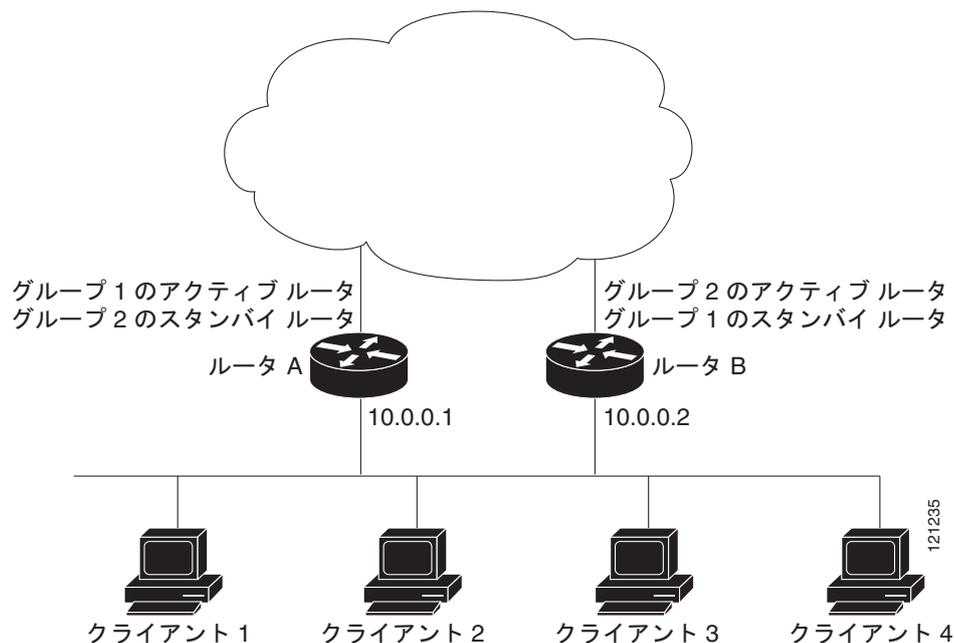
設定手順の例については、「MHSRP の設定」(P.46-10) を参照してください。



(注)

MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプトによりロードシェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 46-2 MHSRP ロードシェアリング



HSRP の設定

ここでは、次の設定について説明します。

- 「HSRP のデフォルト設定」(P.46-5)
- 「HSRP HSRP 設定時の注意事項」(P.46-6)
- 「HSRP のイネーブル化」(P.46-6)

- 「HSRP のプライオリティの設定」 (P.46-8)
- 「MHSRP の設定」 (P.46-10)
- 「HSRP 認証およびタイマーの設定」 (P.46-11)
- 「ICMP リダイレクト メッセージの HSRP サポートのイネーブル化」 (P.46-12)
- 「HSRP グループおよびクラスタリングの設定」 (P.46-12)
- 「HSRP のトラブルシューティング」 (P.46-12)

HSRP のデフォルト設定

表 46-1 に、HSRP のデフォルト設定を示します。

表 46-1 HSRP のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイ プライオリティ	100
スタンバイ遅延	0 (遅延なし)
スタンバイでのインターフェイス プライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP HSRP 設定時の注意事項

HSRP を設定する場合は、次の注意事項に従ってください。

- IPv4 の HSRP および IPv6 の HSRP は相互に排他的です。両方を同時にイネーブルにはできません。
- HSRPv2 および HSRPv1 は相互に排他的です。HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒に動作しません（その逆も同様）。
- HSRP グループ インスタンスは 32 まで設定できます。
複数のインターフェイス上に同じ HSRP グループ番号を設定した場合、スイッチはそれぞれのインターフェイスを 1 つのインスタンスとして数えます。
たとえば、VLAN 1 とポート 1 上に HSRP グループ 0 を設定すると、スイッチはこれを 2 つのインスタンスとして数えます。
- 次の設定手順では、次に示すレイヤ 3 インターフェイスを指定する必要があります。
 - ルーテッド ポート : **no switchport** インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
 - SVI : **interface vlan vlan_id** グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
 - レイヤ 3 モードの EtherChannel ポート チャンネル : **interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャンネル グループにバインドして作成されたポートチャンネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」の項を参照してください。
- すべてのレイヤ 3 インターフェイスには IP アドレスが割り当てられている必要があります。「レイヤ 3 インターフェイスの設定」(P.14-22) を参照してください。
- 1 つの HSRP インスタンスだけ設定してください。スイッチは HSRPv1、HSRPv2、HSRP の IPv6 をサポートします。
- HSRP グループのバージョンは、グループ番号が 256 より少ない場合にだけ HSRPv2 から HSRPv1 へ変更できます。
- IPv6 で HSRPv2 および HSRP のグループ番号を設定する場合、256 の倍数の範囲のグループ番号を使用する必要があります。有効な範囲は 0 ~ 255、256 ~ 511、512 ~ 767、3840 ~ 4095 などです。
有効なグループ番号、無効なグループ番号の例 :
 - 2、150、225 の番号でグループを設定する場合、3850 の番号を持つ他のグループは設定できません。これは、0 ~ 255 の範囲内ではありません。
 - 520、600、700 の番号でグループを設定する場合、900 の番号を持つ他のグループは設定できません。これは、512 ~ 767 の範囲内ではありません。
- インターフェイスの HSRP バージョンを変更する場合、HSRP グループは新しい MAC アドレスを持つことになるため、リセットされます。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドを実行すると、設定されたインターフェイスで HSRP がアクティブになります。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバ

イ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ ARP がイネーブルの場合、インターフェイスのホットスタンバイステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイグループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

レイヤ 3 インターフェイス上で HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	standby version {1 2}	(任意) インターフェイスに HSRP バージョンを設定します。 <ul style="list-style-type: none"> 1 : HSRPv1 を選択します。 2 : HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	standby [group-number] ip [ip-address [secondary]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成 (またはイネーブルに) します。 <ul style="list-style-type: none"> (任意) group-number : HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 (1 つのインターフェイスで必須、それ以外は任意) ip-address : ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 (任意) secondary : IP アドレスはセカンダリ ホットスタンバイ ルータ インターフェイスです。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show standby [interface-id [group]]	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

HSRP をディセーブルにするには、**no standby [group-number] ip [ip-address]** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイグループで使用される IP アドレスは、HSRP を使用して学習されます。



(注) これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

HSRP のプライオリティの設定

standby priority、**standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプトがイネーブルの場合は、プライオリティが最高のルータがアクティブ ルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。
- 最大の値 (1 ~ 255) が、最高のプライオリティ (アクティブ ルータになる確率が最も高い) を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード (**priority**、**preempt**、または両方) を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが 10 減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track interface-priority** インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- **interface-priority** 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	standby [group-number] priority priority [preempt [delay delay]]	<p>アクティブ ルータを選択するときに使用される priority 値を設定します。指定できる範囲は 1 ~ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。</p> <ul style="list-style-type: none"> （任意） group-number : コマンドが適用されるグループ番号です。 （任意） preempt : ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、アクティブ ルータとして制御を行います。 （任意） delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 (1 時間) で、デフォルトは 0 です (引き継ぐ前の遅延はありません)。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 4	standby [group-number] [priority priority] preempt [delay delay]	<p>ルータを preempt に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。</p> <ul style="list-style-type: none"> （任意） group-number : コマンドが適用されるグループ番号です。 （任意） priority : グループ プライオリティを設定または変更します。指定できる範囲は 1 ~ 255 で、デフォルトは 100 です。 （任意） delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 (1 時間) で、デフォルトは 0 です (引き継ぐ前の遅延はありません)。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 5	standby [group-number] track type number [interface-priority]	<p>他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。</p> <ul style="list-style-type: none"> （任意） group-number : コマンドが適用されるグループ番号です。 type : 追跡対象のインターフェイス タイプを (インターフェイス番号とともに) 入力します。 number : 追跡対象のインターフェイス番号を (インターフェイス タイプとともに) 入力します。 （任意） interface-priority : インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	スタンバイ グループの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのプライオリティ、プリエンプト、遅延値に戻すには、**no standby [group-number] priority priority [preempt [delay delay]]** および **no standby [group-number] [priority priority] preempt [delay delay]** インターフェイス コンフィギュレーション コマンドを使用します。

追跡を解除するには、**no standby [group-number] track type number [interface-priority]** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、グループのアクティブ ルータとして 2 つのルータを設定し、仮想ルータをスタンバイ ルータとして設定します。次に、[図 46-2](#) に示した MHSRP 設定をイネーブルにする例を示します。故障したルータが回復した場合にプリエンプションが発生してロード バランシングが復元されるように、各 HSRP インターフェイスで **standby preempt** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイプライオリティは 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイプライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定

HSRP 認証ストリングを設定したり、hello タイム インターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常の場合、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、認証を設定する HSRP インターフェイスを入力します。
ステップ 3	standby [group-number] authentication string	(任意) authentication string : すべての HSRP メッセージで伝達されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトのストリングは cisco です。 (任意) group-number : コマンドが適用されるグループ番号です。
ステップ 4	standby [group-number] timers hellotime holdtime	(任意) hello パケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 <ul style="list-style-type: none"> • group-number : コマンドが適用されるグループ番号です。 • hellotime : hello インターバル (秒) です。指定できる範囲は 1 ~ 255 秒で、デフォルトは 3 秒です。 • holdtime : アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間 (秒) です。指定できる範囲は 1 ~ 255 秒で、デフォルトは 10 秒です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	スタンバイ グループの設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

認証ストリングを削除するには、**no standby [group-number] authentication string** インターフェイス コンフィギュレーション コマンドを使用します。タイマーをデフォルト値に戻すには、**no standby [group-number] timers hellotime holdtime** インターフェイス コンフィギュレーション コマンドを使用します。

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、*word* を設定する例を示します。

```
Switch# configure terminal
```

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP には、ホストへのエラー パケットの方向付けや送信などの診断機能があります。

スイッチで HSRP が動作している場合、ホストが HSRP グループ内のルータのインターフェイス（または実際の）MAC アドレスを検出できないことに注意してください。ICMP によってホストがルータの実際の MAC アドレスへリダイレクトされて、そのルータに障害が発生した場合、ホストからのパケットは消失します。

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクスト ホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『Cisco IOS IP Configuration Guide, Release 12.2』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンドスイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンドスイッチおよびルーティングの冗長性を確保するには、**cluster standby-group HSRP-group-name [routing-redundancy]** グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

次に、スタンバイ グループ `my_hsrp` をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンドスイッチおよびルータの冗長性に使用する例を示します。このコマンドを実行できるのは、コマンドスイッチに対してだけです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch# configure terminal
Switch(config)# cluster standby-group my_hsrp routing-redundancy
Switch(config)# end
```

HSRP のトラブルシューティング

表 46-2 で説明されている状況のいずれかが発生した場合、以下のメッセージが表示されます。

```
%FHRP group not consistent with already configured groups on the switch stack -
virtual MAC reservation failed
```

表 46-2 HSRP のトラブルシューティング

状況	アクション
32 個を超える HSRP グループ インスタンスを設定する。	最大 32 個のグループ インスタンスに設定されるように HSRP グループを削除します。
IPv4 の HSRP および IPv6 の HSRP を同時に設定する。	スイッチ上に IPv4 の HSRP または IPv6 の HSRP のいずれかを設定します。
256 までの有効な範囲にないグループ番号を設定する。	有効な範囲にあるグループ番号を設定します。

HSRP 設定の表示

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

```
show standby [interface-id [group]] [brief] [detail]
```

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルト表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

次に、**show standby** 特権 EXEC コマンドを実行し、2 つのスタンバイ グループ（グループ 1 およびグループ 100）の HSRP 情報を表示する例を示します。

```
Switch# show standby
VLAN1 - Group 1
  Local state is Standby, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.182
  Hot standby IP address is 172.20.128.3 configured
  Active router is 172.20.128.1 expires in 00:00:09
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac01
  Name is bbb
VLAN1 - Group 100
  Local state is Active, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.262
  Hot standby IP address is 172.20.138.51 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac64
  Name is test
```

VRRP の設定

Cisco IOS Release 12.2(58)SE 以降では、スイッチは仮想ルータ冗長プロトコル（VRRP）をサポートします。

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当てる選択プロトコルです。この場合、マルチアクセス リンク上にある何台かのルータが同じ仮想 IP アドレスを使用できるようにし

ます。VRRP ルータは、LAN に接続された 1 つ以上の他のルータと関係して VRRP プロトコルを実行するように設定されます。VRRP 設定では、1 台のルータが仮想ルータ マスターとして選定され、他のルータは仮想ルータ マスターが機能を停止した場合のバックアップとして動作します。

VRRP の制限事項

- スイッチは HSRP または VRRP のいずれかをサポートしますが、両方をサポートしません。スイッチは HSRP と VRRP の両方が設定されたスタックを参加できません。
- スイッチの VRRP 実装は、RFC 2787 で指定された MIB をサポートしません。
- スイッチの VRRP 実装は、テキストベースの認証 だけをサポートします。
- IPv4 および IPv6 グループの VRRP を同時にイネーブルにはできません。

VRRP の詳細と設定手順については、『[Configuring VRRP](#)』のフィーチャ モジュールを参照してください。



CHAPTER 47

Cisco IOS IP SLA 動作の設定

この章では、IE 3000 スイッチで Cisco IOS IP サービス レベル契約 (SLA) を使用方法について説明します。Cisco IP SLA は Cisco IOS ソフトウェアの一部であり、シスコのお客様は連続的で信頼性の高い確実な方法でトラフィックを生成するアクティブトラフィックモニタリングを行って IP アプリケーションとサービスの IP サービス レベルを分析し、ネットワークパフォーマンスを測定することができます。Cisco IOS SLA を使用すると、サービスプロバイダーのお客様はサービスレベル契約の検討と提供、企業のお客様はサービスレベルの検証、外部委託しているサービスレベル契約の検証、およびネットワークパフォーマンスを把握することができます。Cisco IOS IP SLA は、ネットワークアセスメントを実行することで Quality of Service (QoS) の検証、新しいサービス導入の簡易化、ネットワークトラブルシューティングの補助を可能にします。



(注)

LAN ベースイメージを実行するスイッチは、IP SLA 応答側の機能だけをサポートしており、IP SLA のすべての機能をサポートする他の装置 (IP サービスイメージを実行する IE 3000 スイッチなど) とともに構成する必要があります。

IP SLA の詳細については、次の URL の『Cisco IOS IP SLAs Configuration Guide, Release 12.4T』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

このコマンド構文の詳細については、次の URL のコマンドリファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

この章の内容は、次のとおりです。

- 「Cisco IOS IP SLA の概要」 (P.47-1)
- 「IP SLA 動作の設定」 (P.47-6)
- 「IP SLA 動作のモニタリング」 (P.47-13)

Cisco IOS IP SLA の概要

CiscoIOS IP SLA はネットワークにデータを送信し、複数のネットワーク間あるいは複数のネットワークパス内のパフォーマンスを測定します。ネットワークデータおよび IP サービスをシミュレーションし、ネットワークパフォーマンス情報をリアルタイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワークアプリケーションサーバのようリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワークトポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドライン インターフェイス (CLI) MIB および Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) MIB に格納されます。IP SLA パケットには設定可能な IP レイヤおよびアプリケーション層のオプションがあります。たとえば、発信元および宛先 IP アドレス、ユーザ データグラム プロトコル (UDP) /TCP ポート番号、タイプ オブ サービス (ToS) バイト (Differentiated Services Code Point (DSCP; DiffServ コード ポイント) および IP プレフィックス ビットを含む)、VPN Routing/Forwarding Instance (VRF; VPN ルーティング/転送インスタンス)、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンド ユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のような一意のパフォーマンス メトリックのサブセットを収集します。

- 遅延 (往復および一方向)
- ジッタ (方向性あり)
- パケット損失 (方向性あり)
- パケット シーケンス (パケット順序)
- パス (ホップ単位)
- 接続 (方向性あり)
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Works Internetwork Performance Monitor (IPM) やサードパーティ製パフォーマンス管理製品などの Performance Monitoring (PM; パフォーマンス モニタリング) アプリケーションでも使用できます。Cisco IOS IP SLA を使用するネットワーク管理製品については、次の URL を参照してください。

<http://www.cisco.com/go/ipsla>

IP SLA を使用すると次のような利点があります。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
 - ネットワーク内のジッタ、遅延、パケット損失が測定できる。
 - 連続的で信頼性のある確実な評価ができる。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる (たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる)。
- 信頼性の高い評価を連続的に行ってネットワーク動作のトラブルシューティングを行うので、問題をすぐに特定しトラブルシューティングにかかる時間を短縮できる。
- マルチプロトコル ラベル スイッチング (MPLS) パフォーマンス モニタリングとネットワークの検証を行う (MPLS をサポートするスイッチの場合)。

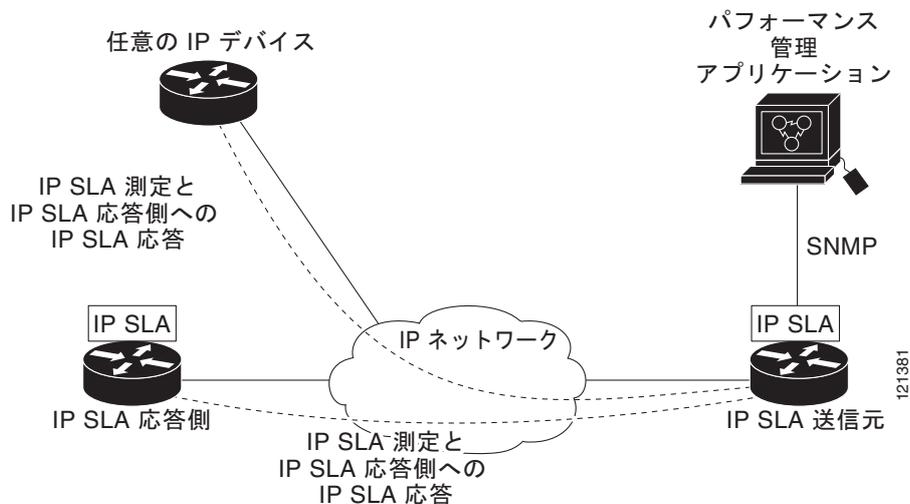
ここでは、次の IP SLA 機能について説明します。

- 「Cisco IOS IP SLA によるネットワーク パフォーマンスの測定」(P.47-3)
- 「IP SLA Responder と IP SLA コントロール プロトコル」(P.47-4)
- 「IP SLA の応答時間の計算」(P.47-4)
- 「IP SLA 動作のスケジューリング」(P.47-5)
- 「IP SLA 動作のしきい値のモニタリング」(P.47-5)

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。図 47-1 に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。IP SLA 動作は、特定のプロトコル (UDP など) を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 47-1 Cisco IOS IP SLA 動作



IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

1. 必要であれば、IP SLA Responder をイネーブルにします。
2. 必要な IP SLA 動作タイプを設定します。
3. 指定された動作タイプのオプションを設定します。
4. 必要であれば、しきい値条件を設定します。
5. 動作の実行スケジュールを指定し、しばらく動作を実行して統計情報を収集します。
6. Cisco IOS CLI を使用するか Network Management System (NMS; ネットワーク管理システム) と SNMP を併用して、動作の結果を表示し確認します。

IP SLA の動作の詳細については、次の URL の『Cisco IOS IP SLAs Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html



(注)

スイッチでは、ゲートキーパー登録遅延動作測定を使用する Voice over IP (VoIP) サービス レベルをサポートしません。IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。

IP SLA Responder と IP SLA コントロール プロトコル

IP SLA Responder は宛先シスコ デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求 パケットを予想して応答します。Responder は専用プローブなしで正確な測定を行います。Responder は、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。



(注)

IP SLA 応答側には、LAN Base イメージを実行する Catalyst 2960 または IE 3000 スイッチ、あるいは IP Base イメージを実行する Catalyst 3560 スイッチまたは 3750 スイッチのような Cisco IOS レイヤ 2 の応答側に設定可能なスイッチを使用できます。Responder は、IP SLA 機能を全面的にサポートする必要はありません。

図 47-1 に、IP ネットワーク内での Cisco IOS IP SLA Responder の配置場所を示します。Responder は、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。この間に、Responder は要求を受け付け、応答します。Responder は、IP SLA パケットに回答した後または指定の時間が経過したらポートをディセーブルにします。セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

すべての IP SLA 動作に対して宛先デバイスの Responder をイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス (Telnet や HTTP など) は Responder では必要ありません。他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

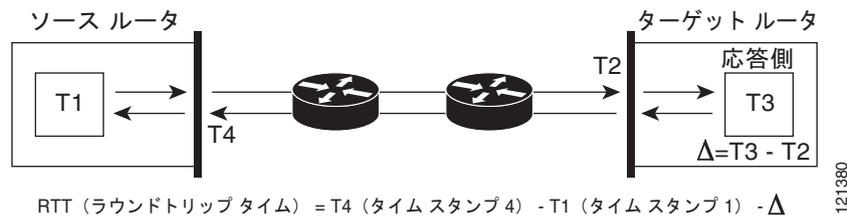
IP SLA の応答時間の計算

スイッチとルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA はソース デバイスとターゲット デバイス (Responder が使用されている場合) の処理遅延を最小化し、正しい Round-Trip Time (RTT; ラウンドトリップ時間) を識別します。IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA Responder がイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

図 47-2 に、Responder の動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲット ルータで Responder 機能がイネーブルの場合、タイム スタンプ 3 (TS3) からタイム スタンプ 2 (TS2) を引いてテストパケットの処理にかかった時間を求め、デルタ (Δ) で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース ルータにも適用されます。その場合、着信タイム スタンプ 4 (TS4) が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 47-2 Cisco IOS IP SLA Responder タイムスタンプ



この他にも、ターゲットデバイスに2つのタイムスタンプがあれば一方方向遅延、ジッタ、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし一方方向遅延測定を取り込むには、ソースルータとターゲットルータの両方に Network Time Protocol (NTP; ネットワークタイムプロトコル) を設定し、両方のルータを同じロックソースに同期させる必要があります。一方方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作のスケジューリングをします。スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。また、pending オプションを使用して、あとで動作を開始するように設定することもできます。pending オプションは動作の内部状態に関するもので、SNMP で表示できます。トリガーを待機する反応 (しきい値) 動作の場合も pending オプションを使用します。スケジューリングでは、1度に1つのIP SLA 動作をさせることも、グループの動作をさせることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で1つのコマンドを使用して、IP サービスイメージを稼働する複数のIP SLA 動作をスケジューリングできます。等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリングトラフィックの数を制御できます。IP SLA 動作をこのように分散させるとCPU利用率を最小限に抑え、ネットワークスケーラビリティを向上させることができます。

IP SLA の複数動作のスケジューリング機能に関する詳細については、次のURLにある『Cisco IOS IP SLAs Configuration Guide』の「IP SLAs - Multiple Operation Scheduling」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作のしきい値のモニタリング

SLA モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。IP SLA は SNMP トラップを送信して、次のような場合にイベントをトリガーします。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッタしきい値
- 一方方向パケット損失
- 一方方向ジッタ

- 一方向 Mean Opinion Score (MOS; 平均オピニオン評点)
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。たとえば、回数を増やしたり、ICMP パス エコーや ICMP パス ジッタ動作を開始してトラブルシューティングを行うことができます。

しきい値タイプとレベル設定の決定は複雑で、ネットワークで使用する IP サービス タイプによって異なります。Cisco IOS IP SLA 動作でしきい値を使用する詳細については、次の URL で『Cisco IOS IP SLAs Configuration Guide』の「IP SLAs—Proactive Threshold Monitoring」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作の設定

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『Cisco IOS IP SLAs Configuration Guide』を参照してください。ここでは、応答側の設定、UDP ジッタ動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。



(注)

LAN ベース イメージを実行するスイッチは、IP SLA 応答側の機能だけをサポートします。完全な IP SLA 機能を使用するには、スイッチで IP サービス イメージが稼働している必要があります。

他の動作の設定に関する詳細については、次の URL にアクセスして『Cisco IOS IP SLAs Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

ここでは、次の情報について説明します。

- 「デフォルト設定」(P.47-6)
- 「設定時の注意事項」(P.47-6)
- 「IP SLA Responder の設定」(P.47-8)
- 「UDP ジッタ動作を使用した IP サービス レベルの分析」(P.47-8)
- 「ICMP エコー動作を使用した IP サービス レベルの分析」(P.47-11)

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA コマンドについては、次の URL で『Cisco IOS IP SLAs Command Reference, Release 12.4T』のコマンドリファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

詳しい説明と設定手順については、次の URL の『Cisco IOS IP SLAs Configuration Guide, Release 12.4T』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

スイッチでは、このガイドで説明する IP SLA コマンドや動作がすべてサポートされているわけではありません。スイッチでは、UDP ジッタ、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッタ、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。ゲートキーパー登録遅延動作測定を使用した Voice over IP (VoIP) サービス レベルはサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。コマンド出力例は次のとおりです。

```
Switch# show ip sla application

      IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured      : 0
Number of active Entries         : 0
Number of pending Entries        : 0
Number of inactive Entries       : 0

      Supported Operation Types
Type of Operation to Perform: 802.lagEcho
Type of Operation to Perform: 802.lagJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

IP SLA Responder の設定

IP SLA 応答側は、完全な IP SLA 機能をサポートしていないレイヤ 2 スイッチ（例：LAN ベース イメージを実行する IE 3000）などの Cisco IOS ソフトウェアベース デバイスでだけ利用可能です。特権 EXEC モードで、ターゲット デバイス（動作ターゲット）に IP SLA Responder を設定する手順は次のとおりです。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip sla responder {tcp-connect udp-echo} ipaddress ip-address port port-number</code>	<p>スイッチを IP SLA Responder に設定します。</p> <p>オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • tcp-connect : Responder の TCP 接続動作をイネーブルにします。 • udp-echo : Responder のユーザ データグラム プロトコル (UDP) エコー動作またはジッタ動作をイネーブルにします。 • ipaddress ip-address : 宛先 IP アドレスを入力します。 • port port-number : 宛先ポート番号を入力します。 <p>(注) IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip sla responder</code>	デバイスの IP SLA Responder 設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA Responder をディセーブルにするには、**no ip sla responder** グローバル コンフィギュレーション コマンドを入力します。次に、デバイスを UDP ジッタ IP SLA 動作の Responder に設定する例を示します。UDP ジッタ IP SLA 動作については次の項で説明します。

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```



(注) IP SLA Responder が機能するためには、Catalyst 3750 スイッチまたは Catalyst 3560 スイッチのような、IP サービス イメージを実行して IP SLA をすべてサポートしている送信元デバイスを設定する必要があります。送信元デバイスの設定情報については、マニュアルを参照してください。

UDP ジッタ動作を使用した IP サービス レベルの分析

ジッタはパケット間の遅延がばらつくことを指します。発信元から宛先に向かって複数のパケットを 10 ミリ秒遅れで送信した場合、ネットワークが正常に動作していれば宛先でも 10 ミリ秒遅れで受信します。しかし、ネットワーク内に遅延がある場合（キューの発生や別のルータ経由で到着するなど）、パケットの到着遅延が 10 ミリ秒を上回ったり、下回ったりします。正のジッタ値は、パケットの到着が 10 ミリ秒を超えていることを意味します。パケットの到着が 12 ミリ秒の場合のジッタ値は +2 ミリ秒（正の値）です。8 ミリ秒で到着する場合は、2 ミリ秒（負の値）です。遅延による影響を受けやすいネットワークの場合、正のジッタ値は望ましくありません。ジッタ値 0 が理想的です。

ジッタのモニタリング以外にも、IP SLA UDP ジッタ動作を多目的データ収集動作に使用できます。パケット IP SLA は搬送パケットを生成し、送信元ターゲットと動作ターゲット間でシーケンス情報の送受信とタイムスタンプの送受信を行います。以上の点に基づき、UDP ジッタ動作は次のデータを測定します。

- 方向別ジッタ（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッタ動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲットルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。デフォルトでは、10 バイトのペイロードサイズのパケットフレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、NTP などによる送信元デバイスとターゲットデバイス間のクロック同期が必要です。一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。送信元デバイスとターゲットデバイスのクロックが同期されていない場合、一方向ジッタおよびパケット損失データは戻されますが、UDP ジッタ動作による一方向遅延測定値は 0 で戻ります。



(注) 送信元デバイスに UDP ジッタ動作を設定する前に、ターゲットデバイス（動作ターゲット）の IP SLA 応答側を有効にしておく必要があります。

送信元デバイス上で UDP ジッタ動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip sla operation-number</code>	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	udp-jitter { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> }] [source-port <i>port-number</i>] [control { enable disable }] [num-packets <i>number-of-packets</i>] [interval <i>interpacket-interval</i>]	IP SLA 動作に UDP ジッタ動作を設定し、UDP ジッタ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • <i>destination-ip-address</i> <i>destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • <i>destination-port</i> : 宛先ポート番号を 1 ~ 65535 の範囲で指定します。 • (任意) source-ip {<i>ip-address</i> <i>hostname</i>} : 送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • (任意) source-port <i>port-number</i> : 送信元ポート番号を 1 ~ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • (任意) control : IP SLA コントロール メッセージの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA コントロール メッセージが宛先デバイスに送信されて、IP SLA 応答側との接続が確立します。 • (任意) num-packets <i>number-of-packets</i> : 生成するパケット数を入力します。指定できる範囲は 1 ~ 6000 です。デフォルトは 10 です。 • (任意) interval <i>inter-packet-interval</i> : パケットの送信間隔をミリ秒で指定します。指定できる範囲は 1 ~ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 4	frequency <i>seconds</i>	(任意) 指定した IP SLA 動作の反復間隔を設定します。指定できる範囲は 1 ~ 604800 秒で、デフォルトは 60 秒です。
ステップ 5	exit	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm</i> [<i>:ss</i>] [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 <ul style="list-style-type: none"> • <i>operation-number</i> : RTR エントリ番号を入力します。 • (任意) life : 動作の実行を無制限 (forever) に指定するか、<i>秒数</i>を指定します。有効な範囲は 0 ~ 2147483647 です。デフォルトは 3600 秒 (1 時間) です。 • (任意) start-time : 情報の収集を開始する時刻を入力します。 <ul style="list-style-type: none"> – 特定の時刻に開始する場合は、時、分、秒 (24 時間表記)、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 – pending と入力すれば、開始時刻を指定するまでは情報を収集しません。 – now と入力すれば、ただちに動作を開始します。 – after <i>hh:mm:ss</i> と入力すれば、指定した時刻の経過後に動作を開始します。 • (任意) ageout <i>seconds</i> : 情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ~ 2073600 秒です。デフォルトは 0 秒 (いつまでも保存する) です。 • (任意) recurring : 毎日、動作を自動的に実行します。
ステップ 7	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ8	show ip sla configuration [operation-number]	(任意) 設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する方法と、指定した動作だけを表示する方法があります。
ステップ9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作を無効にするには、**no ip sla operation-number** グローバル コンフィギュレーション コマンドを入力します。次に、UDP ジッタ IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.
```

```
Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 30
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
```

ICMP エコー動作を使用した IP サービス レベルの分析

ICMP エコー動作は、シスコ デバイスと IP を使用する任意のデバイスとの間でエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信して ICMP エコー応答を受信するまでの時間を測定して算出します。大多数のカスタマーが IP SLA ICMP ベース動作、社内 ping テスト、ping ベース専用プローブを使用して、送信元 IP SLA デバイスと宛先 IP デバイス間の応答時間を測定しています。IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答時間が得られます。



(注) この動作では、IP SLA 応答側を有効にしておく必要はありません。

ソース デバイス上で ICMP エコー動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip sla operation-number	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-id</i>]	IP SLA 動作に ICMP エコー動作を設定し、ICMP エコー コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • <i>destination-ip-address</i> <i>destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • (任意) source-ip {<i>ip-address</i> <i>hostname</i>} : 送信元 IP アドレスまたはホスト名を指定します。送信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • (任意) source-interface <i>interface-id</i> : 動作に対する送信元インターフェイスを指定します。
ステップ 4	frequency <i>seconds</i>	(任意) 指定した IP SLA 動作の反復間隔を設定します。指定できる範囲は 1 ~ 604800 秒で、デフォルトは 60 秒です。
ステップ 5	exit	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm</i> [: <i>ss</i>] [<i>month</i> <i>day</i> <i>day</i> <i>month</i>] pending now after <i>hh:mm:ss</i> }] [ageout <i>seconds</i>] [recurring]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 <ul style="list-style-type: none"> • <i>operation-number</i> : RTR エントリ番号を入力します。 • (任意) life : 動作の実行を無制限 (forever) に指定するか、<i>秒数</i>を指定します。有効な範囲は 0 ~ 2147483647 です。デフォルトは 3600 秒 (1 時間) です。 • (任意) start-time : 情報の収集を開始する時刻を入力します。 <ul style="list-style-type: none"> – 特定の時刻に開始する場合は、時、分、秒 (24 時間表記)、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 – pending と入力すれば、開始時刻を指定するまでは情報を収集しません。 – now と入力すれば、ただちに動作を開始します。 – after <i>hh:mm:ss</i> と入力すれば、指定した時刻の経過後に動作を開始します。 • (任意) ageout <i>seconds</i> : 情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ~ 2073600 秒です。デフォルトは 0 秒 (いつまでも保存する) です。 • (任意) recurring : 毎日、動作を自動的に実行します。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show ip sla configuration [<i>operation-number</i>]	(任意) 設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する方法と、指定した動作だけを表示する方法があります。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作を無効にするには、**no ip sla operation-number** グローバル コンフィギュレーション コマンドを入力します。次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 60
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 15
  History Filter Type: None
Enhanced History:
```

IP SLA 動作のモニタリング

表 47-1 に示すユーザ EXEC コマンドまたは特権 EXEC コマンドを使用して、IP SLA 動作の設定と結果を表示します。

表 47-1 IP SLA 動作のモニタリング

コマンド	目的
show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [<i>entry-number</i>]	設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する方法と、指定した動作だけを表示する方法があります。

表 47-1 IP SLA 動作のモニタリング (続き)

コマンド	目的
<code>show ip sla enhanced-history {collection-statistics distribution statistics} [entry-number]</code>	収集した履歴バケットの拡張履歴統計情報を表示します。あるいは、すべての IP SLA 動作または特定の動作に関する分散統計情報を表示します。
<code>show ip sla ethernet-monitor configuration [entry-number]</code>	IP SLA 自動イーサネット設定を表示します。
<code>show ip sla event-publisher</code>	IP SLA の通知を受信するために登録されているクライアント アプリケーションのリストを表示します。
<code>show ip sla group schedule [schedule-entry-number]</code>	IP SLA グループ スケジューリング設定と詳細情報を表示します。
<code>show ip sla history [entry-number full tabular]</code>	すべての IP SLA 動作に関して収集した履歴を表示します。
<code>show ip sla mpls-lsp-monitor {collection-statistics configuration ldp operational-state scan-queue summary [entry-number] neighbors}</code>	MPLS ラベル スイッチドパス (LSP) ヘルス モニタ動作を表示します。
<code>show ip sla reaction-configuration [entry-number]</code>	すべての IP SLA 動作または特定の動作について、事前に設定したしきい値のモニタリングを表示します。
<code>show ip sla reaction-trigger [entry-number]</code>	すべての IP SLA 動作または特定の動作に関する反応トリガー情報を表示します。
<code>show ip sla responder</code>	IP SLA Responder の情報を表示します。
<code>show ip sla standards</code>	IP SLA 標準に関する情報を表示します。
<code>show ip sla statistics [entry-number aggregated details]</code>	現在のまたは集約した動作ステータスと統計情報を表示します。



CHAPTER 48

拡張オブジェクト トラッキングの設定

この章では、IE 3000 スイッチに拡張オブジェクト追跡を設定する方法について説明します。この機能には、より完成度の高い Hot Standby Routing Protocol (HSRP) トラッキング メカニズムが採用されており、インターフェイスのラインプロトコル ステータスを追跡できます。インターフェイスのラインプロトコル ステータスがダウンすると、インターフェイスの HSRP プライオリティが減少して、よりプライオリティの高い他の HSRP デバイスがアクティブになります。拡張オブジェクト トラッキング機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外のプロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステータスに加えて他のオブジェクトも追跡できます。HSRP などのクライアント プロセスでは、トラッキングするオブジェクトを登録して、オブジェクトがステータスを変更した時に通知を要求することができます。この機能は、ルーティング システムのオペラビリティを高め、復旧のスピードを速めるとともに、停止および停止期間を削減します。



(注)

この機能は、IP サービス イメージが稼働しているスイッチでだけサポートされます。

特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

拡張オブジェクト トラッキングおよびこれを設定するためのコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html

この章で説明する内容は、次のとおりです。

- 「拡張オブジェクト トラッキングの概要」 (P.48-1)
- 「拡張オブジェクト トラッキング機能の設定」 (P.48-2)
- 「拡張オブジェクト トラッキングのモニタリング」 (P.48-13)

拡張オブジェクト トラッキングの概要

各追跡対象オブジェクトには、トラッキング CLI (コマンドライン インターフェイス) で指定される一意の番号があります。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。トラッキング プロセスは、追跡対象オブジェクトに値の変化がないかどうかを定期的にポーリングし、(アップまたはダウン値など) 変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステータスに変化した場合に、それぞれが異なるアクションを実行できます。

複数のオブジェクトを組み合わせることで 1 つのリストにして追跡することもできます。このリストの状態判定には、重みしきい値またはパーセンテージを使用します。オブジェクトの組み合わせには、ブールロジックを使用できます。「AND」ブール関数を使用する追跡リストの場合、リスト内の各オブジェクトがアップ状態でないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストの場合、リスト内の 1 つのオブジェクトだけがアップ状態であれば追跡対象オブジェクトはアップになります。

拡張オブジェクト トラッキング機能の設定

ここでは、次のような拡張オブジェクト トラッキングの設定について説明します。

- 「デフォルト設定」(P.48-2)
- 「インターフェイス ラインプロトコルまたは IP ルーティング ステートの追跡」(P.48-2)
- 「追跡リストの設定」(P.48-3)
- 「HSRP オブジェクト トラッキングの設定」(P.48-7)
- 「その他の追跡特性の設定」(P.48-8)
- 「IP SLA オブジェクト トラッキングの設定」(P.48-9)
- 「スタティック ルーティング サポートの設定」(P.48-10)

デフォルト設定

オブジェクト トラッキング タイプは設定されていません。

インターフェイス ラインプロトコルまたは IP ルーティング ステートの追跡

インターフェイス ラインプロトコル ステートまたはインターフェイス IP ルーティング ステートのいずれかを追跡できます。IP ルーティング ステートを追跡する場合、オブジェクトをアップするには次の 3 つの条件が必要です。

- インターフェイス上で IP ルーティングがイネーブル、かつアクティブになっている。
- インターフェイス ラインプロトコル ステートが使用可能な状態（アップ）にある。
- 既知のインターフェイス IP アドレスを使用している。

この 3 つの条件がすべて合致しないと、IP ルーティング ステートはダウンになります。

インターフェイスのラインプロトコル ステートまたは IP ルーティング ステートを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 track object-number interface interface-id line-protocol	(任意) インターフェイスのラインプロトコル ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> object-number : 追跡対象オブジェクトの番号です。指定できる範囲は 1 ~ 500 です。 interface interface-id : 追跡されるインターフェイスです。
ステップ3 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ4 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ5 track object-number interface interface-id ip routing	(任意) インターフェイスの IP ルーティング ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。IP ルート追跡では、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 <ul style="list-style-type: none"> object-number : 追跡対象オブジェクトの番号です。指定できる範囲は 1 ~ 500 です。 interface interface-id : 追跡されるインターフェイスです。
ステップ6 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ7 end	特権 EXEC モードに戻ります。
ステップ8 show track object-number	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスのラインプロトコル ステートの追跡を設定し、その設定を確認する例を示します。

```
Switch(config)# track 33 interface gigabitethernet 1/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
Interface GigabitEthernet1/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:18:28
```

追跡リストの設定

オブジェクトの追跡リストは、ブール式、重みしきい値、またはパーセントしきい値を使用して設定できます。トラッキング対象リストには 1 つまたは複数のオブジェクトが含まれます。オブジェクトは存在していないと追跡リストに追加できません。

- 設定にブール式による演算を指定する場合は、「AND」または「OR」演算子を使用します。

- 追跡リストのステートを重みしきい値で判定する場合は、追跡リスト内の各オブジェクトに重み番号を割り当てます。追跡リストのステータスは、このしきい値に合致したかどうかで判定されます。各オブジェクトのステータスは、すべてのオブジェクトの重みの合計と各オブジェクトのしきい値の重みを比較して判定されます。
- 追跡リストをパーセントしきい値で判定する場合は、追跡リスト内のすべてのオブジェクトにパーセントしきい値を割り当てます。各オブジェクトのステータスは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

ブール式による追跡リストの設定

ブール式を使用して追跡リストを設定すると、「AND」または「OR」演算子を使用した演算が可能になります。たとえば、「AND」演算子で 2 つのインターフェイスを追跡すると、*up* は両方のインターフェイスがアップであることを意味し、*down* はどちらかのインターフェイスがダウンであることを意味します。

ブール式を使用してオブジェクトの追跡リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>track track-number list boolean {and or}</code>	追跡リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる <i>track-number</i> の範囲は 1 ~ 500 です。 <ul style="list-style-type: none"> • boolean : 追跡リストのステータスがブール計算に基づくことを指定します。 • and : すべてのオブジェクトがアップの場合にリストはアップであること、また、1 つまたは複数のオブジェクトがダウンの場合にリストはダウンであることを指定します。 • or : 1 つのオブジェクトがアップの場合にリストはアップであること、または、すべてのオブジェクトがダウンの場合にリストはダウンであることを指定します。
ステップ 3	<code>object object-number [not]</code>	追跡対象オブジェクトを指定します。指定できる範囲は 1 ~ 500 です。 not はオブジェクトのステータスを否定します。つまり、オブジェクトがアップの場合に、追跡リストはそのオブジェクトをダウンとして検出することを意味します。 (注) オブジェクトは存在しないと追跡リストに追加できません。
ステップ 4	<code>delay {up seconds [down seconds] [up seconds] down seconds}</code>	(任意) 追跡対象オブジェクトのステータス変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show track object-number</code>	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除するには、`no track track-number` グローバル コンフィギュレーション コマンドを使用します。

次に、AND ブール式を使用して追跡リスト 4 を作成する例を示します。リストには 2 つのオブジェクトが含まれ、そのうち 1 つのオブジェクトが否定されます。このリストがアップの場合は、`object 2` がダウンであることを検出しています。

```
Switch(config)# track 4 list boolean and
```

```
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

重みしきい値による追跡リストの設定

重みしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、重みをしきい値として使用することを指定したあと、各オブジェクトに重み値を設定します。各オブジェクトのステータスは、アップであるすべてのオブジェクトの重み合計と各オブジェクトのしきい値の重みを比較して判定されます。

重みしきい値のリストには、「NOT」ブール演算子を使用できません。

重みしきい値を使用してオブジェクトの追跡リストを作成し、各オブジェクトに重み値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	track track-number list threshold weight	追跡リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる <i>track-number</i> の範囲は 1 ~ 500 です。 <ul style="list-style-type: none"> threshold : 追跡リストのステータスがしきい値に基づくことを指定します。 weight : しきい値が重みに基づくことを指定します。
ステップ3	object object-number [weight weight-number]	追跡対象オブジェクトを指定します。指定できる範囲は 1 ~ 500 です。任意の weight weight-number には、オブジェクトのしきい値の重みを指定します。指定できる範囲は 1 ~ 255 です。 (注) オブジェクトは存在しないと追跡リストに追加できません。
ステップ4	threshold weight {up number [down number]}	しきい値の重みを指定します。 <ul style="list-style-type: none"> up number : 指定できる範囲は 1 ~ 255 です。 down number : (任意) 指定できる範囲は、up number で指定した数により異なります。up number を 25 に設定すると、down number の範囲は 0 ~ 24 です。
ステップ5	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステータス変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show track object-number	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除するには、**no track track-number** グローバル コンフィギュレーション コマンドを使用します。

次に、重みしきい値により追跡する追跡リスト 4 を設定する例を示します。object 1 および object 2 がダウンの場合、object 3 が up 30 というしきい値を満たすので、追跡リスト 4 はアップです。object 3 がダウンの場合、object 1 および object 2 の両方がアップでないと、しきい値の重みを満たしません。

```
Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit
```

この設定は、object 1 および object 2 が 2 つの小さな帯域幅の接続を、object 3 が大きな帯域幅の接続を表す場合に有効です。設定した **down 10** の値は、追跡対象オブジェクトがいったんアップになると、しきい値が 10 以下になるまではダウンにならないことを意味します。この例で 10 以下は、すべての接続がダウンすることを意味します。

パーセントしきい値による追跡リストの設定

パーセントしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、パーセンテージをしきい値として使用することを指定したあと、リスト内のすべてのオブジェクトにパーセンテージを指定します。リストのステータスは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

パーセントしきい値のリストには、「NOT」ブール演算子を使用できません。

パーセントしきい値を使用してオブジェクトの追跡リストを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	track track-number list threshold percentage	追跡リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる <i>track-number</i> の範囲は 1 ~ 500 です。 <ul style="list-style-type: none"> • threshold : 追跡リストのステータスがしきい値に基づくことを指定します。 • percentage : しきい値がパーセンテージに基づくことを指定します。
ステップ 3	object object-number	追跡対象オブジェクトを指定します。指定できる範囲は 1 ~ 500 です。 (注) オブジェクトは存在していないと追跡リストに追加できません。
ステップ 4	threshold percentage {up number [down number]}	しきい値の割合を指定します。 <ul style="list-style-type: none"> • up number : 指定できる範囲は 1 ~ 100 です。 • down number : (任意) 指定できる範囲は、up number で指定した数により異なります。up number を 25 に設定すると、down number の範囲は 0 ~ 24 です。
ステップ 5	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステータス変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show track object-number	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

追跡リストを削除するには、**no track track-number** グローバル コンフィギュレーション コマンドを使用します。

次に、3 つのオブジェクトを持つ追跡リスト 4 を作成し、パーセンテージを指定してリストのステータスを判定する例を示します。

```
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```

HSRP オブジェクト トラッキングの設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいて HSRP プライオリティを変更できるようにスタンバイ HSRP グループを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 track object-number {interface interface-id {line-protocol ip routing} ip route ip-address/prefix-length {metric threshold reachability} list {boolean {and or}} {threshold {weight percentage}}}	<p>(任意) 設定されたステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> 指定できる <i>object-number</i> の範囲は 1 ~ 500 です。 追跡するインターフェイスを指定するには、interface interface-id を入力します。 インターフェイス ライン プロトコル ステートを追跡するには、line-protocol を入力します。また、インターフェイス IP ルーティング ステートを追跡するには、ip routing を入力します。 IP ルートのステートを追跡するには、ip route ip-address/prefix-length を入力します。 しきい値メトリックを追跡する場合は metric threshold、ルートが達成できるかどうかを追跡するには reachability を入力します。 デフォルトの up しきい値は 254、デフォルトの down しきい値は 255 です。 リスト内の一連のオブジェクトを追跡するには、list を入力します。リストはこれまでのページの説明に従って作成してください。 <ul style="list-style-type: none"> Boolean については、「ブール式による追跡リストの設定」(P.48-4) を参照してください。 threshold weight については、「重みしきい値による追跡リストの設定」(P.48-5) を参照してください。 threshold percentage については、「パーセントしきい値による追跡リストの設定」(P.48-6) を参照してください。 <p>(注) 追跡するインターフェイスごとにこの手順を繰り返してください。</p>
ステップ3 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ4 interface interface-id	インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 5	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 <ul style="list-style-type: none"> （任意）group-number : HSRP をイネーブルにするインターフェイスのグループ番号を入力します。指定できる範囲は 0 ~ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 （1 つのインターフェイスで必須、それ以外は任意）ip-address : ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 （任意）secondary : IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 6	standby [<i>group-number</i>] track <i>object-number</i> [decrement [<i>priority-decrement</i>]]	特定のオブジェクトを追跡し、そのオブジェクト ステートに基づいてホットスタンバイ プライオリティを変更できるように HSRP を設定します。 <ul style="list-style-type: none"> （任意）group-number : 追跡が適用されるグループ番号を入力します。 object-number : 追跡対象のオブジェクト番号を入力します。指定できる範囲は 1 ~ 500 で、デフォルトは 1 です。 （任意）decrement priority-decrement : 追跡対象のオブジェクトがダウンになった場合（またはアップに戻った場合）に、ルータのホットスタンバイ プライオリティを減少（または増加）させる幅を指定します。指定できる範囲は 1 ~ 255 で、デフォルトは 10 です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show standby	スタンバイ ルータの IP アドレスおよび追跡ステートを確認します。
ステップ 9	copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

その他の追跡特性の設定

拡張オブジェクト トラッキングを使用して他の特性を追跡することもできます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがしきい値を超えているか下回っているかを確認できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティング プロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer** トラッキング コンフィギュレーション コマンドを使用すると、追跡対象オブジェクトを定期的にポーリングするようにトラッキング プロセスを設定できます。

拡張オブジェクト トラッキング設定を確認する場合は、**show track** 特権 EXEC コマンドを使用してください。

拡張オブジェクト トラッキングおよびこれを設定するためのコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html

IP SLA オブジェクト トラッキングの設定

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) は、ネットワーク パフォーマンスの測定と診断を行うツールです。ネットワーク パフォーマンスを測定するためのトラフィック生成には、アクティブ モニタリングが使用されます。Cisco IP SLA 動作は、ネットワークのトラブルシューティングや設計、分析に使用できるリアルタイム メトリックを収集します。

スイッチの Cisco IP SLA について詳しくは、第 47 章「Cisco IOS IP SLA 動作の設定」を参照してください。IP SLA コマンドについては、次の URL の『Cisco IOS IP SLAs Command Reference, Release 12.4T』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

IP SLA 動作のオブジェクト トラッキングを活用すると、クライアントは IP SLA オブジェクトの出力を追跡して、その情報をアクションのトリガーに使用できます。各 IP SLA 動作は、OK または *OverThreshold* のような Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 動作の戻りコード値を保持しているため、トラッキング プロセス側で解釈できます。IP SLA 動作は、ステートと到達可能性の 2 つの面を追跡できます。ステートの場合、戻りコードが OK のとき、トラック ステートがアップします。リターン コードが OK ではないとき、トラック ステートはダウンします。到達可能性の場合、戻りコードが OK または *OverThreshold* のとき、到達可能性がアップします。リターン コードが OK ではないとき、到達可能性はダウンします。

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 track object-number rtr operation-number state	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 <ul style="list-style-type: none"> 指定できる <i>object-number</i> の範囲は 1 ~ 500 です。 指定できる <i>operation-number</i> の範囲は 1 ~ 2147483647 です。
ステップ3 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ4 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ5 track object-number rtr operation-number reachability	トラッキング コンフィギュレーション モードを開始し、IP SLA IP ホストの到達可能性を追跡します。 <ul style="list-style-type: none"> 指定できる <i>object-number</i> の範囲は 1 ~ 500 です。 指定できる <i>operation-number</i> の範囲は 1 ~ 2147483647 です。
ステップ6 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) 追跡対象オブジェクトのステート変化を通知する際の遅延時間を秒単位で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ7 end	特権 EXEC モードに戻ります。
ステップ8 show track object-number	追跡情報を表示し、設定を確認します。
ステップ9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例で、IP SLA ステート トラッキングの設定と表示方法を示します。

```
Switch(config)# track 2 200 state
Switch(config)# end
```

```
Switch# show track 2
Track 2
  Response Time Reporter 1 state
  State is Down
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

次の出力例で、ルートが到達可能であるかどうかを示します。

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
  Response Time Reporter 1 reachability
  Reachability is Up
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (millisecs) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

スタティック ルーティング サポートの設定

Cisco IOS Release 12.2(46)SE 以降の IP サービスが稼働しているスイッチは、拡張オブジェクト トラッキングのスタティック ルーティングをサポートしています。拡張オブジェクト トラッキングを使用したスタティック ルーティング サポートを使用することで、スイッチが Internet Control Message Protocol (ICMP) ping を使用して設定済みのスタティック ルートまたは DHCP ルートのダウン時を特定できます。トラッキングを有効にしている場合、システムはルート ステートを追跡し、ステートの変化をクライアントに通知できます。スタティック ルート オブジェクト トラッキングは、プライマリ ゲートウェイへの接続状態をモニタするために、Cisco IP SLA を使用して ICMP ping を生成します。

- スwitchの Cisco IP SLA サポートについては、第 47 章「Cisco IOS IP SLA 動作の設定」を参照してください。
- スタティック ルート オブジェクト トラッキングの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

次の手順に従って、スタティック ルート オブジェクト トラッキングを設定します。

-
- ステップ 1** スタティック ルーティングまたは DHCP のプライマリ インターフェイスを設定します。
 - ステップ 2** IP SLA エージェントを設定し、プライマリ インターフェイスおよびエージェント状態をモニタするトラック オブジェクトを使用して IP アドレスへ ping を実行します。
 - ステップ 3** セカンダリ インターフェイスを使用してデフォルトのスタティック ルートを設定します。このルートは、プライマリ ルートが削除された場合にだけ使用します。
-

プライマリ インターフェイスの設定

スタティック ルーティングのプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに説明を追加します。
ステップ 4	ip address ip-address mask [secondary]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。

DHCP のプライマリ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに説明を追加します。
ステップ 4	ip dhcp client route track number	DHCP クライアントを設定し、追加されたルートを指定の追跡番号に関連付けます。有効な数値は 1 ~ 500 です。
ステップ 5	ip address dhcp	DHCP からイーサネット インターフェイスの IP アドレスを取得します。
ステップ 6	exit	グローバル コンフィギュレーション モードに戻ります。

Cisco IP SLA モニタリング エージェントおよびトラック オブジェクトの設定

Cisco IP SLA でネットワーク モニタリングを設定するには、特権 EXEC モードで次の手順を実行します。

ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip sla operation-number	Cisco IP SLA 動作の設定を始め、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	icmp-echo {destination-ip-address destination hostname [source- ipaddr {ip-address hostname source-interface interface-id]}	Cisco IP SLA エンドツーエンド ICMP エコー応答時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 4	timeout milliseconds	要求パケットの応答に対する動作の待機時間を設定します。
ステップ 5	frequency seconds	動作がネットワークに送信される頻度を設定します。
ステップ 6	threshold milliseconds	反応イベントを生成し、その動作の履歴情報を保存するしきい値 (ヒステリシス) の上限を設定します。
ステップ 7	exit	IP SLA ICMP エコー コンフィギュレーション モードに戻ります。

ステップ 8	ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] start-time <i>time</i> pending now after <i>time</i>] [ageout <i>seconds</i>] [recurring]	1 つの IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 9	track <i>object-number</i> rtr <i>operation-number</i> { state reachability }	Cisco IOS IP SLA 動作の状態を追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show track <i>object-number</i>	追跡情報を表示し、設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してバックアップ スタティック ルーティングのルーティング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。手順内のコマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list <i>access-list-number</i>	拡張 IP アクセス リストを定義します。オプションの文字を設定します。
ステップ 3	route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>]	ルートマップ コンフィギュレーション モードを開始し、特定のルーティングから別のルーティングへの再配信ルートの条件を定義します。
ステップ 4	match ip address { <i>access-list number</i> <i>access-list name</i> }	標準または拡張アクセス リストに許可された宛先ネットワーク番号 アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。複数の番号または名前を入力できます。
ステップ 5	set ip next-hop dynamic dhcp	DHCP ネットワーク専用。DHCP クライアントが学んだ最新のゲートウェイへのネクスト ホップを設定します。
ステップ 6	set interface <i>interface-id</i>	スタティック ルーティング ネットワーク専用。ポリシー ルーティングのルート マップ一致条件をパスした出力パケットの送信場所を指定します。
ステップ 7	exit	ルートマップ コンフィギュレーション モードに戻ります。
ステップ 8	ip local policy route-map <i>map-tag</i>	ルート マップを特定し、ローカル ポリシー ルーティングに使用します。
ステップ 9	ip route <i>prefix mask</i> { <i>ip-address</i> <i>interface-id</i> [<i>ip-address</i>]} [<i>distance</i>] [<i>name</i>] [permanent track <i>track-number</i>] [<i>tag tag</i>]	スタティック ルーティング ネットワーク専用。スタティック ルートを確立します。 track track-number を入力し、設定のトラック オブジェクトがアップした場合にかぎり、スタティック ルートがインストールされるように指定します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show ip route track table	IP ルート トラック テーブルの情報を表示します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定例については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

拡張オブジェクト トラッキングのモニタリング

表 48-1 に示す特権 EXEC コマンドまたはユーザ EXEC コマンドを使用して、拡張オブジェクト トラッキング情報を表示します。

表 48-1 追跡情報を表示するためのコマンド

コマンド	目的
<code>show ip route track table</code>	IP ルート トラック テーブルの情報を表示します。
<code>show track [object-number]</code>	すべての追跡リストまたは指定リストの情報を表示します。
<code>show track brief</code>	追跡情報出力を 1 行表示します。
<code>show track interface [brief]</code>	追跡されたインターフェイス オブジェクトの情報を表示します。
<code>show track ip [object-number] [brief] route</code>	追跡された IP ルート オブジェクトの情報を表示します。
<code>show track resolution</code>	追跡されたパラメータの解析を表示します。
<code>show track timers</code>	追跡されたポーリング インターバル タイマーを表示します。



CHAPTER 49

WCCP を使用した Web キャッシュ サービスの設定

この章では、Web キャッシュ通信プロトコル (WCCP) を使用して、トラフィックを広域アプリケーション エンジン (Cisco Cache Engine 550 など) にリダイレクトするように IE 3000 スイッチを設定する方法について説明します。このソフトウェア リリースでは、WCCP バージョン 2 (WCCPv2) だけをサポートします。

WCCP はシスコが開発したコンテンツ ルーティング技術です。WCCP を使用すると広域アプリケーション エンジン (以降、アプリケーション エンジンと呼ぶ) をネットワーク インフラストラクチャに統合できます。アプリケーション エンジンは、頻繁にアクセスのあるコンテンツを透過的に格納し、その同じコンテンツへの要求を満たし、Web サーバから同一コンテンツが繰り返し伝送されることを防ぎます。アプリケーション エンジンは、コンテンツ配信を加速させ、最大限のスケラビリティとコンテンツの可用性を実現します。サービスプロバイダ ネットワークのアクセス ポイント (POP) で、WCCP およびアプリケーション エンジン ソリューションを展開できます。エンタープライズ ネットワークでは、地域ポイントおよび小規模ブランチ オフィスで WCCP およびアプリケーション エンジン ソリューションを展開できます。

この機能を使用するには、スイッチ上で IP サービス イメージが稼働している必要があります。



(注)

この章で使用しているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「*System Management Commands*」の「*WCCP Router Configuration Commands*」を参照してください。このマニュアルには、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「WCCP の概要」 (P.49-1)
- 「WCCP の設定」 (P.49-5)
- 「WCCP のモニタおよびメンテナンス」 (P.49-10)

WCCP の概要

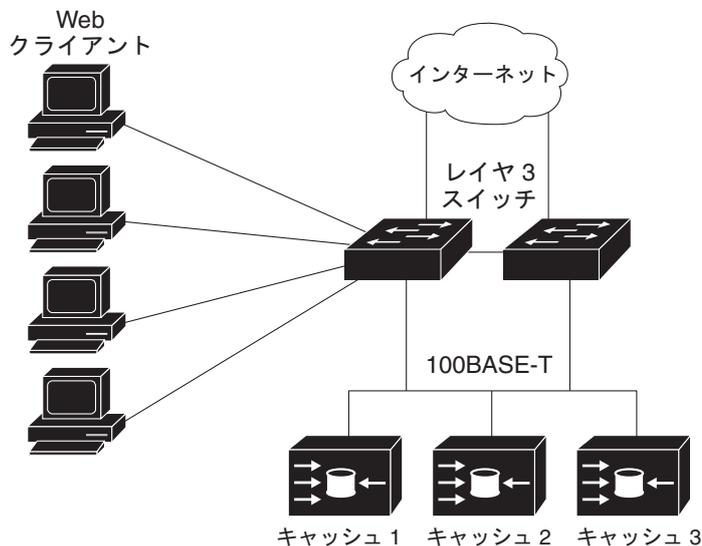
WCCP およびシスコのキャッシュ エンジン (または WCCP が稼働している他のアプリケーション エンジン) は、ネットワークでのトラフィック パターンをローカライズし、コンテンツ要求がローカルで実現されるようにします。

WCCP により、サポート対象の Cisco ルータおよびスイッチは、コンテンツ要求を透過的にリダイレクトできます。透過リダイレクトを使用すると、ユーザは使用しているブラウザが Web プロキシを使用するように設定する必要がありません。代わりに、ターゲット URL を使用してコンテンツを要求でき、その要求は自動的にアプリケーション エンジンにリダイレクトされます。透過という用語は、エンドユーザが、自分の要求したファイル (Web ページなど) が、もとの指定したサーバからではなくアプリケーション エンジンから送信されるのを知らないという意味です。

アプリケーション エンジンが要求を受け取ると、自身のローカル キャッシュからサービスしようとします。要求された情報が存在しない場合、アプリケーション エンジンは別個の要求をエンドサーバに送信し、要求された情報を取得します。取得した情報は、アプリケーション エンジンが要求元のクライアントに転送するとともに、その後の要求に応えるため、情報をキャッシュします。

WCCP では、アプリケーションエンジン クラスタ (一連のアプリケーション エンジン) は、[図 49-1](#)にあるように、複数のルータまたはスイッチにサービスできます。

図 49-1 シスコのキャッシュ エンジンおよび WCCP ネットワーク コンフィギュレーション



WCCP メッセージ交換

この一連のイベントでは、WCCP メッセージ交換を説明します。

1. アプリケーション エンジンは、WCCP を使用して IP アドレスを WCCP 対応スイッチに送信し、*Here I am* メッセージを通して自己の存在を伝えます。スイッチおよびアプリケーション エンジンは、UDP ポート 2048 に基づき、制御チャネルを介して互いに通信します。
2. WCCP 対応スイッチは、アプリケーション エンジンの IP 情報を使用してクラスタ ビュー (クラスタ内のアプリケーション エンジンのリスト) を作成します。このビューが、*I see you* メッセージでクラスタ内の各アプリケーション エンジンに送信すると、本質的にすべてのアプリケーション エンジンが互いの存在を認識するようになります。クラスタのメンバーシップが一定時間同じままになった後で、安定したビューが確立されます。
3. 安定したビューが確立されると、クラスタ内の低い IP アドレスを持つアプリケーション エンジンが指定アプリケーション エンジンとして選択されます。

WCCP ネゴシエーション

WCCP プロトコル メッセージを交換するとき、指定アプリケーション エンジンおよび WCCP 対応スイッチは次の項目をネゴシエートします。

- 転送方式 (スイッチがパケットをアプリケーション エンジンに転送するとき使用される方式)。スイッチは、パケット宛先 MAC アドレスをターゲット アプリケーション エンジン MAC アドレスに置き換えて、レイヤ 2 ヘッダーを書き換えます。次にスイッチは、パケットをアプリケーション エンジンに転送します。この転送方式では、ターゲット アプリケーション エンジンがレイヤ 2 でスイッチに直接接続されている必要があります。
- 割り当て方式 (パケットをクラスタ内のアプリケーション エンジン間に配信するとき使用される方式)。スイッチは宛先 IP アドレス、送信元 IP アドレス、宛先レイヤ 4 ポート、および送信元レイヤ 4 ポートの一部のビットを使用して、リダイレクトされたパケットを受け取るアプリケーション エンジンを判別します。
- パケット戻し方式 (パケットをアプリケーション エンジンから通常の転送用スイッチに戻るとき使用される方式)。アプリケーション エンジンがパケットを拒否し、パケット戻し機能を起動するのは以下の理由があります。
 - アプリケーション エンジンが過負荷となり、パケットにサービスする余裕がない。
 - アプリケーション エンジンが Web サーバからエラー メッセージ (プロトコル エラーや認証エラーなど) を受け取り、ダイナミック クライアント バイパス機能を使用している。バイパスは、クライアントがアプリケーション エンジンをバイパスし、Web サーバに直接接続できるようにします。

アプリケーション エンジンがパケットを WCCP 対応スイッチに戻し、アプリケーション エンジンが存在しないかのように Web サーバに転送します。アプリケーション エンジンは、再接続試行を代行受信しません。このようにして、アプリケーション エンジンは効率的にアプリケーション エンジンへのパケットのリダイレクトをキャンセルし、バイパス フローを作成します。戻し方式が **Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化)** である場合、スイッチは、アプリケーション エンジンで設定されている GRE トンネルを介して戻されたパケットを受け取ります。スイッチの CPU は **Cisco Express Forwarding (CEF)** を使用して、これらのパケットをターゲット Web サーバに送信します。戻し方式がレイヤ 2 書き換えである場合、パケットはハードウェア内でターゲット Web サーバに転送されます。サーバが要求された情報に回答しているとき、スイッチは通常のレイヤ 3 転送を使用して、情報を要求しているクライアントに戻します。

MD5 セキュリティ

WCCP は各プロトコル メッセージでオプションのセキュリティ コンポーネントを提供し、スイッチとアプリケーション エンジン間のメッセージで MD5 認証をスイッチが使用できるようにします。(スイッチの認証がイネーブルになっているとき) MD5 で認証されないメッセージは、スイッチによって廃棄されます。パスワード文字列は、MD5 値と組み合わせられ、スイッチとアプリケーション エンジン間の接続のセキュリティを確立します。各アプリケーション エンジンで同じパスワードを設定する必要があります。

パケットのリダイレクトおよびサービス グループ

WCCP を設定して、FTP、プロキシ Web キャッシュ処理、音声およびビデオアプリケーションなど、リダイレクト用トラフィックを分類できます。この分類はサービス グループと呼ばれ、プロトコル タイプ (TCP または UDP) およびレイヤ 4 送信元ポート番号と宛先ポート番号に基づきます。サービス グループは、TCP ポート 80 を意味する、Web キャッシュなどの Well-known 名または 0 ~ 99 のサー

ビス番号のいずれかで識別されます。サービス グループは、プロトコルおよびレイヤ 4 ポート番号にマッピングするように設定され、独立して確立および維持されます。WCCP は、アプリケーション エンジンに加入して分類基準を動的に提供するダイナミック サービス グループを許可します。

スイッチまたはスイッチ スタックでは最大 8 つまでのサービス グループを、サービス グループにつき 32 までのキャッシュ エンジンを設定できます。WCCP のグループ定義には、サービス グループのプライオリティがあります。WCCP は、プライオリティを使用して、スイッチ ハードウェアのサービス グループを設定します。たとえば、サービス グループ 1 はプライオリティ 100 で、宛先ポート 80 を探していて、サービス グループ 2 はプライオリティ 50 で、送信元ポート 80 を探している場合、送信元および宛先ポート 80 の着信パケットは、サービス グループ 1 を使用して転送されます。これは、サービス グループ 1 の方がプライオリティが高いためです。

WCCP は各サービス グループのアプリケーション エンジンのクラスタをサポートします。リダイレクトされたトラフィックは、アプリケーション エンジンの 1 つに送信可能です。スイッチは、サービス グループのクラスタ内のアプリケーション エンジン間で、トラフィックのロードバランシングのマスク割り当て方式をサポートします。

WCCP がスイッチ上で設定された後、スイッチはクライアントから受信したすべてのサービス グループ パケットをアプリケーション エンジンに転送します。ただし、以下のパケットはリダイレクトされません。

- アプリケーション エンジンから発信され、Web サーバに宛てられたパケット
- アプリケーション エンジンから発信され、クライアントに宛てられたパケット
- アプリケーション エンジンにより返送または拒否されたパケット。これらのパケットは、Web サーバに送信されます。

プロトコル メッセージの送受信に、サービス グループにつき 1 つのマルチキャスト アドレスを設定できます。マルチキャスト アドレスが 1 つの場合、アプリケーション エンジンは通知を 1 つのアドレスに送信することになり、たとえば 225.0.0.0 など、サービス グループのすべてのルータにカバレッジを提供します。ルータを動的に追加および削除する場合、1 つのマルチキャスト アドレスを使用することで、コンフィギュレーションが簡単になります。これは、特に WCCP ネットワークのすべてのデバイスのアドレスを入力する必要がないためです。

ルータ グループ リストを使用すれば、アプリケーション エンジンから受け取ったプロトコル パケットを検証できます。グループ リストのアドレスに一致するパケットは処理され、グループ リスト アドレスに一致しないパケットはドロップされます。

特定クライアント、サーバ、またはクライアントとサーバのペアのキャッシングをディセーブルにするには、WCCP リダイレクト Access Control List (ACL) を使用します。リダイレクト ACL に一致しないパケットはキャッシュをバイパスし、通常どおりに転送されます。

WCCP パケットがリダイレクトされる前、スイッチはインターフェイス上に設定されているすべての着信機能に関連した ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。



(注)

WCCP リダイレクト リストでは、許可 ACL エントリだけがサポートされます。

パケットがリダイレクトされると、リダイレクトされたインターフェイスに関連付けられた出力 ACL がパケットに適用されます。元のポートに関連付けられた ACL は、リダイレクトされたインターフェイス上で必須出力 ACL を特に設定しない限り適用されません。

サポートしない WCCP 機能

次の WCCP 機能は、このソフトウェア リリースでサポートされていません。

- **ip wccp redirect out** インターフェイス コンフィギュレーション コマンドを使用して設定された発信インターフェイスでのパケットのリダイレクト（このコマンドはサポートされません）
- パケットリダイレクトの GRE 転送方式
- ロードバランシング用のハッシュ割り当て方式
- WCCP への SNMP サポート

WCCP の設定

ここでは、スイッチで WCCP を設定する方法について説明します。

- 「[WCCP のデフォルト設定](#)」(P.49-5)
- 「[WCCP 設定時の注意事項](#)」(P.49-5)
- 「[Web Cache Service のイネーブル化](#)」(P.49-6)（必須）

WCCP のデフォルト設定

表 49-1 に、WCCP のデフォルト設定を示します。

表 49-1 WCCP のデフォルト設定

機能	デフォルト設定
WCCP イネーブル ステート	WCCP サービスはディセーブルです。
プロトコル バージョン	WCCPv2
インターフェイス上で受信したトラフィックのリダイレクト	ディセーブル

WCCP 設定時の注意事項

スイッチで WCCP を設定する前に、次に挙げる設定時の注意事項を確認してください。

- 同じサービス グループ内のアプリケーション エンジンおよびスイッチは、WCCP 対応のスイッチに直接接続された同一サブネットワーク内に存在する必要があります。
- Web クライアント、アプリケーション エンジン、およびレイヤ 3 インターフェイスとしての Web サーバ（ルーテッド ポートおよびスイッチ仮想インターフェイス [SVI]）に接続されたスイッチ インターフェイスを設定します。WCCP パケットのリダイレクトが機能するためには、サーバ、アプリケーション エンジン、およびクライアントが、異なるサブネット上に存在する必要があります。
- 各アプリケーション エンジンに 1 つのマルチキャスト アドレスを設定するときは、予約されていないマルチキャスト アドレスだけを使用します。
- WCCP エントリおよび PBR エントリは、同じ TCAM リージョンを使用します。WCCP は、PBR（アクセス、ルーティング、デュアル IPv4/v6 ルーティング）をサポートするテンプレート上でだけサポートされます。
- TCAM エントリを WCCP エントリの追加に使用できない場合、パケットはリダイレクトされず、標準ルーティング テーブルを使用して転送されます。

- 使用可能な PBR ラベルの数は、WCCP 入力方法でイネーブルになるインターフェイスが増えるにつれて減っていきます。サービス グループをサポートする各インターフェイスでは、ラベルが 1 つ消費されます。WCCP ラベルは PBR ラベルから取得されます。PBR と WCCP 間で使用可能なラベルを監視および管理する必要があります。ラベルが使用できないと、スイッチはサービス グループを追加できなくなります。ただし、別のインターフェイスに同じ連のサービス グループがある場合、新しいラベルは必要にならず、グループをインターフェイスに追加できます。
- スタック メンバー スイッチで設定されたルーティング最大伝送単位 (MTU) サイズは、クライアント MTU サイズより長い必要があります。アプリケーション エンジンに接続されたポートで設定された MAC レイヤ MTU サイズは、GRE トンネル ヘッダー バイトを考慮する必要があります。
- 同じスイッチ インターフェイス上では、WCCP と VPN ルーティングおよび転送 (VRF) を設定できません。
- 同じスイッチ インターフェイス上では、WCCP および PBR を設定できません。
- 同じスイッチ インターフェイス上では、WCCP およびプライベート VLAN (PVLAN) を設定できません。

Web Cache Service のイネーブル化

WCCP パケットリダイレクトが機能するために、クライアントに接続されたスイッチ インターフェイスが着信パケットをリダイレクトするように設定する必要があります。

この手順では、ルーテッド ポートでこれらの機能を設定する方法を示します。これらの機能を SVI で設定するには、手順に従った設定例を参照してください。



(注)

WCCP コマンドを設定する前に SDM テンプレートを設定し、スイッチを再起動します。詳細については、第 10 章「SDM テンプレートの設定」を参照してください。

Web キャッシュ サービスをイネーブルにしたり、マルチキャスト グループ アドレスまたはグループ リストを設定したり、ルーテッド インターフェイスを設定したり、クライアントから受信した着信パケットをアプリケーション エンジンにリダイレクトしたり、マルチキャスト アドレスを受信するように インターフェイスをイネーブルにしたり、パスワードを設定したりするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip wccp {web-cache service-number} [group-address groupaddress] [group-list access-list] [redirect-list access-list] [password encryption-number password]	<p>Web キャッシュ サービスをイネーブルにし、アプリケーション エンジンで定義されたダイナミック サービスに対応するサービス番号を指定します。デフォルトでは、この機能はディセーブルになっています。</p> <p>(任意) group-address groupaddress には、スイッチおよびアプリケーション エンジンがサービス グループに加入するときに使用するマルチキャスト グループ アドレスを指定します。</p> <p>(任意) group-list access-list には、マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。</p> <p>(任意) redirect-list access-list には、特定ホストのリダイレクト サービスまたはホストから特定パケットを指定します。</p> <p>(任意) password encryption-number password には、暗号化番号を指定します。指定できる範囲は 0 ~ 7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。7 文字以内でパスワード名を指定します。スイッチは、パスワードと MD5 認証値を組み合わせて、スイッチとアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。</p> <p>各アプリケーション エンジンで同じパスワードを設定する必要があります。</p> <p>認証がイネーブルになっている場合、スイッチは認証されないメッセージを廃棄します。</p>
ステップ 3 interface interface-id	アプリケーション エンジンまたは Web サーバに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 no switchport	レイヤ 3 モードを開始します。
ステップ 5 ip address ip-address subnet-mask	IP アドレスおよびサブネット マスクを設定します。
ステップ 6 no shutdown	インターフェイスをイネーブルにします。
ステップ 7 exit	グローバル コンフィギュレーション モードに戻ります。各アプリケーション エンジンおよび Web サーバにステップ 3 ~ 7 を繰り返します。
ステップ 8 interface interface-id	クライアントに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9 no switchport	レイヤ 3 モードを開始します。
ステップ 10 ip address ip-address subnet-mask	IP アドレスおよびサブネット マスクを設定します。
ステップ 11 no shutdown	インターフェイスをイネーブルにします。
ステップ 12 ip wccp {web-cache service-number} redirect in	クライアントから受信したパケットをアプリケーション エンジンにリダイレクトします。クライアントに接続されているインターフェイス上でイネーブルにします。

	コマンド	目的
ステップ 13	ip wccp {web-cache service-number} group-listen	(任意) マルチキャスト グループ アドレスを使用するとき、 group-listen はインターフェイスをイネーブルにしてマルチキャスト アドレスを受信します。アプリケーション エンジンに接続されているインターフェイス上でイネーブルにします。
ステップ 14	exit	グローバル コンフィギュレーション モードに戻ります。各クライアントにステップ 8 ~ 13 を繰り返します。
ステップ 15	end	特権 EXEC モードに戻ります。
ステップ 16	show ip wccp web-cache および show running-config	設定を確認します。
ステップ 17	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Web キャッシュ サービスをディセーブルにするには、**no ip wccp web-cache** グローバル コンフィギュレーション コマンドを使用します。着信パケット リダイレクトをディセーブルにするには、**no ip wccp web-cache redirect in** インターフェイス コンフィギュレーション コマンドを使用します。この手順を完了した後、ネットワークでアプリケーション エンジンを設定する必要があります。

次に、ルーテッド インターフェイスを設定し、マルチキャスト グループ アドレスとリダイレクト アクセス リストで Web キャッシュ サービスをイネーブルにする例を示します。ギガビット イーサネット ポート 1 はアプリケーション エンジンに接続され、IP アドレス 172.20.10.30 のルーテッド ポートとして設定され、再イネーブル化されています。ギガビット イーサネット ポート 2 はインターネット経由で Web サーバに接続され、IP アドレス 175.20.20.10 のルーテッド ポートとして設定され、再イネーブル化されています。ギガビット イーサネット ポート 3 ~ 6 はクライアントに接続され、IP アドレス 175.20.30.20、175.20.40.30、175.20.50.40、および 175.20.60.50 のルーテッド ポートとして設定されています。スイッチはマルチキャスト トラフィックを受信し、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.40.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/5
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address 175.20.50.40 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/6
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.60.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
```

次に、SVI を設定し、マルチキャスト グループ リストで Web キャッシュ サービスをイネーブルにする例を示します。VLAN 299 は、IP アドレス 175.20.20.10 で作成および設定されています。ギガビットイーサネットのポート 1 をインターネット経由で Web サーバに接続し、VLAN 299 のアクセスポートとして設定します。VLAN 300 は、IP アドレス 172.20.10.30 で作成および設定されています。ギガビットイーサネット ポート 2 はアプリケーション エンジンに接続され、VLAN 300 のアクセスポートとして設定されています。VLAN 301 は、IP アドレス 175.20.30.50 で作成および設定されています。クライアントに接続されているファストイーサネット ポート 3～6 は、VLAN 301 のアクセスポートとして設定されています。スイッチは、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。



(注)

リダイレクトリストには許可 ACL エントリだけを使用します。拒否エントリはサポートされていません。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-list 15
Switch(config)# access-list 15 permit host 171.69.198.102
Switch(config)# access-list 15 permit host 171.69.198.104
Switch(config)# access-list 15 permit host 171.69.198.106
Switch(config)# vlan 299
Switch(config-vlan)# exit
Switch(config)# interface vlan 299
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 299
Switch(config)# vlan 300
Switch(config-vlan)# exit
Switch(config)# interface vlan 300
Switch(config-if)# ip address 171.69.198.100 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 300
Switch(config-if)# exit
Switch(config)# vlan 301
Switch(config-vlan)# exit
Switch(config)# interface vlan 301
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/3 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 301
Switch(config-if-range)# exit
```

WCCP のモニタおよびメンテナンス

WCCP をモニタしてメンテナンスするには、表 49-2 に記載された特権 EXEC コマンドを 1 つまたは複数使用します。

表 49-2 WCCP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>clear ip wccp web-cache</code>	Web キャッシュ サービスの統計情報を削除します。
<code>show ip wccp web-cache</code>	WCCP に関連するグローバル情報を表示します。
<code>show ip wccp web-cache detail</code>	WCCP クラスタのスイッチおよびすべてのアプリケーション エンジンの情報を表示します。
<code>show ip interface</code>	たとえば、「Web Cache Redirect is enabled / disabled.」など、インターフェイス上で設定された IP WCCP リダイレクト コマンドに関するステータスを表示します。
<code>show ip wccp web-cache view</code>	他のどのメンバーが検出されたか、またはされなかったのかを表示します。



CHAPTER 50

IP マルチキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP マルチキャスト ルーティングを設定する方法について説明します。IP マルチキャストは、ネットワークのリソースをより効率的に使用する方法です。特に、音声やビデオなど、帯域幅を消費するサービスに効果があります。IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP 「マルチキャスト グループ アドレス」と呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバー）のグループにパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

この IP マルチキャスト ルーティング機能を使用するには、スイッチ上で IP サービス イメージが稼働している必要があります。



(注)

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

この章の内容は、次のとおりです。

- 「Cisco IP マルチキャスト ルーティングの実装の概要」 (P.50-1)
- 「IP マルチキャスト ルーティングの設定」 (P.50-10)
- 「高度な PIM 機能の設定」 (P.50-37)
- 「オプションの IGMP 機能の設定」 (P.50-40)
- 「オプションのマルチキャスト ルーティング機能の設定」 (P.50-46)
- 「基本的な DVMRP 相互運用性機能の設定」 (P.50-50)
- 「高度な DVMRP 相互運用性機能の設定」 (P.50-56)
- 「IP マルチキャスト ルーティングのモニタおよびメンテナンス」 (P.50-63)

Multicast Source Discovery Protocol (MSDP) の設定の詳細については、第 51 章「MSDP の設定」を参照してください。

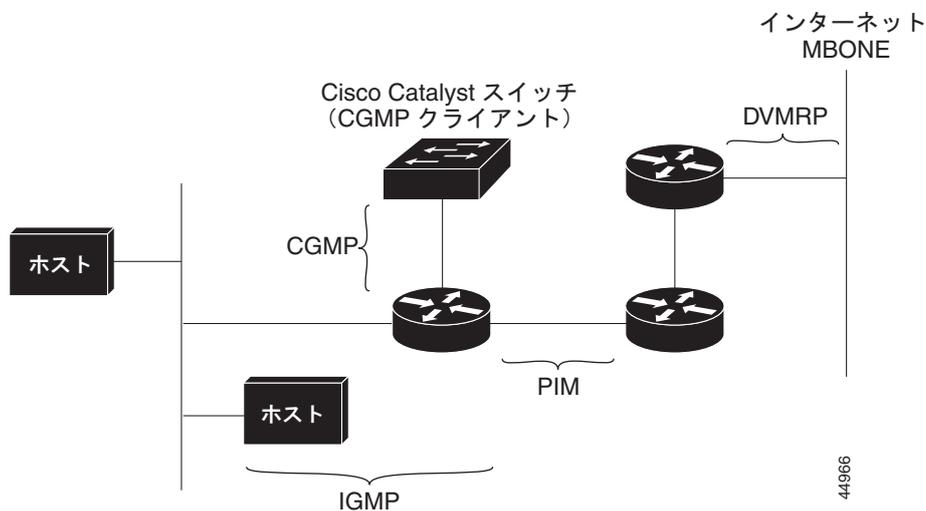
Cisco IP マルチキャスト ルーティングの実装の概要

Cisco IOS ソフトウェアは IP マルチキャスト ルーティングを実装するため、次のプロトコルをサポートしています。

- Internet Group Management Protocol (IGMP) : LAN のホストおよび LAN のルータ (およびマルチレイヤ スイッチ) 間で使用され、ホストがメンバーとして属するマルチキャスト グループを追跡します。
- Protocol-Independent Multicast (PIM) : ルータおよびマルチレイヤ スイッチ間で使用され、相互に転送されるマルチキャスト パケット、および直接接続された LAN に転送されるマルチキャスト パケットを追跡します。
- Distance Vector Multicast Routing Protocol (DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル) : インターネットの Multicast Backbone (MBONE) に使用されます。ソフトウェアは PIM と DVMRP の相互作用をサポートします。
- Cisco Group Management Protocol (CGMP) : レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。

図 50-1 に、これらのプロトコルが動作する IP マルチキャスト環境内の位置を示します。

図 50-1 IP マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャストアドレスは 0100:5e で始まり、IP アドレスの末尾 23 ビットが付加されます。Catalyst 3560 スイッチでは、マルチキャスト パケットがスイッチのマルチキャストアドレスと一致しない場合、パケットは次のように取り扱われます。

- パケットにマルチキャスト IP アドレスとユニキャスト MAC アドレスがある場合、パケットはソフトウェアで転送されます。これは、従来型デバイスのプロトコルの中に、マルチキャスト IP アドレスとともにユニキャスト MAC アドレスを使用するものがあるために発生します。
- パケットにマルチキャスト IP アドレスと不一致のマルチキャスト MAC アドレスがある場合、パケットはドロップします。

ここでは、次の情報について説明します。

- 「[IGMP の概要](#)」 (P.50-3)
- 「[PIM の概要](#)」 (P.50-4)
- 「[DVMRP の概要](#)」 (P.50-9)
- 「[CGMP の概要](#)」 (P.50-9)

IGMP の概要

IP マルチキャストリングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。このプロトコルは、クエリアおよびホストの役割を定義します。

- クエリアは、指定されたマルチキャスト グループに属するネットワーク デバイスを検出するためのクエリー メッセージを送信するネットワーク デバイスです。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバです。

同じ送信元からのマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは IGMP メッセージを使用して、マルチキャスト グループに加入および脱退します。

どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。マルチキャスト グループのアクティブ状態および所属メンバーは、グループや時間によって変化し、マルチキャスト グループを長時間または短時間アクティブにすることもできます。グループのメンバーシップはいつでも変更可能です。メンバーを含むグループにアクティビティがない場合もあります。

IP マルチキャスト トラフィックには、グループ アドレス（クラス D アドレス）が使用されます。クラス D アドレスの上位ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ~ 239.255.255.255 です。224.0.0.0 ~ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは、次に示す IP マルチキャスト グループ アドレスを使用して送信されます。

- IGMP 汎用クエリアは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象グループの IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象グループの IP アドレスを宛先とします。
- IGMPv2 (IGMP バージョン 2) Leave メッセージは、アドレス 224.0.0.2（サブネット上のすべてのマルチキャスト ルータ）を宛先とします。古いホスト IP スタックの中には、Leave メッセージの宛先がすべてのルータのアドレスでなく、グループの IP アドレスとなっているものがあります。

IGMPv1

IGMP Version 1 (IGMPv1) にはクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ スイッチは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

PIM の概要

PIM はプロトコルに依存しません。ユニキャスト ルーティング テーブルを読み込むために使用されるユニキャスト ルーティング プロトコルに関係なく、このテーブルの情報を使用してマルチキャスト転送を実行します。マルチキャスト ルーティング テーブルは個別に維持されません。

PIM は、RFC 2362 『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』で規定されています。次に示す Internet Engineering Task Force (IETF) インターネット ドラフトを参照してください。

- 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』
- 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』
- 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』
- 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』
- 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント (RP) を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップ ルータ (BSP) は耐障害性のある、自動化された RP ディスカバリ メカニズム、および配信メカニズムを提供します。これらのメカニズムにより、ルータおよびマルチレイヤ スイッチはグループ/RP マッピングを動的に取得できます。
- Sparse Mode (SM; スパース モード) および Dense Mode (DM; デンス モード) は、インターフェイスではなく、グループに関するプロパティです。SM または DM のいずれか一方だけでなく、SM-DM (sparse-dense モード) を使用してください。
- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリーを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RP への登録メッセージが境界ルータによって送信されるか、あるいは指定ルータによって送信されるかは、メッセージ自身によって指定されます。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

PIM のモード

PIM は DM、SM、または PIM SM-DM のいずれかのモードで動作します。PIM DM-SM では、スパース グループとデンス グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元ベースのマルチキャスト配信ツリーが構築されます。DM の場合、PIM DM のルータまたはマルチレイヤ スイッチは、他のすべてのルータまたはマルチレイヤ スイッチで常にグループ宛てのマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバーが存在しない場合、PIM DM デバイスがマルチキャスト パケットを受信すると、プルーン メッセージが送信元に送信され、不要なマルチキャスト トラフィックが停止されます。このプルーン済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラディングしません。レシーバーを含まないブランチが配信ツリーからプルーンされ、レシーバーを含むブランチだけが存続するためです。

プルーン済みツリー内ブランチのレシーバがマルチキャスト グループに新規に加入すると、PIM DM デバイスは新しいレシーバを検出し、配信ツリーの送信元方向にすぐに接合メッセージを送信します。アップストリームの PIM DM デバイスが接合メッセージを受信すると、受信したデバイスは接合メッセージが着信したインターフェイスをすぐにフォワーディング ステートにし、マルチキャスト トラフィックのレシーバへの転送を開始します。

PIM SM

PIM SM は共有ツリーおよび Shortest-Path-Trees (SPT) を使用し、マルチキャスト トラフィックをネットワーク内のマルチキャスト レシーバーに配信します。PIM SM の場合、ルータまたはマルチレイヤ スイッチは、トラフィックに関する明示的な要求 (Join メッセージ) がないかぎり、他のルータまたはスイッチではグループ宛てのマルチキャスト パケットが転送されないと想定します。IGMP を使用してホストがマルチキャスト グループに加入すると、直接接続された PIM SM デバイスは、RP と呼ばれるルートに向けて PIM Join メッセージを送信します。この Join メッセージはルートに向かってルータを順次移動しながら、共有ツリーのブランチを作成します。

RP はマルチキャスト レシーバーを追跡します。また、送信元の先頭ホップ ルータ (指定ルータ (DR)) から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバへの共有ツリーパスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信し、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルーンする場合は、プルーン メッセージが配信ツリーの上方方向に送信されます。この結果、明示的な Join メッセージによって作成された共有ツリーまたは SPT のブランチが不要になった場合、これらの解除が可能となります。

PIM スタブルーティング

PIM スタブルーティング機能は、エンドユーザの近くにルーテッド トラフィックを移動し、リソースの利用率を軽減します。

PIM スタブルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブルーティングを設定しているスイッチ経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト (IGMP) レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

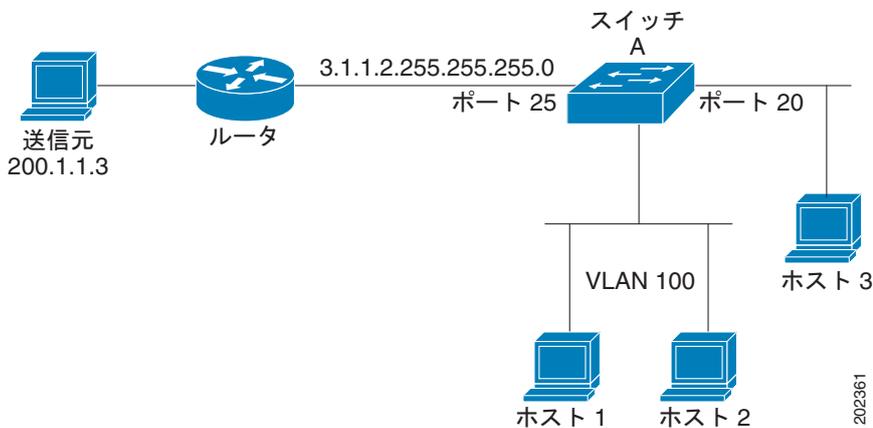
PIM スタブルーティングを使用しているときは、IP マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、IP サービス フィーチャセットにアップグレードする必要があります。

また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「[EIGRP スタブ ルーティングの設定](#)」(P.41-42) を参照してください。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長 トポロジーが存在します。PIM メッセージはブロックされ、PIM 資産および指定ルータ検出メカニズムは、PIM 受動インターフェイスでサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされません。非冗長 トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

図 50-2 では、スイッチ A ルーテッドアップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できます。詳細については、「[PIM スタブ ルーティングの設定](#)」(P.50-23) を参照してください。

図 50-2 PIM スタブ ルータ設定



IGMP ヘルパー

PIM スタブ ルーティングによって、ルーテッド トラフィックがエンド ユーザの近くに移動し、ネットワーク トラフィックが軽減されます。また、スタブ ルータ (スイッチ) に IGMP ヘルパー機能を設定してトラフィックを軽減させることもできます。

igmp helper help-address インターフェイス コンフィギュレーション コマンドを使用してスタブ ルータ (スイッチ) を設定すると、スイッチによるネクストホップ インターフェイスへのレポート送信をイネーブルにできます。ダウンストリーム ルータに直接接続されていないホストはアップストリーム ネットワークの送信元マルチキャスト グループに加入できます。この機能が設定されていると、マルチキャスト ストリームへの加入を求めるホストからの IGMP パケットはアップストリームのネクストホップ デバイスに転送されます。アップストリームのセントラル ルータは、ヘルパー IGMP レポートまたは leave を受信すると、そのグループの発信インターフェイス リストからインターフェイスの追加または削除を行います。

ip igmp helper-address コマンドの詳細な構文と使い方については、『[Cisco IOS IP and IP Routing Command Reference, Release 12.1](#)』を参照してください。

自動 RP

この独自の機能により、ネットワーク内のルータまたはマルチレイヤ スイッチごとに RP 情報を手動で設定する必要がなくなります。自動 RP を機能させるには、Cisco ルータまたはマルチレイヤ スイッチをマッピング エージェントとして設定します。マッピング エージェントは IP マルチキャストを使用して、候補 RP アナウンスメントを受信する候補 RP として設定可能なネットワーク内のルータまたはスイッチを取得します。候補 RP はマルチキャスト RP アナウンス メッセージを特定のグループまたはグループ範囲に定期的送信し、それらが使用可能であることをアナウンスします。

マッピング エージェントはこれらの候補 RP アナウンスメントを受信し、この情報を使用して、グループ/RP マッピング キャッシュにエントリを作成します。受信されたグループ/RP 範囲に対して複数の候補 RP が RP アナウンスメントを送信した場合でも、この範囲には 1 つのマッピング キャッシュ エントリだけが作成されます。RP アナウンス メッセージ着信時に、マッピング エージェントは IP が最大であるルータまたはスイッチをアクティブ RP として選択し、この RP アドレスをグループ/RP マッピング キャッシュ内に保存します。

マッピング エージェントは、グループ/RP マッピング キャッシュの内容を定期的にマルチキャストします。このため、すべてのルータおよびスイッチで、サポート対象のグループに使用される RP が自動的に検出されます。ルータまたはスイッチが RP ディスカバリ メッセージの受信に失敗し、グループ/RP マッピング情報が期限切れになると、ルータまたはスイッチは、`ip pim rp-address` グローバル コンフィギュレーション コマンドによって定義された、静的に設定された RP に変更されます。静的に設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を DM に変更します。

複数の RP がさまざまなグループ範囲として、または互いのホット バックアップとして機能します。

BSR

PIMv2 BSR は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤ スイッチに配信する別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由してホップ単位で送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR によって、Time to Live (TTL; 存続可能時間) 値が 1 である BSR メッセージが送信されます。隣接する PIMv2 ルータまたはマルチレイヤ スイッチは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス (BSR メッセージの着信インターフェイスを除く) にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップ単位で移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディング メカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズメントを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップ単位で移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送および逆経路チェック

ユニキャストルーティングの場合、ルータおよびマルチレイヤスイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが格納されている宛先ホストへ、ネットワーク内の単一のパスに沿ってトラフィックを送信します。パス上の各ルータおよびスイッチはユニキャストルーティングテーブル内の宛先アドレスを参照し、指定されたインターフェイスを経由して、宛先方向のネクストホップへパケットを転送します。そのあと、パケット内の宛先 IP アドレスを使用して、ユニキャスト転送判断を行います。

マルチキャストルーティングの場合、送信元は IP パケットの宛先アドレス フィールドに格納された、マルチキャストグループアドレスで表されるホストの任意のグループにトラフィックを送信します。着信マルチキャストパケットの転送または、ドロップを決定するため、ルータまたはマルチレイヤスイッチで、パケットに対する Reverse Path Forwarding (RPF) チェックを使用します (図 50-3 を参照)。

1. ルータまたはマルチレイヤスイッチは着信したマルチキャストパケットの送信元アドレスを調べ、逆経路上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。
2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス (ルータのすべてのインターフェイスとは限りません) にパケットが転送されます。
3. RPF チェックに失敗した場合、パケットは廃棄されます。

DVMRP など一部のマルチキャストルーティングプロトコルでは、マルチキャストルーティングテーブルは個別に維持され、RPF チェックに使用されます。ただし、PIM では RPF チェックを実行するためにユニキャストルーティングテーブルが使用されます。

図 50-3 に、送信元 151.10.3.21 からのマルチキャストパケットを受信するポート 2 を示します。表 50-1 により、送信元への逆経路上にあるポートはポート 2 ではなく、ポート 1 であることがわかります。RPF チェックに失敗したため、マルチレイヤスイッチはパケットを廃棄します。送信元 151.10.3.21 からの別のマルチキャストパケットは、ポート 1 に着信します。ルーティングテーブルにより、このポートは送信元への逆経路上にあることがわかります。RPF チェックに合格したため、パケットは発信ポート リスト内のすべてのポートに転送されます。

図 50-3 RPF チェック

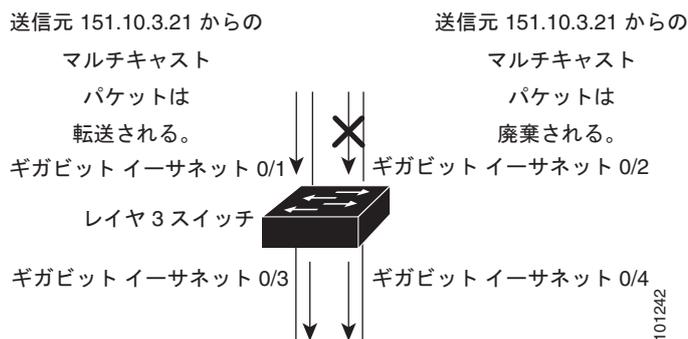


表 50-1 RPF チェックのルーティング テーブル例

ネットワーク	ポート
151.10.0.0/16	ギガビット イーサネット 0/1
198.14.32.0/32	ギガビット イーサネット 0/3
204.1.16.0/24	ギガビット イーサネット 0/4

101242

PIM は送信元ツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します（「PIM DM」(P.50-5) および「PIM SM」(P.50-5) を参照）。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤ スイッチが送信元ツリー ステートである場合（つまり [S,G] エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ スイッチが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

PIM SM は RPF 参照機能を使用し、加入およびブルーニング メッセージを送信する必要があるかどうかを決定します。

- (S,G) Join メッセージ（送信元ツリー ステート）は送信元に向け送信されます。
- (*,G) Join メッセージ（共有ツリー ステート）は RP に向け送信されます。

DVMRP および PIM DM では送信元ツリーだけが使用され、上記のように RPF が使用されます。

DVMRP の概要

DVMRP は多くのベンダーのデバイスに実装されており、パブリック ドメインでマルチキャスト ルーティング (mroute) されたプログラムに基づいて動作します。このプロトコルは MBONE、およびその他のドメイン内マルチキャスト ネットワークに採用されています。

Cisco ルータおよびマルチレイヤ スイッチでは PIM が動作し、マルチキャスト パケットの DVMRP ネイバーへの転送および、DVMRP ネイバーからの受信を可能にします。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。ソフトウェアは DVMRP ルートを伝播し、ルータやマルチレイヤ スイッチごとにこれらのルートのデータベースを個別に構築します。ただし、PIM はこのルーティング情報をパケット転送判断に使用します。ソフトウェアに完全な DVMRP は実装されていません。ただし、DVMRP ルータのダイナミック ディスカバリをサポートし、従来のメディア（イーサネットやファイバ分散データ インターフェイス (FDDI) など）または DVMRP 固有のトンネルを通して、これらを相互運用します。

DVMRP ネイバーは、送信元ネットワーク ルーティング情報をルートレポート メッセージに格納して定期的に交換し、ルート テーブルを構築します。DVMRP ルーティング テーブルに格納されているルーティング情報は、ユニキャスト ルーティング テーブルから独立し、送信元配信ツリーの構築および、RPF によるマルチキャスト転送の実行に使用されます。

DVMRP は DM プロトコルです。抑制されたマルチキャスト モデルを使用して親子データベースを構築し、マルチキャスト パケットの送信元でルーティングされた転送ツリーを構築します。マルチキャスト パケットはまず、この送信元ツリーの下方向にフラッディングされます。冗長パスが送信元ツリー上にある場合、パケットはこれらのパスに沿って転送されません。これらの親子リンクでブルーニング メッセージが受信されるまで転送が行われ、これによってマルチキャスト パケットのブロードキャストが抑制されます。

CGMP の概要

このソフトウェア リリースは、スイッチ上で CGMP サーバサポート機能を提供します。クライアント側の機能は提供されません。スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれているデバイス用の CGMP サーバとして機能します。

CGMP はレイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。CGMP を使用すると、レイヤ 2 グループメンバーシップ情報を CGMP サーバからスイッチに通信できます。これにより、スイッチはすべてのスイッチ インターフェイスにマルチキャスト トラフィックをフラッドしない、マルチキャストメンバーが存在するインターフェイスを取得できるようになります (IGMP スヌーピングは、マルチキャスト パケットのフラッドを抑制するためのもう 1 つの方法です)。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。

CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポートメッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

CGMP と HSRPv1 は両立できません。CGMP 脱退処理と HSRPv1 を同時にイネーブルにできません。ただし、CGMP と HSRPv2 は同時にイネーブルにできます。詳細については、「HSRP のバージョン」(P.46-3) を参照してください。

IP マルチキャスト ルーティングの設定

ここでは、次の設定について説明します。

- 「マルチキャスト ルーティングのデフォルト設定」(P.50-10)
- 「マルチキャスト ルーティング設定時の注意事項」(P.50-11)
- 「基本的なマルチキャスト ルーティングの設定」(P.50-12) (必須)
- 「Source-Specific Multicast の設定」(P.50-14)
- 「Source-Specific Multicast マッピングの設定」(P.50-17)
- 「PIM スタブ ルーティングの設定」(P.50-23) (任意)
- 「RP の設定」(P.50-25) (インターフェイスがスパース-デンス モードで、グループをスパースグループとして扱う場合に必須)
- 「自動 RP および BSR の使用法」(P.50-35) (他社製の PIMv2 デバイスをシスコ製 PIMv1 デバイスと相互運用する場合に必須)
- 「RP マッピング情報のモニタ」(P.50-36) (任意)
- 「PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング」(P.50-36) (任意)

マルチキャスト ルーティングのデフォルト設定

表 50-2 に、マルチキャスト ルーティングのデフォルト設定を示します。

表 50-2 マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル

表 50-2 マルチキャスト ルーティングのデフォルト設定 (続き)

機能	デフォルト設定
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

マルチキャスト ルーティング設定時の注意事項

スイッチ上でのマルチキャスト ルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

- 「PIMv1 および PIMv2 の相互運用性」(P.50-11)
- 「自動 RP および BSR 設定時の注意事項」(P.50-12)

PIMv1 および PIMv2 の相互運用性

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合があります。

PIMv2 に差別的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。したがって、PIMv2 の使用を推奨します。BSR メカニズムは、Cisco ルータおよびマルチレイヤ スイッチ上の自動 RP と相互運用します。詳細については、「自動 RP および BSR 設定時の注意事項」(P.50-12) を参照してください。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への変換を簡単に行うための推奨事項は次のとおりです。

- 領域全体で自動 RP を使用します。

- 領域全体で SM-DM を設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。詳細については、「[自動 RP の設定](#)」(P.50-27) を参照してください。

自動 RP および BSR 設定時の注意事項

PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- 使用しているネットワークがすべて Cisco ルータおよびマルチレイヤ スイッチである場合は、自動 RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- Cisco PIMv1 および PIMv2 ルータとマルチレイヤ スイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤ スイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤ スイッチだけが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤ スイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。詳細については、「[自動 RP および BSR の使用法](#)」(P.50-35) を参照してください。

基本的なマルチキャスト ルーティングの設定

IP マルチキャスト ルーティングをイネーブルにし、PIM バージョンおよび PIM モードを設定する必要があります。これにより、ソフトウェアはマルチキャスト パケットを転送し、スイッチがそのマルチキャスト ルーティング テーブルを読み込むことができます。

インターフェイスは PIM DM、SM、または SM-DM のいずれかに設定できます。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。IP マルチキャスト ルーティングを実行するには、インターフェイスに対して、これらの PIM モードのいずれかをイネーブルにする必要があります。インターフェイスで PIM をイネーブルにすると、同じインターフェイス上で IGMP 処理もイネーブルになります。



(注)

複数のインターフェイスで PIM をイネーブルにした場合、そのほとんどのインターフェイスが発信インターフェイス リストになく、IGMP スヌーピングがディセーブルであると、余分なレプリケーションのために発信インターフェイスでマルチキャスト トラフィックのラインレートを維持することができません。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。特定の送信元からのマルチキャスト トラフィックが十分であれば、レシーバの先頭ホップ ルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

デフォルトでは、マルチキャスト ルーティングはディセーブルとなっており、モードは設定されていません。この手順は必須です。

IP マルチキャストをイネーブルにし、PIM バージョンおよび PIM モードを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip multicast-routing distributed</code>	IP マルチキャストによる分散スイッチングをイネーブルにします。
ステップ 3	<code>interface interface-id</code>	<p>マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッド ポート : no switchport インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI : interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。詳細については、「レイヤ 3 インターフェイスの設定」(P.14-22)を参照してください。</p>
ステップ 4	<code>ip pim version [1 2]</code>	<p>インターフェイスに PIM バージョンを設定します。</p> <p>デフォルトでは、バージョン 2 がイネーブルです (推奨設定)。</p> <p>PIMv2 モードのインターフェイスに PIMv1 ネイバーが存在する場合、インターフェイスは自動的に PIMv1 モードにダウングレードされます。バージョン 1 のすべてのネイバーがシャットダウンするかアップグレードされると、インターフェイスはバージョン 2 モードに戻ります。</p> <p>詳細については、「PIMv1 および PIMv2 の相互運用性」(P.50-11)を参照してください。</p>
ステップ 5	<code>ip pim {dense-mode sparse-mode sparse-dense-mode}</code>	<p>インターフェイスで PIM モードをイネーブルにします。</p> <p>デフォルトで、モードは設定されていません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • dense-mode : DM 動作をイネーブルにします。 • sparse-mode : SM 動作をイネーブルにします。SM を設定する場合は、RP も設定する必要があります。詳細については、「RP の設定」(P.50-25)を参照してください。 • sparse-dense-mode : グループが属するモードでインターフェイスが処理されます。DM-SM 設定を推奨します。

	コマンド	目的
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャストルーティングをディセーブルにするには、**no ip multicast-routing distributed** グローバル コンフィギュレーション コマンドを使用します。デフォルトの PIM バージョンに戻すには、**no ip pim version** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで PIM をディセーブルにするには、**no ip pim** インターフェイス コンフィギュレーション コマンドを使用します。

Source-Specific Multicast の設定

ここでは、Source-Specific Multicast (SSM) の設定方法を説明します。ここで説明する SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」の章を参照してください。この章で言及する他のコマンドについては、コマンドリファレンス マスター インデックス (オンライン検索) を使用して、該当するマニュアルを参照してください。

SSM は IP マルチキャストの拡張機能です。この機能を使用すると、レシーバーに転送されるデータグラム トラフィックは、そのレシーバーが明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー (共有ツリーはない) だけが作成されます。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション (ブロードキャスト アプリケーション) に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキング テクノロジーです。このスイッチは次の SSM 対応コンポーネントをサポートしています。

- Protocol Independent Multicast Source-Specific Mode (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode (PIM-SM) に基づいています。

- Internet Group Management Protocol version 3 (IGMPv3)

IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートする必要があります。

Internet Standard Multicast と SSM の違い

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol (MSDP) に基づいています。これらのプロトコルには、Internet Standard Multicast (ISM) サービス モデルの限界があります。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信でなりたっています。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス **S** と IP 宛先アドレスとしてのマルチキャスト グループアドレス **G** のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。

ホスト グループのメンバーシップに必要なのは、IGMP version 1、2、または 3 によるホスト グループへのシグナリングだけです。SSM では、データグラムは (S, G) チャンネルに基づいて配信されます。SSM と ISM のいずれも、送信元になるのにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために (S, G) への加入または脱退を行う必要があります。つまり、レシーバーは加入した (S, G) チャンネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャンネル加入シグナリングの標準的な方法として、IGMP include モードメンバーシップ レポートの使用が提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ~ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なプロトコル (MSDP、自動 RP、Bootstrap Router (BSR; ブートストラップ ルータ) など) がすべて揃っていないネットワークでも、SSM を単独で導入できます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセス コントロール設定が必要になる場合もあります。

SSM を設定しイネーブルにするには、`ip pim ssm` グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モードメンバーシップ レポートを通じて、(S, G) チャンネルに加入できます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM (S, G) の join と prune のメッセージだけであり、(S, G) の Rendezvous Point Tree (RPT) や (*, G) の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます (SSM をサポートしていない場合など)。
- SSM 範囲内の Source-Active (SA) メッセージは、受け入れ、生成、転送のいずれも実行されません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストはマルチキャストグループのラストホップ ルータにメンバーシップ シグナルを送信します。ホストは、グループ メンバーシップ シグナルの送信に、送信元に関するフィルタリング機能を使用できます。ホストは、いくつかの特定の送信元を除くすべての送信元からグループへのトラフィックを受信する (**exclude** モード) というシグナルか、または、いくつかの特定の送信元からグループへのトラフィックだけを受信する (**include** モード) というシグナルを送信できます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、**exclude** と **include** の両方のモードのレポートを適用できます。SSM では、ラストホップ ルータは **include** モードのレポートだけを受け入れます。**exclude** モードのレポートは無視されます。

設定時の注意事項

ここでは、SSM を設定する際の注意事項について説明します。

SSM 範囲のレガシー アプリケーションに関する制約

SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、(S, G) チャネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。

アドレス管理に関する制約

SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol (CGMP)、IGMP スヌーピング、または Router-Port Group Management Protocol (RGMP) でサポートされるのはグループ固有のフィルタリングだけであり、(S, G) チャネル固有のフィルタリングはサポートされていません。同じスイッチド ネットワーク内の異なるレシーバーが異なる (S, G) チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての (S, G) チャネルトラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループアドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV (S, G) チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバーが接続されていても、レイヤ 2 スイッチを含むネットワークでトラフィック エイリアシングが発生しなくなります。

IGMP スヌーピングおよび CGMP の制限

IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング スイッチでは正しく認識されない場合があります。

IGMP (特に CGMP) に関連したスイッチング問題の詳細については、「[IGMP の概要](#)」(P.50-3) を参照してください。

ステート管理の制限事項

PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な (S, G) 加入登録があると、定期的に (S, G) join メッセージを送信します。そのため、レシーバーが (S, G) 加入メッセージを送信する限り、送信元から長時間（またはまったく）トラフィックが送信されなくても、レシーバーから送信元への Shortest Path Tree (SPT; 最短パスツリー) ステートは維持されます。

これは、送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ (S, G) ステートが維持される PIM-SM とは対照的です。PIM-SM では、送信元がトラフィックの送信を 3 分間停止すると、(S, G) ステートは削除され、再確立されるのは、その送信元からのパケットが RPT を通じて再度到達した場合だけです。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが (S, G) チャンネルの受信を要求している限り、(S, G) ステートを維持する必要があります。

SSM の設定

SSM を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>ip pim ssm [default range access-list]</code>	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 2	<code>interface type number</code>	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim {sparse-mode sparse-dense-mode}</code>	インターフェイスの PIM をイネーブルにします。sparse mode と sparse-dense mode のどちらかを使用する必要があります。
ステップ 4	<code>ip igmp version 3</code>	このインターフェイスに対して IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM のモニタリング

SSM をモニタするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
<code>show ip igmp groups detail</code>	IGMPv3 による (S, G) チャンネル加入登録を表示します。
<code>show ip mroute</code>	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

Source-Specific Multicast マッピングの設定

Source Specific Multicast (SSM) マッピング機能は、管理上または技術上の理由からエンドシステムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

ここで説明する内容は次のとおりです。

- 「設定時の注意事項」 (P.50-18)
- 「SSM マッピングの概要」 (P.50-18)
- 「SSM マッピングの設定」 (P.50-20)
- 「SSM マッピングのモニタリング」 (P.50-23)

設定時の注意事項

SSM マッピング設定時の注意事項を次に示します。

- SSM マッピングを設定する前に、IP マルチキャスト ルーティングをイネーブルにし、PIM スパース モードをイネーブルにして、SSM を設定します。IP マルチキャスト ルーティングおよび PIM スパース モードのイネーブル化については、「マルチキャスト ルーティングのデフォルト設定」 (P.50-10) を参照してください。
- スタティック SSM マッピングを設定する場合は、事前に Access Control List (ACL; アクセス コントロール リスト) を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。ACL の設定の詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- SSM マッピングと DNS ルックアップを設定し使用するには、稼働中の DNS サーバにレコードを追加できなければなりません。稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

Cisco Network Registra (CNR; Cisco ネットワーク レジストラ) などの製品が使用できます。詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml>

SSM マッピングには次のような制約があります。

- SSM マッピング機能では、SSM の利点をすべて得られるわけではありません。SSM マッピング機能では、ホストからグループ加入を得て、このグループを 1 つ以上の送信元に関連付けられたアプリケーションと関連付けるので、サポートできるアプリケーションは各グループに 1 つだけです。複数の完全な SSM アプリケーションが SSM マッピング内の同じグループを共有できます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている (SSM はサポートしていない) ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM マッピングの概要

典型的な STB 配置では、各 TV チャンネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャンネルの送信を行うアクティブなサーバは 1 つです。1 つのサーバから複数の TV チャンネルへの送信は可能ですが、各チャンネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は、そのマルチキャスト グループに関連付けられている TV チャンネルの well-known TV サーバになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャンネル メンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、そのグループに 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップ レポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップ レポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

SSM マッピングの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

スタティック SSM マッピング

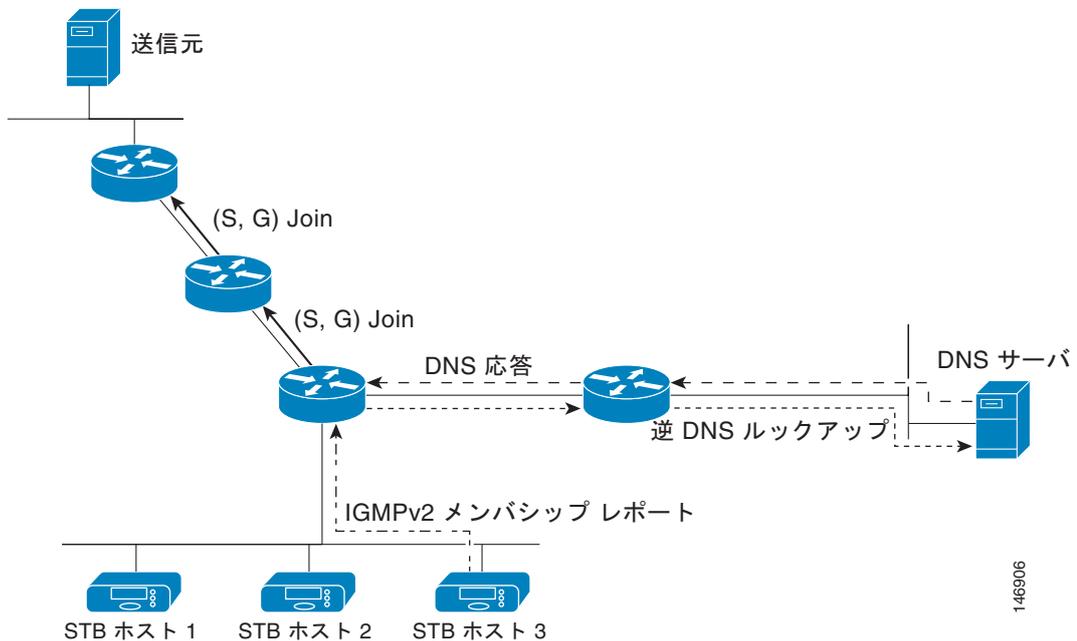
スタティック SSM マッピングでは、ラストホップ ルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。その後、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングできます。

DNS が必要とされないか、またはローカルで DNS マッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、ラストホップ ルータが継続的に逆 DNS ルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNS ベースの SSM マッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータは IP アドレス リソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSM マッピングでサポートできる送信元の数は、グループごとに最大 20 です。ルータは各グループに設定されているすべての送信元に加入します (図 50-4 を参照)。

図 50-4 DNS ベースの SSM マッピング



ラストホップルータが1つのグループの複数の送信元に参加できるようにする SSM マッピングメカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップルータは、SSM マッピングを使用し、同じ TV チャンネルに対して2つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップルータでのビデオトラフィックの重複を防ぐため、ビデオ送信元がサーバ側でスイッチオーバーメカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、その TV チャンネルにビデオトラフィックを送信します。サーバ側のスイッチオーバーメカニズムによって、実際にその TV チャンネルにビデオトラフィックを送信するサーバは1つだけになります。

G1、G2、G3、G4 を含むグループの1つ以上の送信元アドレスを検索するには、DNS サーバに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout]IN A source-address-1
IN A source-address-2
IN A source-address-n
```

DNS リソースレコードの詳細については、DNS サーバのマニュアルを参照してください。SSM マッピングの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」(P.50-21) (必須)
- 「DNS ベースの SSM マッピングの設定」(P.50-21) (必須)
- 「SSM マッピングを使用したスタティックトラフィック転送の設定」(P.50-22) (任意)

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip igmp ssm-map enable</code>	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。 (注) デフォルトでは、このコマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ3	<code>no ip igmp ssm-map query dns</code>	(任意) DNS ベースの SSM マッピングをディセーブルにします。 (注) スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、 <code>ip igmp ssm-map</code> グローバル コンフィギュレーション コマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ4	<code>ip igmp ssm-map static access-list source-address</code>	スタティック SSM マッピングを設定します。 <i>access-list</i> に入力した ACL によって、 <i>source-address</i> に入力した送信元 IP アドレスにマッピングされるグループが決まります。 (注) 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、スイッチは、設定されている各 <code>ip igmp ssm-map static</code> コマンドを使用して、そのグループに関連付けられている送信元アドレスを決定します。スイッチは各グループに最大 20 の送信元を関連付けます。
ステップ5	必要な場合は、ステップ 4 を繰り返して、追加のスタティック SSM マッピングを設定します。	—
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show running-config</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定例については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

DNS ベースの SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp ssm-map enable</code>	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。
ステップ 3	<code>ip igmp ssm-map query dns</code>	(任意) DNS ベースの SSM マッピングをイネーブルにします。 デフォルトでは、 <code>ip igmp ssm-map</code> コマンドによって DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドを no 形式で使用した場合だけです。 (注) DNS ベースの SSM マッピングがディセーブルになっている場合、このコマンドを使用すると、DNS ベースの SSM マッピングが再度イネーブルになります。
ステップ 4	<code>ip domain multicast domain-prefix</code>	(任意) スイッチが DNS ベースの SSM マッピングに使用するドメインプレフィックスを変更します。 デフォルトでは、スイッチは <code>ip-addr.arpa</code> ドメインプレフィックスを使用します。
ステップ 5	<code>ip name-server server-address1</code> [<code>server-address2... server-address6</code>]	1 つまたは複数のネームサーバのアドレスを指定して、名前およびアドレスの解決に使用します。
ステップ 6	必要な場合は、ステップ 5 を反復し、追加の DNS サーバを設定して冗長構成にします。	—
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングを使用したスタティック トラフィック転送の設定

SSM マッピングを使用したスタティック トラフィック転送によって、特定グループに SSM トラフィックをスタティックに転送できます。

SSM マッピングによるスタティック トラフィック転送を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface type number</code>	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 (注) SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。

コマンド	目的
ステップ3 ip igmp static-group <i>group-address</i> source ssm-map	そのインターフェイスから (S, G) チャンネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャンネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ4 show running-config	設定を確認します。
ステップ5 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

SSM マッピングのモニタリング

SSM マッピングを監視するには、表 50-3 の特権 ECEC コマンドを使用します。

表 50-3 SSM マッピングのモニタリングに使用するコマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングについての情報を表示します。
show ip igmp ssm-mapping <i>group-address</i>	SSM マッピングが特定のグループに使用する送信元を表示します。
show ip igmp groups [<i>group-name</i> <i>group-address</i> <i>interface-type interface-number</i>] [<i>detail</i>]	ルータに直接接続されているレシーバーおよび IGMP によって取得されたレシーバーのマルチキャスト グループを表示します。
show host	デフォルトのドメイン名、名前検索サービスの方式、サーバホスト名のリスト、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
debug ip igmp <i>group-address</i>	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM マッピング モニタリングの例については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html#wp1047772

PIM スタブルーティングの設定

PIM スタブルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは IGMP トラフィックだけです。

PIM スタブルーティングの設定時の注意事項

インターフェイスで PIM スタブルーティングをイネーブルにするときは、次の注意事項に従ってください。

- PIM スタブ ルーティングを設定する前に、スタブ ルータと中央のルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。さらに、スタブ ルータのアップリンク インターフェイスに PIM モード (dense-mode、sparse-mode、または dense-sparse-mode が設定されている必要があります)。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト (EIGRP) スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」(P.41-42) を参照してください。
- 直接接続されたマルチキャスト (IGMP) レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip pim passive	インターフェイスに PIM スタブ機能を設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip pim interface	各インターフェイスでイネーブルになっている PIM スタブを表示します。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、**no ip pim passive** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています (**sparse-dense-mode** がイネーブル)。図 50-2 では、VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet1/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
```

```
Switch(config)# interface GigabitEthernet1/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

各インターフェイスの PIM スタブがイネーブルになっていることを確認するには、**show ip pim interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet1/25 v2/SD 1 30 1 3.1.1.2

100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet1/20 v2/P 0 30 1 10.1.1.1
```

これらの特権 EXEC コマンドを使用すると、PIM スタブの設定およびステータスについての情報が表示されます。

- **show ip pim interface** では、各インターフェイスでイネーブルになっている PIM スタブが表示されます。
- **show ip igmp detail** では、特定のマルチキャスト送信元グループに参加した対象クライアントが表示されます。
- **show ip igmp mroute** では、送信元から対象クライアントへマルチキャスト ストリームが転送されることを確認できます。

RP の設定

インターフェイスが SM-DM で、グループをスパース グループとして扱う場合には、RP を設定する必要があります。ここに記載するいくつかの方法を使用できます。

- 「[マルチキャスト グループへの RP の手動割り当て](#)」(P.50-25)
- 「[自動 RP の設定](#)」(P.50-27) (PIMv1 から独立した、スタンドアロンのシスコ独自のプロトコル)
- 「[PIMv2 BSR の設定](#)」(P.50-31) (IETF 標準のトラッキング プロトコル)

動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。詳細については、「[PIMv1 および PIMv2 の相互運用性](#)」(P.50-11) および「[自動 RP および BSR 設定時の注意事項](#)」(P.50-12) を参照してください。

マルチキャスト グループへの RP の手動割り当て

ここでは、RP を手動で割り当てる方法について説明します。ダイナミック メカニズム (自動 RP や BSR など) を使用してグループの RP を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップルータ (指定ルータ) から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「合流地点」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチは PIM DM 技術を使用し、グループをデンスとして処理します。

RP のアドレスを手動で設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip pim rp-address ip-address [access-list-number] [override]</code>	<p>PIM RP のアドレスを設定します。</p> <p>デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ スイッチ (RP を含む) で、RP の IP アドレスを設定する必要があります。グループに RP が設定されていない場合、スイッチは PIM DM 技術を使用し、グループをデンスとして処理します。</p> <p>1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。</p> <ul style="list-style-type: none"> <code>ip-address</code> には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 (任意) <code>access-list-number</code> を指定する場合は、1 ~ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 (任意) <code>override</code> キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、RP が使用されるマルチキャスト グループのアドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RP アドレスを削除するには、`no ip pim rp-address ip-address [access-list-number] [override]` グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 225.2.2.2 の場合だけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

自動 RP の設定

自動 RP は IP マルチキャストを使用し、グループ/RP マッピングを PIM ネットワーク内のすべての Cisco ルータおよびマルチレイヤ スイッチに自動配信します。自動 RP には次の利点があります。

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ スイッチで矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

自動 RP を設定するときには、次の注意事項に従ってください。

- PIM を SM または SM-DM に設定し、自動 RP を設定しない場合は、RP を手動で設定する必要があります（「マルチキャスト グループへの RP の手動割り当て」(P.50-25) を参照）。
- ルーテッドインターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッドインターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが自動 RP グループの手動 RP アドレスを使用して設定されていなくても、自動 RP は引き続き使用できます。

ここでは、自動 RP を設定する方法について説明します。

- 「新規インターネットワークでの自動 RP の設定」(P.50-27) (任意)
- 「既存の SM クラウドへの自動 RP の追加」(P.50-27) (任意)
- 「問題のある RP への Join メッセージの送信禁止」(P.50-29) (任意)
- 「着信 RP アナウンスメント メッセージのフィルタリング」(P.50-30) (任意)

概要については、「自動 RP」(P.50-7) を参照してください。

新規インターネットワークでの自動 RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。「既存の SM クラウドへの自動 RP の追加」(P.50-27) に記載された手順に従ってください。ただし、PIM ルータをローカル グループの RP として設定する場合は、ステップ 3 を省略してください。

既存の SM クラウドへの自動 RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

既存の SM クラウドに自動 RP を導入するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 show running-config	<p>すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、ip pim rp-address グローバル コンフィギュレーション コマンドによって設定済みです。</p> <p>SM-DM 環境の場合、このステップは不要です。</p> <p>選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ (224.x.x.x やその他のグローバル グループなど) に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番目の RP を使用することもできます。</p>
ステップ 2 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3 ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds	<p>別の PIM デバイスをローカル グループの候補 RP として設定します。</p> <ul style="list-style-type: none"> interface-id には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 scope ttl には、ホップの TTL 値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。有効値は 1 ~ 255 です。 group-list access-list-number を指定する場合は、1 ~ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 interval seconds には、アナウンスメント メッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ~ 16383 です。
ステップ 4 access-list access-list-number {deny permit} source [source-wildcard]	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> access-list-number には、ステップ 3 で指定したアクセス リスト番号を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 source には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>

コマンド	目的
ステップ5 ip pim send-rp-discovery scope ttl	接続が中断される可能性がないスイッチを検索し、RP マッピング エージェントの役割を割り当てます。 scope ttl には、ホップの TTL 値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。有効値は 1 ~ 255 です。
ステップ6 end	特権 EXEC モードに戻ります。
ステップ7 show running-config show ip pim rp mapping show ip pim rp	設定を確認します。 関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。 ルーティング テーブルに保管されている情報を表示します。
ステップ8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定された PIM デバイスを解除するには、**no ip pim send-rp-announce interface-id** グローバル コンフィギュレーション コマンドを使用します。RP マッピング エージェントとして設定されたスイッチを解除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセスリスト 5 には、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、あとでこの問題を解決できます。ルータまたはマルチレイヤ スイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。この手順は任意です。

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

着信 RP アナウンスメントメッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

着信 RP アナウンスメントメッセージをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip pim rp-announce-filter rp-list access-list-number group-list access-list-number</code>	<p>着信 RP アナウンスメントメッセージをフィルタリングします。</p> <p>ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメントメッセージがデフォルトで許可されます。</p> <p><code>rp-list access-list-number</code> を指定する場合は、候補 RP アドレスのアクセス リストを設定します。アクセス リストが許可されている場合は、<code>group-list access-list-number</code> 変数で指定されたグループ範囲に対してアクセス リストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。</p> <p>複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピング エージェント間でフィルタを統一する必要があります。</p>
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント (<code>rp-list Access Control List (ACL; アクセス コントロール リスト)</code>) がマッピング エージェントによって許可されるかを指定するアクセス リストを作成します。 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト (グループリスト ACL) を作成します。 <code>source</code> には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

着信 RP アナウンスメント メッセージに関するフィルタを削除するには、**no ip pim rp-announce-filter rp-list access-list-number [group-list access-list-number]** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

この例では、マッピング エージェントは 2 つのデバイス (172.16.5.1 および 172.16.2.1) からの候補 RP アナウンスメントだけを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ~ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。マッピング エージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ~ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

PIMv2 BSR の設定

ここでは、PIMv2 ネットワークでの BSR の設定方法について説明します。

- 「PIM ドメイン境界の定義」(P.50-31) (任意)
- 「IP マルチキャスト境界の定義」(P.50-32) (任意)
- 「候補 BSR の設定」(P.50-33) (任意)
- 「候補 RP の設定」(P.50-34) (任意)

概要については、「BSR」(P.50-7) を参照してください。

PIM ドメイン境界の定義

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えてきました。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが共存し、間違ったドメイン内で RP が選択されたりします。

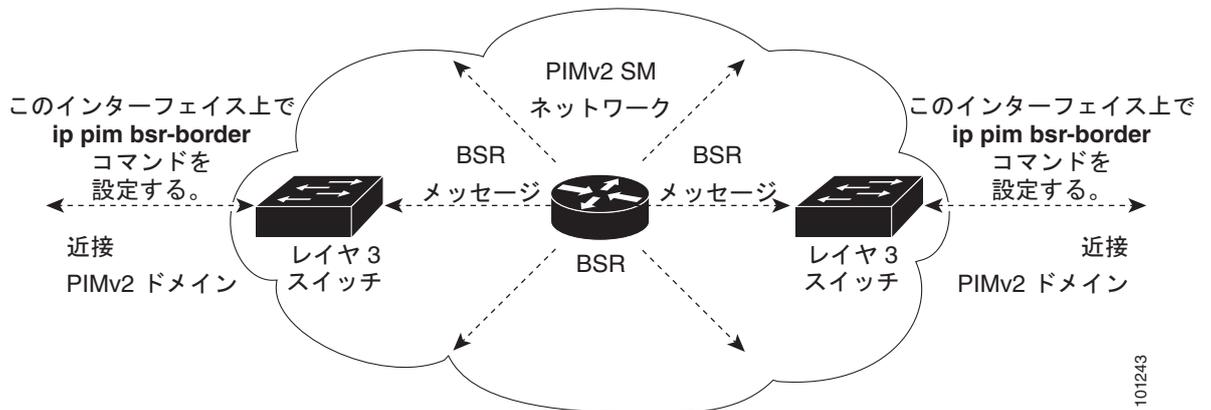
PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

コマンド	目的
ステップ3 ip pim bsr-border	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、スイッチは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます (図 50-5 を参照)。
ステップ4 end	特権 EXEC モードに戻ります。
ステップ5 show running-config	設定を確認します。
ステップ6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM 境界を削除するには、**no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。

図 50-5 PIMv2 BSR メッセージの抑制



IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

マルチキャスト境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	access-list access-list-number deny source [source-wildcard]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <i>access-list-number</i> の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。 <i>source</i> には、自動 RP 情報を伝達するマルチキャストアドレス 224.0.1.39 および 224.0.1.40 を入力します。 (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ3	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ip multicast boundary access-list-number	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip multicast boundary 1
```

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

スイッチを候補 BSR として設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip pim bsr-candidate interface-id hash-mask-length [priority]	候補 BSR となるようにスイッチを設定します。 <ul style="list-style-type: none"> <i>interface-id</i> には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となる、スイッチ上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポートチャンネル、VLAN などです。 <i>hash-mask-length</i> には、ハッシュ機能呼び出す前に、グループアドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットだけが使用されます。 （任意）<i>priority</i> を指定する場合は、0 ~ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 BSR として設定されたデバイスを解除するには、**no ip pim bsr-candidate** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet0/2 30 10
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/2 30 10
```

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス空間全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されている Cisco ルータおよびマルチレイヤ スイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤ スイッチを RP として設定できます。

スイッチが自身を PIMv2 候補 RP として BSR にアドバタイズするよう設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip pim rp-candidate interface-id [group-list access-list-number]	候補 RP となるようにスイッチを設定します。 <ul style="list-style-type: none"> interface-id には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 (任意) group-list access-list-number を指定する場合は、1 ~ 99 の IP 標準アクセス リスト番号を入力します。group-list を指定しない場合は、スイッチがすべてのグループの候補 RP となります。
ステップ3	access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> access-list-number には、ステップ 2 で指定したアクセス リスト番号を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 source には、パケットの送信元であるネットワークまたはホストの番号を入力します。 (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show running-config	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定されたデバイスを解除するには、**no ip pim rp-candidate interface-id** グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet1/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

自動 RP および BSR の使用法

ネットワーク上のルータがすべてシスコ デバイスである (他のベンダー製のルータが存在しない) 場合には、BSR を設定する必要はありません。PIMv1 と PIMv2 が両方とも動作しているネットワークに、自動 RP を設定します。

シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 ルータまたはマルチレイヤ スイッチを、自動 RP マッピング エージェントと BSR の両方に設定してください。

BSR を 1 つまたは複数使用する必要がある場合は、次の推奨事項に従ってください。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。詳細については、「[自動 RP の設定](#)」(P.50-27) および「[候補 BSR の設定](#)」(P.50-33) を参照してください。
- グループプレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループプレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループプレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

グループ/RP マッピングの一貫性を確認するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>show ip pim rp [[group-name group-address] mapping]</code>	任意のシスコ デバイスに関して、使用可能な RP マッピングを表示します。 <ul style="list-style-type: none"> (任意) <code>group-name</code> を指定する場合は、RP を表示するグループの名前を指定します。 (任意) <code>group-address</code> を指定する場合は、RP を表示するグループのアドレスを指定します。 (任意) シスコ デバイスによって認識されている（設定されているか、自動 RP によって取得されている）すべてのグループ/RP マッピングを表示するには、<code>mapping</code> キーワードを使用します。
ステップ 2	<code>show ip pim rp-hash group</code>	PIMv2 ルータまたはマルチレイヤ スイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 <code>group</code> には、RP 情報を表示するグループ アドレスを入力します。

RP マッピング情報のモニタ

RP マッピング情報をモニタするには、特権 EXEC モードで次のコマンドを使用します。

- `show ip pim bsr` : 現在選択されている BSR の情報を表示します。
- `show ip pim rp-hash group` : 指定グループに選択されている RP を表示します。
- `show ip pim rp [group-name | group-address | mapping]` : スイッチが RP を学習する方法 (BSR 経由か、または自動 RP メカニズムによるか) を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題をデバッグするには、次の点を順にチェックします。

- `show ip pim rp-hash` 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
- DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します (この場合は、登録停止にตอบสนองし、カプセル化が解除されたデータ パケットをレジスタから転送します)。

高度な PIM 機能の設定

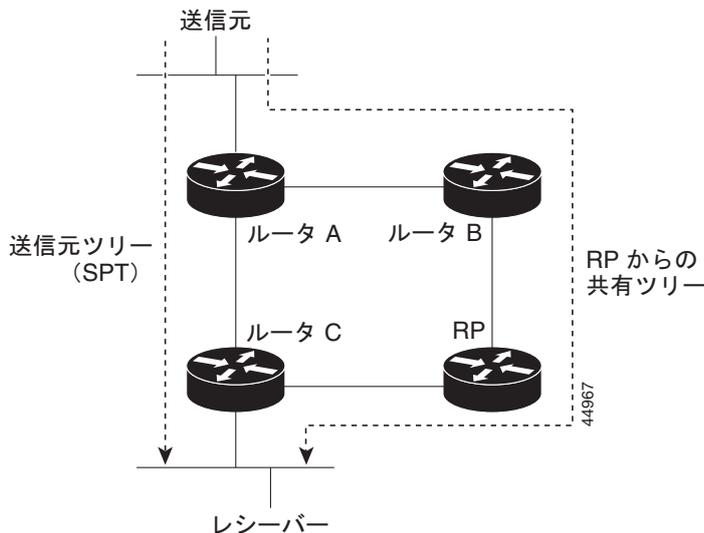
ここでは、高度なオプションの PIM 機能について説明します。

- 「PIM 共有ツリーおよび送信元ツリーの概要」(P.50-37)
- 「PIM SPT 使用の延期」(P.50-38) (任意)
- 「PIM ルータクエリー メッセージ インターバルの変更」(P.50-39) (任意)

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。図 50-6 に、このタイプの共有配信ツリーを示します。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 50-6 共有ツリーおよび送信元ツリー (SPT)



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ (ダウンストリーム接続がないルータ) で使用できます。このタイプの配信ツリーは、SPT または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバがグループに加入します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります (カプセル化されたデータ、およびネイティブ状態のデータ)。

5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は登録停止メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が Join メッセージを送信元に送信するよう要求します。
7. (S,G) に関するデータを受信すると、ルータ C は送信元宛てのプルーニング メッセージを共有ツリーの上方向に送信します。
8. RP は (S,G) の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けてプルーニング メッセージを送信します。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップ単位で送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。

共有ツリー上に存在するように、PIM デバイスを設定できます。詳細については、「[PIM SPT 使用の延期](#)」(P.50-38) を参照してください。

PIM SPT 使用の延期

最初のデータ パケットが最終ホップ ルータ (図 50-6 のルータ C) に着信すると、共有ツリーから送信元ツリーへと変更されます。この変更が生じるのは、`ip pim spt-threshold` グローバル コンフィギュレーション コマンドによってタイミングが制御されるためです。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度 (キロビット/秒) 以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー (SPT) を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、プルーニング メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト (標準アクセス リスト) を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

マルチキャスト ルーティングが送信元ツリーから SPT に切り替わる上限値となるトラフィック速度のしきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成します。 <ul style="list-style-type: none"> <code>access-list-number</code> の範囲は 1 ~ 99 です。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、しきい値が適用されるマルチキャスト グループを指定します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 3	<code>ip pim spt-threshold {kbps infinity} [group-list access-list-number]</code>	SPT に移行する上限値となるしきい値を指定します。 <ul style="list-style-type: none"> <code>kbps</code> を指定する場合は、トラフィック速度をキロビット/秒で指定します。デフォルト値は 0 kbps です。 <p>(注) 有効範囲は 0 ~ 4294967 ですが、スイッチ ハードウェアの制限により、0 kbps 以外は無効です。</p> <ul style="list-style-type: none"> <code>infinity</code> を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 (任意) <code>group-list access-list-number</code> を指定する場合は、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、または <code>group-list</code> を使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip pim spt-threshold {kbps | infinity}` グローバル コンフィギュレーション コマンドを使用します。

PIM ルータクエリー メッセージ インターバルの変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント (サブネット) の DR になるデバイスを判別するため、PIM ルータクエリー メッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM 登録メッセージを送信し、送信元からのマルチキャストトラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

ルータクエリーメッセージインターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	ip pim query-interval seconds	スイッチが PIM ルータクエリーメッセージを送信する頻度を設定します。 デフォルトは 30 秒です。指定できる範囲は 1 ~ 65535 です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show ip igmp interface [interface-id]	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip pim query-interval [seconds]** インターフェイス コンフィギュレーション コマンドを使用します。

オプションの IGMP 機能の設定

ここでは、次の設定について説明します。

- 「IGMP のデフォルト設定」(P.50-41)
- 「グループのメンバーとしてのスイッチの設定」(P.50-41) (任意)
- 「IP マルチキャスト グループへのアクセスの制御」(P.50-42) (任意)
- 「IGMP バージョンの変更」(P.50-43) (任意)
- 「IGMP ホストクエリーメッセージインターバルの変更」(P.50-43) (任意)
- 「IGMPv2 の IGMP クエリータイムアウトの変更」(P.50-44) (任意)
- 「IGMPv2 の最大クエリー応答時間の変更」(P.50-45) (任意)
- 「静的に接続されたメンバーとしてのスイッチの設定」(P.50-45) (任意)

IGMP のデフォルト設定

表 50-4 に、IGMP のデフォルト設定を示します。

表 50-4 IGMP のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバーとしてのマルチレイヤ スイッチ	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP のバージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ スイッチがマルチキャスト グループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された ICMP エコー要求 パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。



注意

この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

スイッチがグループのメンバーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip igmp join-group group-address</code>	マルチキャスト グループに加入するスイッチを設定します。 デフォルトで、グループのメンバーシップは定義されていません。 <code>group-address</code> には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

グループ内のメンバーシップを取り消すには、**no ip igmp join-group group-address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 255.2.2.2 へのスイッチの加入を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、スイッチは、マルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

インターフェイスで許可されるマルチキャスト グループをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp access-group access-list-number	インターフェイスで処理されるサブネット上のホストが加入できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 <i>access-list-number</i> には、IP 標準アドレス アクセス リスト番号を指定します。指定できる範囲は 1 ~ 99 です。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成します。 <ul style="list-style-type: none"> <i>access-list-number</i> には、ステップ 3 で作成したアクセス リストを指定します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>source</i> には、サブネット上のホストが加入できるマルチキャスト グループを指定します。 (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip igmp interface [interface-id]	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスでグループをディセーブルにするには、**no ip igmp access-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに接続されたホストが、グループ 255.2.2.2 にだけ加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

IGMP バージョンを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp version {1 2}	スイッチで使用する IGMP バージョンを指定します。 (注) バージョン 1 に変更すると、 ip igmp query-interval または ip igmp query-max-response-time インターフェイス コンフィギュレーション コマンドを設定できません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip igmp version** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは、IGMP ホストクエリー メッセージを定期的送信し、接続されたネットワーク上にあるマルチキャスト グループを検出します。これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ (224.0.0.1) に送信されます。スイッチはホストクエリー メッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、プルーニング メッセージが送信元のアップストリーム方向へ送信されます。

■ オプションの IGMP 機能の設定

スイッチは LAN (サブネット) 用の PIM DR を選択します。DR は、IP アドレスが最大である、IGMPv2 用のルータまたはマルチレイヤ スイッチです。IGMPv1 の場合、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。

ホストクエリー インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp query-interval seconds	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。指定できる範囲は 1 ~ 65535 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-interval** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、スイッチがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。デフォルトでは、スイッチは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー インターバルの 2 倍の時間だけ待機します。この時間を経過しても、スイッチがクエリーを受信しない場合は、スイッチがクエリアになります。

クエリー インターバルを設定するには、**show ip igmp interface interface-id** 特権 EXEC コマンドを入力します。

IGMP クエリー タイムアウトを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp querier-timeout seconds	IGMP クエリー タイムアウトを指定します。 デフォルトは 60 秒です (クエリー インターバルの 2 倍)。指定できる範囲は 60 ~ 300 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp querier-timeout** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。スイッチは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバーが存在しないことを短時間で検出します。値を小さくすると、グループのブルーニング速度が向上します。

最大クエリー応答時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp query-max-response-time seconds	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ~ 25 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを使用します。

静的に接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないにもかかわらず、そのネットワーク セグメントにマルチキャストトラフィックを送り込むことが必要な場合もあります。マルチキャストトラフィックをネットワーク セグメントに送り込む方法は次のとおりです。

- **ip igmp join-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはマルチキャストパケットの転送だけでなく、受信も行います。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。
- **ip igmp static-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはパケットそのものを受信せず、転送だけを実行します。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャストルート エントリに *L* (ローカル) フラグが付かないことから明らかなように、スイッチ自体はメンバーではありません。

静的に接続されたグループのメンバーになるように（および高速スイッチングできるように）スイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip igmp static-group group-address</code>	スイッチを静的に接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルになっています。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

グループのメンバーとして設定されたスイッチを解除するには、`no ip igmp static-group group-address` インターフェイス コンフィギュレーション コマンドを使用します。

オプションのマルチキャスト ルーティング機能の設定

ここでは、オプションのマルチキャスト ルーティング機能の設定方法について説明します。

- レイヤ 2 接続および MBONE マルチメディア会議セッションに関する機能と設定：
 - 「CGMP サーバ サポート機能のイネーブル化」(P.50-46) (任意)
 - 「sdr リスナー サポート機能の設定」(P.50-47) (任意)
- 帯域幅の利用率を制御する機能：
 - 「IP マルチキャスト境界の設定」(P.50-49) (任意)
- VPN Routing/Forwarding Table (VRF; VPN ルーティング/転送テーブル) にマルチキャストを設定する手順：
 - 「マルチキャスト VRF の設定」(P.41-80)

CGMP サーバ サポート機能のイネーブル化

スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれているデバイス用の CGMP サーバとして機能します。CGMP はレイヤ 2 Catalyst スwitch に接続された Cisco ルータおよびマルチレイヤ スwitch で使用され、IGMP で実行される作業と同様の作業を実行します。CGMP が必要となるのは、レイヤ 2 スwitch で IP マルチキャスト データ パケットと IGMP レポートメッセージを区別できないためです。これらはともに MAC レベルで、同じグループアドレスにアドレス指定されます。

スイッチ インターフェイスで CGMP サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	レイヤ 2 Catalyst スイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	ip cgmp [proxy]	<p>インターフェイス上で CGMP をイネーブルにします。</p> <p>デフォルトでは、CGMP はすべてのインターフェイス上でディセーブルです。</p> <p>CGMP をイネーブルにすると、CGMP Join メッセージが送信されます。レイヤ 2 Catalyst スイッチに接続されたレイヤ 3 インターフェイスでだけ、CGMP をイネーブルにします。</p> <p>(任意) proxy キーワードを入力すると、CGMP プロキシ機能がイネーブルになります。プロキシルータは、CGMP 非対応ルータの MAC アドレス、およびグループ アドレス 0000.0000.0000 が格納された CGMP Join メッセージを送信し、CGMP 非対応ルータが存在することをアドバタイズします。</p> <p>(注) CGMP プロキシを実行するには、スイッチを IGMP クエリアに設定する必要があります。 ip cgmp proxy コマンドを設定する場合は、ネットワークで動作中の IGMP のバージョンに応じて、IP アドレスが最大または最小のスイッチが IGMP クエリアになるように IP アドレスを手動で操作する必要があります。IGMP バージョン 2 クエリアは、インターフェイスの最小の IP アドレスに基づいて選択されます。IGMP バージョン 1 クエリアは、インターフェイスで使用されるマルチキャスト ルーティング プロトコルに基づいて選択されます。</p>
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show running-config	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ7		レイヤ 2 Catalyst スイッチ CGMP クライアントの設定を確認します。詳細については、製品に付属のマニュアルを参照してください。

インターフェイス上で CGMP をディセーブルにするには、**no ip cgmp** インターフェイス コンフィギュレーション コマンドを使用します。

複数のシスコ CGMP 対応デバイスがスイッチド ネットワークに接続されていて、**ip cgmp proxy** コマンドを使用する必要がある場合は、すべてのデバイスを同じ CGMP オプションを使用して設定し、他社製のルータよりも IGMP クエリアになる優先順位を上げてください。

sdr リスナー サポート機能の設定

MBONE は、相互接続された、IP マルチキャスト トラフィックの転送が可能なインターネット ルータ およびホストの小さなサブセットです。その他のマルチメディア コンテンツも、通常は MBONE を通してブロードキャストされます。マルチメディア セッションに加入する前に、このセッションで使用されているマルチメディア グループ アドレス、ポート、セッションがアクティブになる時期、およびワークステーションで必要となるアプリケーションの種類（音声、ビデオなど）を把握する必要があります。この情報は、MBONE Session Directory バージョン 2 (sdr) ツールによって提供されます。このフリーウェア アプリケーションは WWW 上の複数のサイト (<http://www.video.ja.net/mice/index.html> など) からダウンロードできます。

SDR は、Session Announcement Protocol (SAP) マルチキャスト パケット用の Well-known マルチキャスト グループ アドレスおよびポートを、SAP クライアントから傍受するマルチキャスト アプリケーションです (SAP クライアントは、会議セッションをアナウンスします)。これらの SAP パケットには、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループ アドレス、メディア形式、担当者、およびアドバタイズされたマルチメディア セッションに関するその他の情報が格納されます。SAP パケットの情報は、[SDR Session Announcement] ウィンドウに表示されます。

sdr リスナー サポート機能のイネーブル化

デフォルトでは、スイッチでセッション ディレクトリのアドバタイズメントは受信されません。

スイッチがインターフェイスのデフォルトのセッション ディレクトリ グループ (224.2.127.254) に加入し、セッション ディレクトリ アドバタイズメントを受信できるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	sdr に対してイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip sdr listen</code>	sdr リスナー サポート機能をイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

sdr サポート機能をディセーブルにするには、**no ip sdr listen** インターフェイス コンフィギュレーション コマンドを使用します。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュから削除されません。送信元が SAP 情報のアドバタイズを停止した場合に、古いアドバタイズメントが無駄に保持されないようにするため、エントリがアクティブである期間を制限できます。

sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip sdr cache-timeout minutes</code>	sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限します。 デフォルトでは、エントリはキャッシュから削除されません。 <i>minutes</i> に指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip sdr cache-timeout** グローバル コンフィギュレーション コマンドを使用します。キャッシュ全体を削除するには、**clear ip sdr** 特権 EXEC コマンドを使用します。

セッション ディレクトリ キャッシュを表示するには、**show ip sdr** 特権 EXEC コマンドを使用します。

IP マルチキャスト境界の設定

管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャスト アドレス範囲が境界のメカニズムとして使用されます。管理の有効範囲付き境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りすることができません。この結果、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

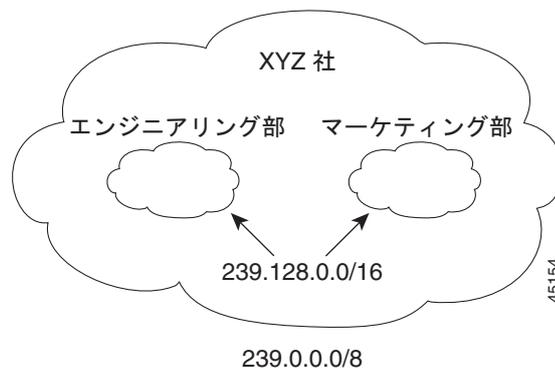


(注)

マルチキャスト境界および TTL しきい値は、マルチキャスト ドメインの有効範囲を制御しますが、TTL しきい値はこのスイッチでサポートされていません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 50-7 に、XYZ 社が自社ネットワーク周辺にあるすべてのルーテッド インターフェイス上で、管理用スコープの境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ~ 239.255.255.255 の範囲のマルチキャスト トラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ~ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ったり、外部に出ることができません。

図 50-7 管理用スコープの境界



マルチキャスト グループ アドレスに対して、ルーテッド インターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。この境界が定義されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。この境界を使用すると、異なる管理ドメイン内で同じマルチキャスト グループ アドレスを再利用できます。

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ~ 239.255.255.255 を管理用スコープのアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できません。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

管理用スコープの境界を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <code>access-list-number</code> の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 3	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>ip multicast boundary access-list-number</code>	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、`no ip multicast boundary` インターフェイス コンフィギュレーション コマンドを使用します。

次に、すべての管理用スコープのアドレスに対して境界を設定する例を示します。

```
Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip multicast boundary 1
```

基本的な DVMRP 相互運用性機能の設定

ここでは、次の設定について説明します。

- 「[DVMRP 相互運用性](#)の設定」(P.50-51) (任意)
- 「[DVMRP トンネル](#)の設定」(P.50-53) (任意)
- 「[DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ](#)」(P.50-55) (任意)
- 「[mrinfo 要求への応答](#)」(P.50-55) (任意)

高度な DVMRP 機能の詳細については、「[高度な DVMRP 相互運用性機能](#)の設定」(P.50-56) を参照してください。

DVMRP 相互運用性の設定

PIM を使用するシスコのマルチキャスト ルータおよびマルチレイヤ スイッチは、DVMRP を使用する他社製のマルチキャスト ルータと相互運用させることができます。

PIM デバイスは、DVMRP プローブ メッセージを受信し、接続されているネットワーク上にある DVMRP マルチキャスト ルータを動的に検出します。DVMRP ネイバーが検出された場合、PIM デバイスは、PIM ドメイン内の到達可能なユニキャスト送信元をアドバタイズする DVMRP レポート メッセージを定期的送信します。デフォルトでは、直接接続されたサブネットおよびネットワークがアドバタイズされます。デバイスは DVMRP ルータによって転送されたマルチキャスト パケットを転送し、次にマルチキャスト パケットを DVMRP ルータに転送します。

DVMRP ルート レポート内でアドバタイズされるユニキャスト ルート数を制限するには、MBONE に接続された PIM ルーテッド インターフェイスにアクセス リストを設定できます。この設定を行わないと、ユニキャスト ルーティング テーブル内のすべてのルートがアドバタイズされます。



(注)

マルチキャスト ルーティングされるプロトコルは、DVMRP のパブリックドメイン実装バージョンです。Cisco ルータおよびマルチレイヤ スイッチを DVMRP ルータに直接接続する場合、または MBONE トンネルを通して DVMRP ルータと相互運用する場合は、マルチキャスト ルーティングのバージョン 3.8 を使用する必要があります (バージョン 3.8 には、DVMRP の非プルーフバージョンが実装されています)。Cisco IOS ソフトウェアによって作成される DVMRP アドバタイズメントを使用すると、マルチキャスト ルーティングされた古いバージョンのプロトコルによってルーティング テーブルやネイバーのルーティング テーブルが破壊されることもあります。

アドバタイズされる送信元、および使用されるメトリックを設定する場合は、`ip dvmrp metric` インターフェイス コンフィギュレーション コマンドを設定します。特定のユニキャスト ルーティング プロセスによって取得されたすべての送信元を、DVMRP にアドバタイズするように指示することもできます。

DVMRP ルートレポート メッセージが送信される時に、アドバタイズされる送信元と使用されるメトリックを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> • <code>access-list-number</code> の範囲は 1 ~ 99 です。 • <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 • <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ 3	<code>interface interface-id</code>	MBONE に接続されている、マルチキャスト ルーティングが可能なインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>ip dvmrp metric metric [list access-list-number] [[protocol process-id] [dvmrp]]</code>	<p>DVMRP レポートの一連の宛先に関連付けられるメトリックを設定します。</p> <ul style="list-style-type: none"> • <i>metric</i> の範囲は、0 ~ 32 です。値が 0 の場合、ルートはアドバタイズされません。値 32 は無限大（到達不能）を意味します。 • (任意) <i>list access-list-number</i> を指定する場合は、ステップ 2 で作成したアクセス リスト番号を入力します。これらが指定されている場合は、アクセス リストと一致するマルチキャスト宛先だけが、設定されたメトリックとともにレポートされます。 • (任意) <i>protocol process-id</i> を指定する場合は、eigrp、igrp、ospf、rip、static、または dvmrp などのユニキャスト ルーティング プロトコルの名前、およびルーティング プロトコルのプロセス ID 番号を入力します。これらが指定されている場合は、指定されたルーティング プロトコルによって取得されたルートだけが、DVMRP レポート メッセージに格納されてアドバタイズされます。 • (任意) dvmrp キーワードが指定されている場合は、設定された <i>metric</i> を使用して DVMRP ルーティング テーブルのルートをアドバタイズしたり、フィルタリングできます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

メトリックまたはルート マップをディセーブルにするには、**no ip dvmrp metric metric [list access-list-number] [[protocol process-id] | [dvmrp]]** または **no ip dvmrp metric metric route-map map-name** インターフェイス コンフィギュレーション コマンドを使用します。

より詳細な方法で上記コマンドと同じ結果を得るには、アクセス リストの代わりに、ルート マップ (**ip dvmrp metric metric route-map map-name** インターフェイス コンフィギュレーション コマンド) を使用します。ユニキャスト ルートが DVMRP に入る前に、ルート マップ条件にユニキャスト ルートを適用します。

次に、PIM デバイスおよび DVMRP ルータが同じネットワーク セグメント上にある場合に、DVMRP 相互運用性を設定する例を示します。次の例では、アクセス リスト 1 はネットワーク (198.92.35.0、198.92.36.0、198.92.37.0、131.108.0.0、および 150.136.0.0) を DVMRP ルータにアドバタイズします。アクセス リスト 2 は他のすべてのネットワークのアドバタイズを禁止します (**ip dvmrp metric 0** インターフェイス コンフィギュレーション コマンド)。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.255.255
Switch(config)# access-list 1 deny 0.0.0.0 255.255.255.255
```

```
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP トンネルの設定

ソフトウェアは、MBONE への DVMRP トンネルをサポートします。一方の端で DVMRP が動作しているルータまたはマルチレイヤスイッチには、DVMRP トンネルを設定できます。これにより、トンネルを通してマルチキャストパケットが送受信されます。この方法で、パス上の一部のルータでマルチキャストルーティングがサポートされていない場合に、PIM ドメインを DVMRP ルータに接続できます。2 つのルータ間で DVMRP トンネルを設定できません。

Cisco ルータまたはマルチレイヤスイッチがトンネルを通して DVMRP を実行している場合は、DVMRP レポートメッセージ内の送信元が、実際のネットワークと同様にアドバタイズされます。また、受信された DVMRP レポートメッセージはキャッシュに格納され、RPF 計算にも使用されます。この動作により、トンネルを通して受信されたマルチキャストパケットの転送が可能になります。

次の場合は、DVMRP トンネルを設定するときに、IP アドレスをトンネルに割り当てる必要があります。

- トンネルを通して IP パケットを送信する場合
- DVMRP サマライズを実行するようにソフトウェアを設定する場合

トンネルとサブネットのネットワーク番号が異なる場合、サブネットはトンネルを通してアドバタイズされません。この場合は、ネットワーク番号だけがトンネルを通してアドバタイズされます。

DVMRP トンネルを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> • <code>access-list-number</code> の範囲は 1 ~ 99 です。 • <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 • <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 3	<code>interface tunnel number</code>	トンネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>tunnel source ip-address</code>	トンネル インターフェイスの送信元アドレスを指定します。スイッチのインターフェイスの IP アドレスを入力します。
ステップ 5	<code>tunnel destination ip-address</code>	トンネル インターフェイスの宛先アドレスを指定します。マルチキャストルーティングされたルータの IP アドレスを入力します。
ステップ 6	<code>tunnel mode dvmrp</code>	DVMRP へのトンネルに対してカプセル化モードを設定します。

	コマンド	目的
ステップ 7	ip address <i>address mask</i> または ip unnumbered <i>type number</i>	インターフェイスに IP アドレスを割り当てます。 または インターフェイスを番号なしとして設定します。
ステップ 8	ip pim [<i>dense-mode</i> <i>sparse-mode</i>]	インターフェイスに PIM モードを設定します。
ステップ 9	ip dvmrp accept-filter <i>access-list-number</i> [<i>distance</i>] neighbor-list <i>access-list-number</i>	着信 DVMRP レポートに対して許可フィルタを設定します。 デフォルトでは、距離が 0 のすべての宛先レポートが許可されます。したがって、すべてのネイバーからのレポートが許可されます。 <ul style="list-style-type: none">• <i>access-list-number</i> には、ステップ 2 で作成したアクセス リスト番号を指定します。アクセス リストに一致するすべての送信元は、距離とともに DVMRP ルーティング テーブルに格納されます。• (任意) <i>distance</i> を指定する場合は、宛先への管理上の距離を入力します。デフォルトでは、DVMRP ルートへの管理上の距離は 0 で、ユニキャスト ルーティング テーブル ルートよりも優先されます。ユニキャスト ルーティングによるパス (マルチキャスト ルーティング プロトコルとして PIM を使用) と DVMRP を使用するパスという、送信元への 2 つのパスがある場合に PIM パスを使用するときは、DVMRP ルートの管理上の距離を増加させます。有効値は 1 ~ 255 です。• neighbor-list <i>access-list-number</i> には、ステップ 2 で作成したネイバー リストの番号を入力します。DVMRP レポートは、リスト内のネイバーでだけ許可されます。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show running-config	設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタをディセーブルにするには、**no ip dvmrp accept-filter** *access-list-number* [*distance*] **neighbor-list** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用します。

次に、DVMRP トンネルを設定する例を示します。この設定では、Cisco スイッチ上のトンネルの IP アドレスに、*unnumbered* が割り当てられます。これにより、トンネルにはポート 1 と同じ IP アドレスが設定されます。トンネルのエンドポイント送信元 IP アドレスは 172.16.2.1 です。トンネルの接続先であるリモート DVMRP ルータのトンネルのエンドポイントアドレスは 192.168.1.10 です。トンネルを通して送信されるパケットは、外部 IP ヘッダー内にカプセル化されます。Cisco スイッチは、198.92.37.0 から 198.92.37.255 への距離が 100 である着信 DVMRP レポートを受信するように設定されます。

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet1/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ

使用しているスイッチがマルチキャスト ルーティング バージョン 3.6 のデバイスと隣接している場合は、ネットワーク 0.0.0.0 (デフォルト ルート) を DVMRP ネイバーにアドバタイズするように、ソフトウェアを設定できます。DVMRP デフォルト ルートでは、具体的なルートと一致しないマルチキャスト送信元の RPF 情報が計算されます。

DVMRP のデフォルト ルートを MBONE にアドバタイズしないでください。

インターフェイスの DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>ip dvmrp default-information {originate only}</code>	DVMRP ネイバーへのネットワーク 0.0.0.0 をアドバタイズします。 このコマンドは、スイッチがマルチキャスト ルーティング バージョン 3.6 のデバイスと近接している場合に限り使用します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • originate : 0.0.0.0 以外の具体的なルートもアドバタイズできます。 • only : 0.0.0.0 以外の DVMRP ルートはアドバタイズされません。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ルートのアドバタイズメントを禁止するには、`no ip dvmrp default-information` インターフェイス コンフィギュレーション コマンドを使用します。

mrinfo 要求への応答

ソフトウェアは、マルチキャスト ルーティングされたシステム、Cisco ルータ、およびマルチレイヤ スイッチによって送信された `mrinfo` 要求に応答します。ソフトウェアはネイバーに関する情報を、DVMRP トンネルおよびすべてのルーテッド インターフェイスを通して戻します。この情報にはメトリック (常に 1 に設定)、設定された TTL しきい値、インターフェイスのステータス、および各種フラグが含まれます。次の例のように、`mrinfo` 特権 EXEC コマンドを使用し、ルータまたはスイッチ自体をクエリーすることもできます。

```
Switch# mrinfo
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

高度な DVMRP 相互運用性機能の設定

Cisco ルータおよびマルチレイヤ スイッチは PIM を実行し、マルチキャスト パケットをレシーバーに転送したり、送信側から受信したりします。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。PIM はこの情報を使用しますが、Cisco ルータおよびマルチレイヤ スイッチでは、マルチキャスト パケットを転送するために DVMRP を実行しません。

ここでは、次の設定について説明します。

- 「DVMRP ユニキャスト ルーティングのイネーブル化」(P.50-56) (任意)
- 「DVMRP の非ブルーニング ネイバーの拒否」(P.50-57) (任意)
- 「ルート交換の制御」(P.50-59) (任意)

基本的な DVMRP 機能の詳細については、「基本的な DVMRP 相互運用性機能の設定」(P.50-50) を参照してください。

DVMRP ユニキャスト ルーティングのイネーブル化

マルチキャスト ルーティングおよびユニキャスト ルーティングには個別のトポロジが必要となるため、PIM はマルチキャスト トポロジに従って、ループのない配信ツリーを構築する必要があります。Cisco ルータ、マルチレイヤ スイッチ、およびマルチキャスト ルーティング ベースのデバイスは、DVMRP ユニキャスト ルーティングを使用して、DVMRP ユニキャスト ルートを交換します。PIM はこれらのルートに逆経路を転送できます。

シスコ デバイスは DVMRP マルチキャスト ルーティングを相互に実行しませんが、DVMRP ルートを交換します。DVMRP ルートは、ユニキャスト トポロジと異なるマルチキャスト トポロジを提供します。このため、マルチキャスト トポロジを通して PIM を実行し、この結果 MBONE トポロジを通しての PIM SM が可能になります。

DVMRP ユニキャスト ルーティングがイネーブルの場合、ルータまたはスイッチは、DVMRP ルーティング テーブル内の DVMRP レポート メッセージで取得されたルートをキャッシュに格納します。PIM が動作中の場合、これらのルートはユニキャスト ルーティング テーブル内のルートよりも優先されます。したがって、MBONE トポロジがユニキャスト トポロジと異なる場合、PIM による MBONE トポロジが可能となります。

DVMRP ユニキャスト ルーティングは、すべてのインターフェイスで実行できます。DVMRP トンネルの場合は、DVMRP マルチキャスト ルーティングが使用されます。この機能を使用しても、Cisco ルータおよびマルチレイヤ スイッチ間で DVMRP マルチキャスト ルーティングはイネーブルになりません。ただし、DVMRP 対応マルチキャスト ルータがある場合は、シスコ デバイスで PIM/DVMRP マルチキャスト ルーティングを実行できます。

DVMRP ユニキャスト ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip dvmrp unicast-routing</code>	DVMRP ユニキャスト ルーティングをイネーブルにします (DVMRP ルートを送受信します)。この機能は、デフォルトではディセーブルになっています。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

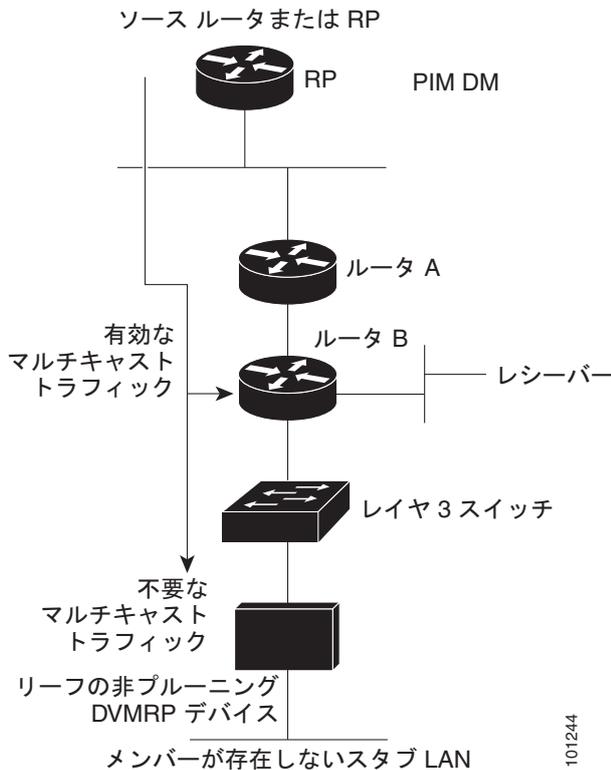
	コマンド	目的
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、`no ip dvmrp unicast-routing` インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP の非プルーニング ネイバーの拒否

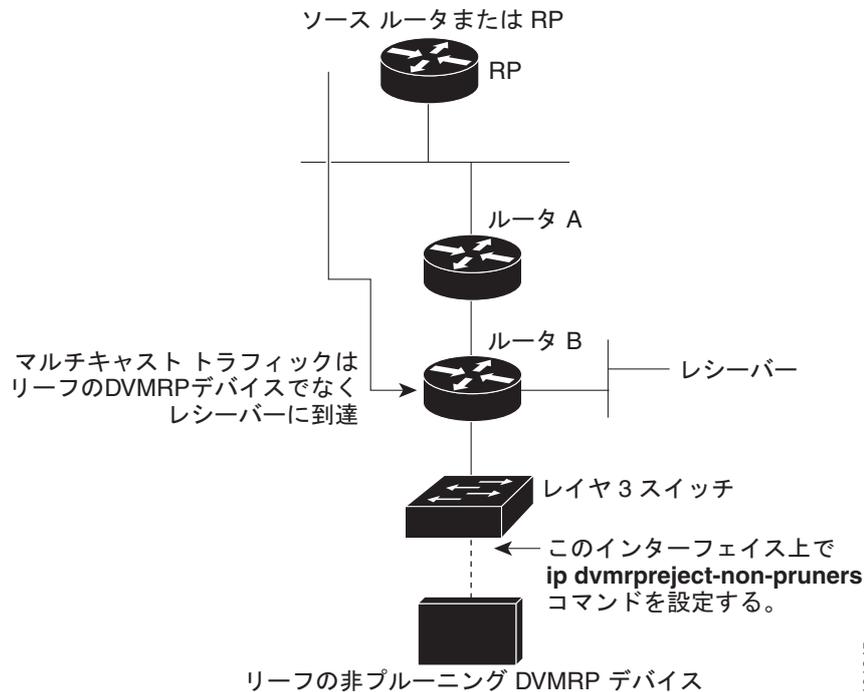
デフォルトでは、DVMRP 機能に関係なく、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の他社製のデバイスでは、プルーニング機能を持たない古いバージョンの DVMRP が動作するため、常時転送パケットが受信されて帯域幅が消費されます。図 50-8 にこの事例を示します。

図 50-8 リーフの非プルーニング DVMRP ネイバー



DVMRP ネイバーで DVMRP プルーニングまたは接合がサポートされていない場合、スイッチとこのネイバーとのピアリング (通信) を禁止できます。これを行うには、非プルーニング デバイスに接続されたインターフェイスで `ip dvmrp reject-non-pruners` インターフェイス コンフィギュレーション コマンドを使用し、スイッチ (リーフの非プルーニング DVMRP デバイスのネイバー) を設定します (図 50-9 を参照)。この場合、プルーニング対応フラグが設定されていない DVMRP プロローブまたはレポート メッセージをスイッチが受信すると、Syslog メッセージがロギングされ、メッセージが廃棄されます。

図 50-9 ルータが非ブルーニング DVMRP ネイバーを拒否する例



ip dvmrp reject-non-pruners インターフェイス コンフィギュレーション コマンドを使用すると、ネイバーとのピアリングだけが禁止されます。拒否されていない非ブルーニング ルータが（レシーバー候補のダウンストリーム方向に）2 ホップ以上離れている場合、非ブルーニング DVMRP ネットワークが存在する場合があります。

非ブルーニング DVMRP ネイバーとのピアリングを禁止するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 interface interface-id	非ブルーニング DVMRP ネイバーに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3 ip dvmrp reject-non-pruners	非ブルーニング DVMRP ネイバーとのピアリングを禁止します。
ステップ4 end	特権 EXEC モードに戻ります。
ステップ5 show running-config	設定を確認します。
ステップ6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip dvmrp reject-non-pruners** インターフェイス コンフィギュレーション コマンドを使用します。

ルート交換の制御

ここでは、DVMRP ルートに関するシスコ デバイスのアドバタイズメントを調整する方法について説明します。

- 「アドバタイズされる DVMRP ルート数の制限」(P.50-59) (任意)
- 「DVMRP ルートしきい値の変更」(P.50-59) (任意)
- 「DVMRP サマリーアドレスの設定」(P.50-60) (任意)
- 「DVMRP 自動サマライズのディセーブル化」(P.50-62) (任意)
- 「DVMRP ルートへのメトリック オフセットの追加」(P.50-62) (任意)

アドバタイズされる DVMRP ルート数の制限

デフォルトでは、DVMRP を実行するためにイネーブル化されたインターフェイス (つまり、DVMRP トンネル、DVMRP ネイバーが検出されたインターフェイス、または `ip dvmrp unicast-routing` インターフェイス コンフィギュレーション コマンドを実行するように設定されたインターフェイス) を通して、7000 の DVMRP ルートだけがアドバタイズされます。

DVMRP ルートの制限を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip dvmrp route-limit count</code>	DVMRP に対してイネーブル化されたインターフェイスを通してアドバタイズされる DVMRP 数を変更します。 このコマンドを使用すると、 <code>ip dvmrp metric</code> インターフェイス コンフィギュレーション コマンドの設定ミスによる MBONE への大量のルート注入を防ぐことができます。 デフォルトでは、7000 のルートがアドバタイズされます。指定できる範囲は 0 ~ 4294967295 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート数が制限されないように設定するには、`no ip dvmrp route-limit` グローバル コンフィギュレーション コマンドを使用します。

DVMRP ルートしきい値の変更

デフォルトでは、1 つのインターフェイスにつき、1 分間に 10000 の DVMRP ルートを受信できます。この速度を超えると、ルート サージが発生した可能性を警告する Syslog メッセージが発行されます。通常この警告は、デバイスの設定ミスにより大量のルートが MBONE に入った場合、迅速な検出を行うために使用されます。

警告送信の基準となるルート数のしきい値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dvmrp routehog-notification <i>route-count</i>	Syslog メッセージの送信基準となるルート数を設定します。 デフォルト値は 10000 ルートで、指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

動作中のルート数を表示するには、**show ip igmp interface** 特権 EXEC コマンドを使用します。このルート数を超えると、***** ALERT ***** が表示行に表示されます。

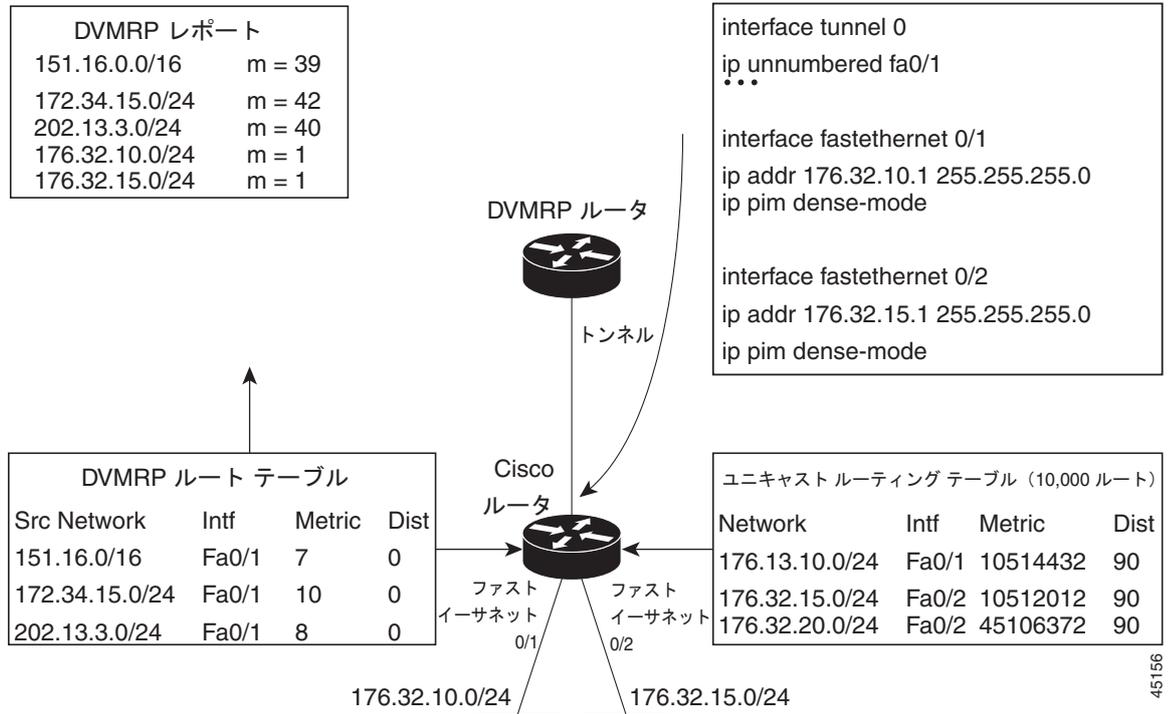
DVMRP サマリー アドレスの設定

デフォルトでは、シスコ デバイスは、ユニキャスト ルーティング テーブル内の接続されたユニキャスト ルートだけ（つまり、ルータに直接接続されたサブネットへのルートだけ）を DVMRP ルートレポート メッセージに格納してアドバタイズします。これらのルートは、通常の DVMRP のクラス指定されたルート サマライズによって処理されます。このプロセスは、アドバタイズされているルートとアドバタイズ中に経由するインターフェイスが、クラス指定された同じネットワーク内にあるかどうかに応じて異なります。

図 50-10 に、デフォルトの動作例を示します。この例で、Cisco ルータによって送信される DVMRP レポートに記述されているのは、DVMRP メトリックに 32 を追加してポイズンリバーサされた DVMRP ルータから受信した 3 つの元のルートです。これらのルートのあとに、ユニキャスト ルーティング テーブルから取得した、直接接続されている 2 つのネットワーク（176.32.10.0/24 および 176.32.15.0/24）にアドバタイズされる 2 つのルートが記述されています。DVMRP トンネルはファストイーサネット ポート 1 と同じ IP アドレスを共有し、直接接続された 2 つのサブネットと同じクラス B ネットワークに分類されるため、これらのルートに対してクラス指定サマライズは実行されません。その結果、DVMRP ルータは、直接接続されたサブネットへ向かうこれらの 2 つのルートだけをポイズンリバーサします。また、これらの 2 つのイーサネット セグメント上の送信元によって送信されたマルチキャストトラフィックに対しては、RPF だけを適切に実行します。これら 2 つのイーサネット セグメント上にはない、Cisco ルータ背後のネットワーク内の他のマルチキャスト送信元では、DVMRP ルータに関する RPF チェックは適切に行われず、廃棄されます。

サマリー アドレス (**ip dvmrp summary-address address mask** インターフェイス コンフィギュレーション コマンドのアドレスおよびマスクのペアで指定) の範囲内にあるルートの代わりに、サマリー アドレスをアドバタイズするように Cisco ルータを設定できます。ユニキャスト ルーティング テーブルにサマリー アドレス範囲内のルートが 1 つまたは複数格納されている場合は、サマリー アドレスが DVMRP ルート レポートに格納されて送信されます。それ以外の場合、サマリー アドレスはアドバタイズされません。図 50-10 では、Cisco ルータ トンネル インターフェイスに **ip dvmrp summary-address** コマンドを設定します。その結果、Cisco ルータは、ユニキャスト ルーティング テーブルのネットワーク 176.32.0.0.16 に、サマライズされた単一のクラス B アドバタイズを送信します。

図 50-10 接続されたユニキャスト ルートにだけアドバタイズ (デフォルト) する例



デフォルトのクラス指定サマライズが要求を満たさない場合に、DVMRP ルートのサマライズをカスタマイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。



(注) 設定されたサマリー アドレスをアドバタイズする前に、ユニキャスト ルーティング テーブルに具体的なルートを 1 つまたは複数設定する必要があります。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション コマンドを入力します。
ステップ3 ip dvmrp summary-address address mask [metric value]	DVMRP サマリー アドレスを指定します。 <ul style="list-style-type: none"> • summary-address address mask には、サマリー IP アドレス、および具体的なルートの代わりにアドバタイズされるマスクを指定します。 • (任意) metric value を指定する場合は、サマリーアドレスとともにアドバタイズされるメトリックを指定します。デフォルトは 1 です。指定できる範囲は 1 ~ 32 です。
ステップ4 end	特権 EXEC モードに戻ります。
ステップ5 show running-config	設定を確認します。
ステップ6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスを削除するには、**no ip dvmrp summary-address address mask [metric value]** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP 自動サマライズのディセーブル化

ソフトウェアでは、デフォルトで一部のレベルの DVMRP サマライズが自動実行されます。サマリーだけでなくすべてのルートを実バタイズする場合は、この機能をディセーブルにします。特別な場合には、すべてのサブネット情報が格納された隣接する DVMRP ルータを使用し、DVMRP ネットワーク内のマルチキャスト トラフィックの流れを詳細に制御できます。この例としては、PIM ネットワークが DVMRP クラウドに複数のポイントで接続されているとき、具体的な（サマライズされていない）ルートが DVMRP ネットワークに送信され、PIM クラウド内の各サブネットへ向かうさらに適切なパスが実バタイズされる場合などがあります。

ip dvmrp summary-address インターフェイス コンフィギュレーション コマンドを設定し、**no ip dvmrp auto-summary** を設定しなかった場合は、カスタムと自動サマリーの両方が得られます。

DVMRP 自動サマリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no ip dvmrp auto-summary	DVMRP 自動サマライズをディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

自動サマライズを再びイネーブルにするには、**ip dvmrp auto-summary** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP ルートへのメトリック オフセットの追加

デフォルトでは、着信 DVMRP レポートに格納されて実バタイズされた DVMRP ルートのメトリック（ホップ数）は、スイッチによって 1 だけ増加されます。特定のルートの優先度を上下させる場合は、メトリックを変更できます。

たとえば、マルチレイヤ スイッチ A からルートが取得され、より大きなメトリックを持つ同じルートがマルチレイヤ スイッチ B から学習されたとします。スイッチ B を経由するパスの方が高速であるため、このパスを使用する場合は、スイッチ A によって学習されたルートにメトリック オフセットを適用し、スイッチ B によって学習されたメトリックよりもメトリックを大きくできます。この結果、スイッチ B を経由するパスを選択できます。

デフォルトのメトリックを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ3	<code>ip dvmrp metric-offset [in out] increment</code>	<p>着信レポートに格納されてアドバタイズされる DVMRP ルートに追加されるメトリックを変更します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • (任意) in : 増分値が着信 DVMRP レポートに追加され、<code>mrinfo</code> 応答内で報告されます。 • (任意) out : 増分値が、DVMRP ルーティング テーブルのルートに対する発信 DVMRP レポートに追加されます。 <p>in と out のどちらも指定しない場合は、in がデフォルトになります。</p> <p><code>increment</code> には、レポート メッセージに格納されてアドバタイズされる DVMRP ルータのメトリックの増分値を指定します。指定できる範囲は 1 ~ 31 です。</p> <p><code>ip dvmrp metric-offset</code> コマンドがインターフェイス上で設定されていない場合、着信ルートのデフォルトの増分値は 1 です。発信ルートのデフォルト値は 0 です。</p>
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip dvmrp metric-offset` インターフェイス コンフィギュレーション コマンドを使用します。

IP マルチキャスト ルーティングのモニタおよびメンテナンス

ここでは、IP マルチキャスト ルーティングのモニタ方法およびメンテナンス方法について説明します。

- 「キャッシュ、テーブル、およびデータベースのクリア」(P.50-63)
- 「システムおよびネットワーク統計情報の表示」(P.50-64)
- 「IP マルチキャスト ルーティングのモニタ」(P.50-65)

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

表 50-5 に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 50-5 キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
<code>clear ip cgmp</code>	Catalyst スイッチによってキャッシュに格納されたすべてのグループ エントリをクリアします。
<code>clear ip dvmrp route {* route}</code>	DVMRP ルーティング テーブルからルートを削除します。
<code>clear ip igmp group [group-name group-address interface]</code>	IGMP キャッシュのエントリを削除します。
<code>clear ip mroute {* group [source]}</code>	IP マルチキャスト ルーティング テーブルのエントリを削除します。
<code>clear ip pim auto-rp rp-address</code>	自動 RP キャッシュをクリアします。
<code>clear ip sdr [group-address "session-name"]</code>	Session Directory Protocol バージョン 2 キャッシュ (sdr キャッシュ エントリ) を削除します。

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。



(注)

このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

表 50-6 に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 50-6 システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
<code>ping [group-name group-address]</code>	マルチキャストグループアドレスに ICMP エコー要求を送信します。
<code>show ip dvmrp route [ip-address]</code>	DVMRP ルーティング テーブルのエントリを表示します。
<code>show ip igmp groups [group-name group-address type number]</code>	スイッチに直接接続されている、IGMP によって取得されたマルチキャストグループを表示します。
<code>show ip igmp interface [type number]</code>	インターフェイスのマルチキャスト関連情報を表示します。
<code>show ip mcache [group [source]]</code>	IP 高速スイッチング キャッシュの内容を表示します。
<code>show ip mpacket [source-address name] [group-address name] [detail]</code>	循環キャッシュヘッダー バッファの内容を表示します。
<code>show ip mroute [group-name group-address] [source] [summary] [count] [active kbps]</code>	IP マルチキャスト ルーティング テーブルの内容を表示します。

表 50-6 システムおよびネットワーク統計情報を表示するコマンド (続き)

コマンド	目的
<code>show ip pim interface [type number] [count] [detail]</code>	PIM 用に設定されたインターフェイスの情報を表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip pim neighbor [type number]</code>	スイッチによって検出された PIM ネイバーのリストを示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip pim rp [group-name group-address]</code>	SM マルチキャスト グループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip rpf {source-address name}</code>	スイッチの RPF の実行方法 (ユニキャスト ルーティング テーブル、DVMPRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれか) を表示します。
<code>show ip sdr [group "session-name" detail]</code>	Session Directory Protocol バージョン 2 のキャッシュを表示します。

IP マルチキャスト ルーティングのモニタ

表 50-7 に示す特権 EXEC コマンドを使用すると、IP マルチキャスト ルータ、パケット、パスをモニタできます。

表 50-7 IP マルチキャスト ルーティングをモニタするためのコマンド

コマンド	目的
<code>mrinfo [hostname address] [source-address interface]</code>	マルチキャスト ルータまたはマルチレイヤ スイッチとピアリングする隣接マルチキャスト デバイスに関して、マルチキャスト ルータまたはマルチレイヤ スイッチをクエリーします。
<code>mstat source [destination] [group]</code>	IP マルチキャスト パケット速度および損失情報を表示します。
<code>mtrace source [destination] [group]</code>	指定されたグループのマルチキャスト配信ツリーに対して、送信元から宛先ブランチへのパスをトレースします。



CHAPTER 51

MSDP の設定

この章では、IE 3000 スイッチに Multicast Source Discovery Protocol (MSDP) を設定する手順について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode (PIM-SM) ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol (MBGP) がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

この機能を使用するには、スタック マスター上で IP サービス イメージが稼働している必要があります。特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「MSDP の概要」 (P.51-1)
- 「MSDP の設定」 (P.51-3)
- 「MSDP のモニタおよびメンテナンス」 (P.51-18)

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべての Rendezvous Point (RP; ランデブー ポイント) に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は伝送制御プロトコル (TCP) を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。交換されるのは、主にマルチキャスト グループを送信する送信元のリストです。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャスト データは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメイン RP で発信する必要があります。

MSDP のドメイン間動作は、Border Gateway Protocol (BGP) または MBGP に大きく依存します。ドメイン内の RP (インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP) で、MSDP を実行してください。

MSDP の動作

図 51-1 に、2 つの MSDP ピア間での MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。MSDP が設定されている場合は、次のシーケンスが発生します。

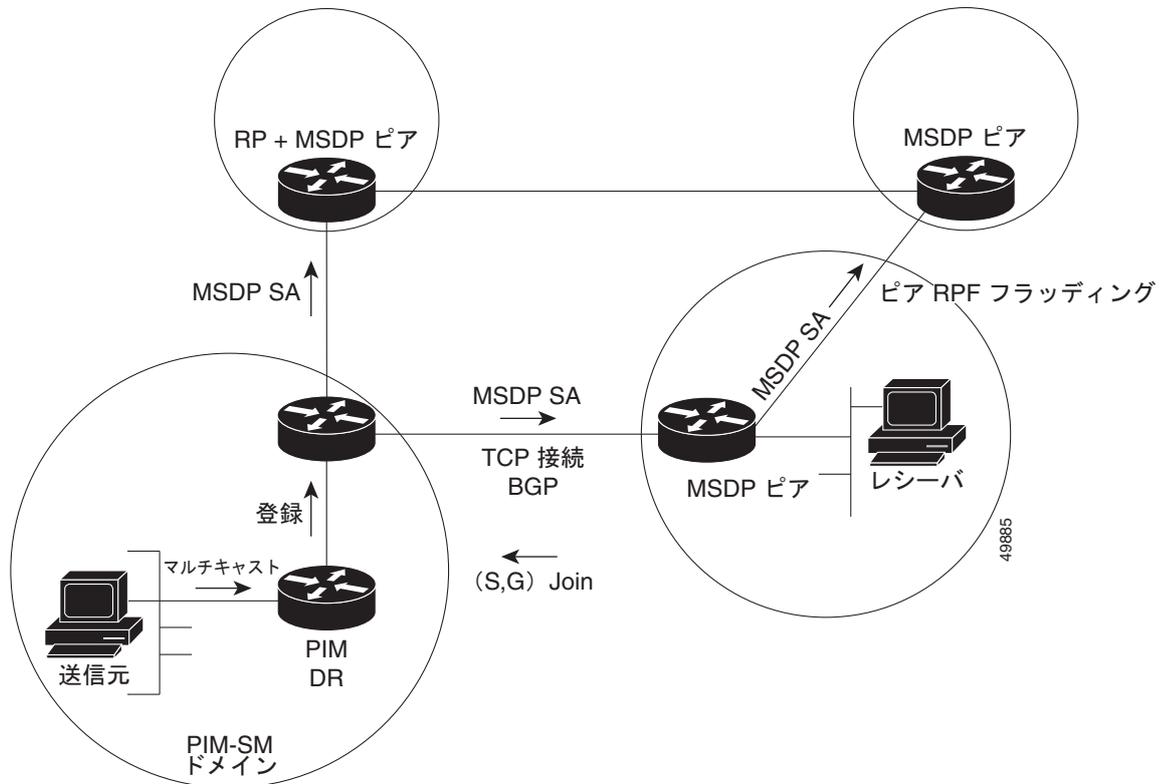
送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ (指定ルータまたは RP) によって RP に PIM 登録メッセージが送信されます。RP は登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active (SA) メッセージもすべての MSDP ピアに転送されます。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID (RP アドレスとして使用されるインターフェイスの IP アドレス) が設定されている場合は、SA メッセージによってこれらが識別されます。

各 MSDP ピアは SA メッセージを発信元の RP から受信して転送し、ピア Reverse-Path Forwarding (RPF) フラッドングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは RPF ピアと呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、「[デフォルトの MSDP ピアの設定](#)」(P.51-4) を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージをドロップします。それ以外の場合、すべての MSDP ピアにメッセージが転送されます。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの加入要求を持ち、空でない発信インターフェイス リストに (*,G) エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に (S,G) Join メッセージが送信されます。(S,G) Join メッセージが送信元の DR に到達すると、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されます。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバへと送信できます。

図 51-1 RP ピア間で動作する MSDP



MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカルメンバーはローカルツリーに加入します。共有ツリーへの Join メッセージはドメインから脱退する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにでき、セキュリティが高まります。
- レシーバだけが配置されているドメインは、グループメンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャストルーティングテーブルステートが不要になり、メモリが削減されます。

MSDP の設定

ここでは、次の設定について説明します。

- 「MSDP のデフォルト設定」(P.51-4)
- 「デフォルトの MSDP ピアの設定」(P.51-4) (必須)
- 「SA ステートのキャッシング」(P.51-6) (任意)

- 「MSDP ピアからの送信元情報の要求」(P.51-8) (任意)
- 「スイッチから発信される送信元情報の制御」(P.51-8) (任意)
- 「スイッチで転送される送信元情報の制御」(P.51-11) (任意)
- 「スイッチで受信される送信元情報の制御」(P.51-13) (任意)
- 「MSDP メッシュ グループの設定」(P.51-15) (任意)
- 「MSDP ピアのシャットダウン」(P.51-15) (任意)
- 「MSDP への境界 PIM DM 領域の追加」(P.51-16) (任意)
- 「RP アドレス以外の発信元アドレスの設定」(P.51-17) (任意)

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

デフォルトの MSDP ピアの設定

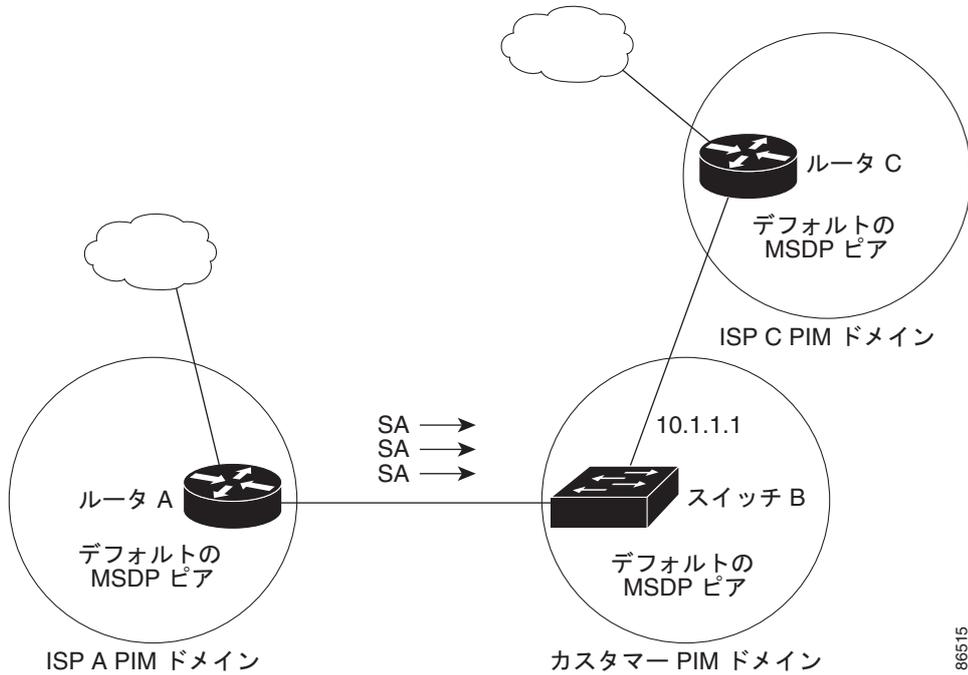
このソフトウェア リリースでは、BGP および MBGP がサポートされていないため、`ip msdp peer` グローバル コンフィギュレーション コマンドを使用して、ローカル スイッチに MSDP ピアを設定できません。その代わりに、デフォルトの MSDP ピアを定義し、そこから送信されるスイッチのすべての SA メッセージを受信できます（そのためには、`ip msdp default-peer` グローバル コンフィギュレーション コマンドを使用します）。デフォルトの MSDP ピアは、事前に設定しておく必要があります。スイッチで MSDP ピアによる BGP または MBGP ピアリングが行われない場合は、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチでは常にそのピアからのすべての SA メッセージを受信されます。

図 51-2 に、デフォルトの MSDP ピアを使用できるネットワークを示します。図 51-2 では、スイッチ B を所有するカスタマーが、2 つの Internet Service Provider (ISP; インターネット サービス プロバイダー) に接続されています。一方の ISP はルータ A、もう一方の ISP はルータ C を所有しています。これらの ISP 間で、BGP または MBGP は動作していません。ISP のドメイン内、または他のドメイン内の送信元を学習するため、カスタマー サイトのスイッチ B はルータ A をデフォルトの MSDP ピアとして識別します。スイッチ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、受信するのはルータ A からの SA メッセージ、またはルータ C からの SA メッセージだけです。ルータ A がコンフィギュレーション ファイルの最初に記述されている場合、ルータ A が動作していれば、ルータ A が使用されます。ルータ A が動作していない場合だけ、スイッチ B はルータ C からの SA メッセージを受信します。これが、プレフィックス リストがない場合のデフォルトの動作です。

プレフィックス リストを指定すると、ピアはリスト内のプレフィックス専用のデフォルトピアになります。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルトピアを設定できます。プレフィックス リストがない場合も、複数のデフォルトピアを設定できますが、アクティブなデフォルトピアになるのは最初のピアだけです（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。最初に設定されたデフォルトピアに障害が発生した場合、またはこのピアが正常に接続されていない場合は、2 番めに設定されているピアがアクティブなデフォルトピアになります。以下同様に処理されます。

通常、ISP はプレフィックス リストを使用して、カスタマーのルータから受信するプレフィックスを定義します。

図 51-2 デフォルトの MSDP ピア ネットワーク



デフォルトの MSDP ピアを指定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>ip msdp default-peer ip-address name [prefix-list list]</code>	<p>すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。</p> <ul style="list-style-type: none"> <code>ip-address name</code> には、MSDP デフォルト ピアの IP アドレスまたはドメイン ネーム システム (DNS) サーバ名を入力します。 (任意) <code>prefix-list list</code> を指定する場合は、リスト内のプレフィックス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 <p>prefix-list キーワードが指定された <code>ip msdp default-peer</code> コマンドを複数入力すると、複数の RP プレフィックスに対してすべてのデフォルト ピアが同時に使用されます。この構文は通常、スタブ サイト クラウドに接続されたサービス プロバイダー クラウドで使用されます。</p> <p>prefix-list キーワードを指定せずに <code>ip msdp default-peer</code> コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。</p>

	コマンド	目的
ステップ 3	<code>ip prefix-list name [description string] seq number {permit deny} network length</code>	(任意) ステップ 2 で指定された名前を使用し、プレフィックスリストを作成します。 <ul style="list-style-type: none"> • (任意) description string を指定する場合は、このプレフィックスリストを説明する 80 文字以下のテキストを入力します。 • seq number には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ~ 4294967294 です。 • deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • network length には、許可または拒否されているネットワークの番号およびネットワーク マスク長 (ビット単位) を指定します。
ステップ 4	<code>ip msdp description {peer-name peer-address} text</code>	(任意) 設定内で、または show コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ピアを削除するには、`no ip msdp default-peer ip-address | name` グローバル コンフィギュレーション コマンドを使用します。

次に、[図 51-2](#) のルータ A およびルータ C の設定の一部を示します。それぞれの ISP には、デフォルトピア (BGP または MBGP 以外) を使用する複数のカスタマーが存在します ([図 51-2](#) のカスタマーと同様)。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィックスリストで SA が許可されている場合、デフォルトピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング

デフォルトでは、スイッチで受信された SA メッセージ内の送信元とグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、次の SA メッセージによって送信元に関する情報が取得されるまでそのメンバーは待機する必要があります。この遅延は加入遅延と呼ばれます。

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにスイッチを設定できます。

送信元とグループのペアのキャッシングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip msdp cache-sa-state [list access-list-number]	送信元とグループのペアのキャッシングをイネーブルにします (SA ステートを作成します)。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 list access-list-number を指定する場合、範囲は 100 ~ 199 です。
ステップ3	access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • access-list-number の範囲は 100 ~ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • protocol には、プロトコル名として ip を入力します。 • source には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • source-wildcard には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • destination には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • destination-wildcard には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show running-config	設定を確認します。
ステップ6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

このコマンドの代わりに、**ip msdp sa-request** グローバル コンフィギュレーション コマンドを使用できます。代替コマンドを使用すると、グループの新しいメンバーがアクティブになった場合に、SA 要求メッセージがスイッチから MSDP ピアに送信されます。詳細については、次の項を参照してください。

デフォルト設定 (SA ステートが作成されていない状態) に戻すには、**no ip msdp cache-sa-state** グローバル コンフィギュレーション コマンドを使用します。

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャストトラフィックを受信する必要がある場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャストトラフィックを受信する必要がある場合、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp sa-request {ip-address name}</code>	指定された MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定します。 <i>ip-address name</i> を指定する場合は、グループの新しいメンバーがアクティブになるときにローカル スイッチの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御

スイッチから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元 (送信元ベース)
- 送信元情報のレシーバー (要求元認識ベース)

詳細については、「送信元の再配信」(P.51-9) および「SA 要求メッセージのフィルタリング」(P.51-10) を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A* フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]	<p>SA メッセージに格納されてアドバタイズされる、マルチキャストルーティング テーブル内の (S,G) エントリを設定します。</p> <p>デフォルトでは、ローカル ドメイン内の送信元だけがアドバタイズされます。</p> <ul style="list-style-type: none"> • (任意) list access-list-name を指定する場合は、IP 標準または IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ~ 99、拡張アクセス リストの範囲は 100 ~ 199 です。アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • (任意) asn aspath-access-list-number を指定する場合は、1 ~ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、ip as-path access-list コマンドでも設定する必要があります。 • (任意) route-map map を指定する場合は、1 ~ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、ip as-path access-list コマンドでも設定する必要があります。 <p>アクセス リストまたは自律システム パス アクセス リストに従って、(S,G) ペアがアドバタイズされます。</p>

	コマンド	目的
ステップ 3	<p>access-list <i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>]</p> <p>または</p> <p>access-list <i>access-list-number</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard</i></p>	<p>IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <p>または</p> <p>IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、標準アクセス リストの範囲は 1 ~ 99、拡張アクセス リストの範囲は 100 ~ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、**no ip msdp redistribute** グローバル コンフィギュレーション コマンドを使用します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているスイッチだけが、SA 要求に応答します。このようなスイッチでは、デフォルトで MSDP ピアからのすべての SA 要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、スイッチを設定できます。標準アクセス リストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。アクセス リスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

これらの方法のいずれかを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp filter-sa-request ip-address name</code> または <code>ip msdp filter-sa-request {ip-address name} list access-list-number</code>	指定された MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。 または 標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセス リストには、複数のグループ アドレスが記述されています。 <code>access-list-number</code> の範囲は 1 ~ 99 です。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • <code>access-list-number</code> の範囲は 1 ~ 99 です。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp filter-sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 に合格して、受信されます。その他のすべてのメッセージは無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチで転送される送信元情報の制御

デフォルトでは、スイッチで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または Time To Live (TTL; 存続可能時間) 値を設定し、発信メッセージがピアに転送されないようにできます。次の項では、この方法について説明します。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp sa-filter out <i>ip-address</i> <i>name</i> または ip msdp sa-filter out { <i>ip-address</i> <i>name</i> } list <i>access-list-number</i> または ip msdp sa-filter out { <i>ip-address</i> <i>name</i> } route-map <i>map-tag</i>	指定された MSDP ピアへの SA メッセージをフィルタリングします。 または IP 拡張アクセス リストに合格する、指定されたピア宛ての SA メッセージだけを通過させます。拡張アクセス リスト <i>access-list-number</i> の範囲は 100 ~ 199 です。 list と route-map の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの (S,G) ペアを通過できません。 または ルート マップ <i>map-tag</i> 内の一致条件を満たす、指定された MSDP ピア宛ての SA メッセージを通過させます。 すべての一致条件を満たす場合、ルート マップに permit が指定されていれば、ルートはフィルタを通過します。 deny が指定されていれば、ルートはフィルタリングされます。
ステップ 3	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i>	(任意) IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、`no ip msdp sa-filter out {ip-address | name} [list access-list-number] [route-map map-tag]` グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 100 を通過する (S,G) ペアだけが SA メッセージに格納され、`switch.cisco.com` という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が `tth` 引数以上であるマルチキャスト パケットだけが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>ip msdp ttl-threshold {ip-address name} ttl</code>	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 <ul style="list-style-type: none"> <code>ip-address name</code> を指定する場合は、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 <code>tth</code> には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ~ 255 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp ttl-threshold {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp sa-filter in <i>ip-address</i> <i>name</i> または ip msdp sa-filter in { <i>ip-address</i> <i>name</i> } list <i>access-list-number</i> または ip msdp sa-filter in { <i>ip-address</i> <i>name</i> } route-map <i>map-tag</i>	指定された MSDP ピアからの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストに合格する、指定されたピア宛ての SA メッセージだけを通過させます。拡張アクセス リスト <i>access-list-number</i> の範囲は 100 ~ 199 です。 list と route-map の両方のキーワードを使用すると、すべての条件に一致しなければ、着信 SA メッセージ内のいずれの (S,G) ペアも通過できません。 または ルート マップ <i>map-tag</i> 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージを通過させます。 すべての一致条件を満たす場合、ルート マップに permit が指定されていれば、ルートはフィルタを通過します。 deny が指定されていれば、ルートはフィルタリングされます。
ステップ 3	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i>	(任意) IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、**no ip msdp sa-filter in {ip-address | name} [list access-list-number] [route-map map-tag]** グローバル コンフィギュレーション コマンドを使用します。

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

MSDP メッシュ グループの設定

MSDP メッシュ グループは、MSDP によって完全なメッシュ型に相互接続された MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメインを越えて SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp mesh-group name {ip-address name}	MSDP メッシュ グループを設定するには、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 <ul style="list-style-type: none"> <i>name</i> には、メッシュ グループの名前を入力します。 <i>ip-address name</i> には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 6		グループ内の MSDP ピアごとに、この手順を繰り返します。

メッシュ グループから MSDP ピアを削除するには、**no ip msdp mesh-group name {ip-address | name}** グローバル コンフィギュレーション コマンドを使用します。

MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp shutdown {peer-name peer address}</code>	設定情報を保持したまま、指定された MSDP ピアを管理上のシャットダウン状態にします。 <i>peer-name</i> <i>peer address</i> を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ピアを再起動するには、`no ip msdp shutdown {peer-name | peer address}` グローバル コンフィギュレーション コマンドを使用します。TCP 接続が再確立されます。

MSDP への境界 PIM DM 領域の追加

Dense-Mode (DM; デンス モード) 領域と PIM SM 領域の境界となるスイッチに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。



(注) `ip msdp border sa-address` グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアダプタイズするように SM ドメインを設定してください。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp border sa-address interface-id</code>	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 <i>interface-id</i> には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 3	<code>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</code>	SA メッセージに格納されてアダプタイズされる、マルチキャストルーティング テーブル内の (S,G) エントリを設定します。 詳細については、「送信元の再配信」(P.51-9) を参照してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

デフォルト設定 (DM 領域内のアクティブな送信元が MSDP に加入しない設定) に戻すには、**no ip msdp border sa-address interface-id** グローバル コンフィギュレーション コマンドを使用します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、ローカルな RP を設定する場合
- PIM SM ドメインと DM ドメインの境界となるスイッチがある場合。サイトの DM ドメインの境界となるスイッチがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このスイッチは RP でないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip msdp originator-id interface-id	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 <i>interface-id</i> には、ローカル スイッチのインターフェイスを指定します。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ip msdp border sa-address と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

この方法で RP アドレスが取得されないようにするには、**no ip msdp originator-id interface-id** グローバル コンフィギュレーション コマンドを使用します。

MSDP のモニタおよびメンテナンス

MSDP SA メッセージ、ピア、ステート、またはピア ステータスをモニタするには、表 51-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 51-1 MSDP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>debug ip msdp [peer-address name] [detail] [routes]</code>	MSDP アクティビティをデバッグします。
<code>debug ip msdp resets</code>	MSDP ピアのリセット原因をデバッグします。
<code>show ip msdp count [autonomous-system-number]</code>	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。 <code>ip msdp cache-sa-state</code> コマンドは、このコマンドによって出力が生成されるように設定する必要があります。
<code>show ip msdp peer [peer-address name]</code>	MSDP ピアに関する詳細情報を表示します。
<code>show ip msdp sa-cache [group-address source-address group-name source-name] [autonomous-system-number]</code>	MSDP ピアから学習した (S,G) ステートを表示します。
<code>show ip msdp summary</code>	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするには、表 51-2 に示す特権 EXEC コマンドを使用します。

表 51-2 MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするためのコマンド

コマンド	目的
<code>clear ip msdp peer peer-address name</code>	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージカウンタをリセットします。
<code>clear ip msdp statistics [peer-address name]</code>	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報カウンタをクリアします。
<code>clear ip msdp sa-cache [group-address name]</code>	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。



CHAPTER 52

フォールバック ブリッジングの設定

この章では、IE 3000 スイッチ上でフォールバック ブリッジング (VLAN ブリッジング) を設定する手順について説明します。フォールバック ブリッジングを使用すると、スイッチが VLAN ブリッジドメインとルーテッドポート間でルーティングしない、非 IP パケットを転送できます。



(注)

この機能を使用するには、スイッチ上で IP サービス イメージが稼働している必要があります。この章で使用しているコマンドの構文および使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある、『Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2』を参照してください。

この章の内容は、次のとおりです。

- 「フォールバック ブリッジングの概要」 (P.52-1)
- 「フォールバック ブリッジングの設定」 (P.52-3)
- 「フォールバック ブリッジングのモニタおよびメンテナンス」 (P.52-11)

フォールバック ブリッジングの概要

フォールバック ブリッジングを使用すると、スイッチは複数の VLAN またはルーテッドポート (特に 1 つのブリッジドメイン内で複数の VLAN に接続されている VLAN またはルーテッドポート) をまとめてブリッジングできます。フォールバック ブリッジングを行うと、スイッチでルーティングおよび転送されないトラフィックや、DECnet などのルーティングできないプロトコルに属するトラフィックが転送されます。

VLAN ブリッジドメインは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) によって表されます。(VLAN が関連付けられていない) 一連の SVI およびルーテッドポートは、ブリッジグループを形成するように設定 (グループ化) できます。SVI はスイッチポートの VLAN を、システム内のルーティング機能またはブリッジング機能へのインターフェイスの 1 つとして表します。1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN 間のルーティング、VLAN 間でルーティングできないプロトコルのフォールバック ブリッジング、またはスイッチと IP ホストの接続を実現する場合にだけ、VLAN に SVI を設定してください。ルーテッドポートはルータ上のポートと同様に機能する物理ポートですが、ルータには接続されていません。ルーテッドポートは特定の VLAN と関連付けられておらず、VLAN サブインターフェイスをサポートしていませんが、通常のルーテッドポートのように動作します。SVI およびルーテッドポートの詳細については、第 14 章「インターフェイス特性の設定」を参照してください。

ブリッジグループは、スイッチ上のネットワーク インターフェイスの内部構造です。ブリッジグループが定義されているスイッチの外側にあるブリッジグループ内では、スイッチングされるトラフィックを識別する目的でのブリッジグループの使用はできません。同じスイッチ上のブリッジグループは、異なるブリッジとして機能します。つまり、スイッチ上の異なるブリッジグループ間で、ブリッジドトラフィックおよび Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) は交換されません。

フォールバック ブリッジングを使用しても、ブリッジングされている VLAN のスパニングツリーは縮小できません。各 VLAN には、独自のスパニングツリー インスタンスと、ループを防止するためにブリッジグループの一番上で動作する個別のスパニングツリー (別名 VLAN ブリッジ スパニングツリー) があります。

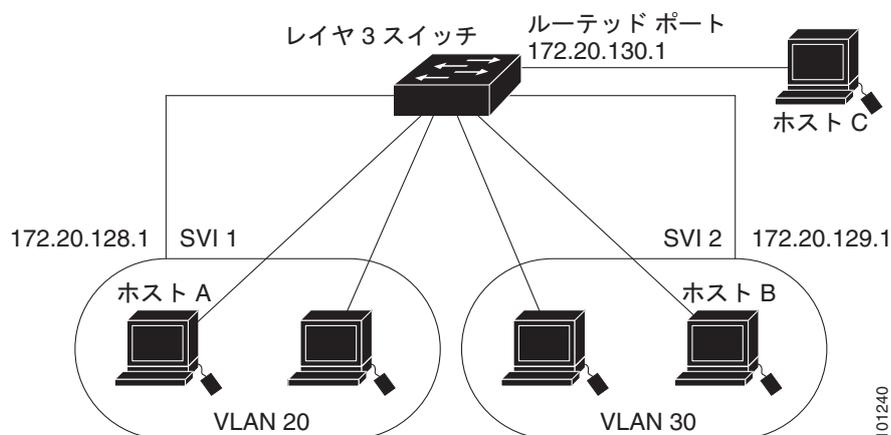
ブリッジグループが作成されると、スイッチは VLAN ブリッジ スパニングツリー インスタンスを作成します。スイッチはブリッジグループを実行し、ブリッジグループ内の SVI およびルーテッドポートをスパニングツリー ポートとして処理します。

ネットワーク インターフェイスをブリッジグループに格納する理由は、次のとおりです。

- ブリッジグループを構成するネットワーク インターフェイス間でルーティングされない全トラフィックをブリッジングするため。宛先アドレスがブリッジテーブルに格納されているパケットは、ブリッジグループ内の単一のインターフェイス上で転送されます。宛先アドレスがブリッジテーブル内に格納されていないパケットは、ブリッジグループ内のすべてのインターフェイス上でフラディングされます。ブリッジグループで送信元 MAC アドレスが学習されるのは、このアドレスが VLAN 上で学習された場合だけです (この逆は成り立ちません)。
- 接続されている LAN 上で BPDU を受信 (場合によっては送信) することにより、スパニングツリー アルゴリズムに参加するため。設定されたブリッジグループごとに、個別のスパニングツリー プロセスが動作します。各ブリッジグループは個別のスパニングツリー インスタンスに参加します。ブリッジグループは、メンバー インターフェイスだけが受信する BPDU に基づいて、スパニングツリー インスタンスを確立します。VLAN がブリッジグループに属していないポートに着信したブリッジ Spanning-Tree Protocol (STP; スパニングツリー プロトコル) BPDU は、VLAN のすべての転送ポートでフラディングされます。

図 52-1 に、フォールバック ブリッジング ネットワークの例を示します。このスイッチには、SVI として 2 つのポートが設定されています。これらの SVI は異なる IP アドレスを持ち、2 つの異なる VLAN に接続されています。さらに、もう 1 つのポートが独自の IP アドレスを持つルーテッドポートとして設定されています。これらの 3 つのポートがすべて同じブリッジグループに割り当てられている場合は、これらのポートが異なるネットワークや異なる VLAN にあっても、スイッチに接続されているエンドステーション間で非 IP プロトコル フレームを転送できます。フォールバック ブリッジングを機能させるために IP アドレスをルーテッドポートや SVI に割り当てる必要はありません。

図 52-1 フォールバック ブリッジング ネットワークの例



フォールバック ブリッジングの設定

ここでは、次の設定について説明します。

- 「フォールバック ブリッジングのデフォルト設定」 (P.52-3)
- 「フォールバック ブリッジング設定時の注意事項」 (P.52-4)
- 「ブリッジグループの作成」 (P.52-4) (必須)
- 「スパニングツリー パラメータの調整」 (P.52-6) (任意)

フォールバック ブリッジングのデフォルト設定

表 52-1 に、フォールバック ブリッジングのデフォルト設定を示します。

表 52-1 フォールバック ブリッジングのデフォルト設定

機能	デフォルト設定
ブリッジグループ	未定義であるか、またはポートに割り当てられていません。VLAN ブリッジ STP は定義されていません。

表 52-1 フォールバックブリッジングのデフォルト設定 (続き)

機能	デフォルト設定
動的に学習されたステーションに対するスイッチからのフレーム転送	イネーブル
スパニングツリー パラメータ	
<ul style="list-style-type: none"> • スイッチ プライオリティ • ポート プライオリティ • ポート パス コスト 	<ul style="list-style-type: none"> • 32768 • 128 • 10 Mb/s : 100 100 Mb/s : 19 1000 Mb/s : 4
<ul style="list-style-type: none"> • hello BPDU インターバル • 転送遅延時間 • 最大アイドル時間 	<ul style="list-style-type: none"> • 2 秒 • 20 秒 • 30 秒

フォールバックブリッジング設定時の注意事項

スイッチには、最大 32 個のブリッジグループを設定できます。

1 つのインターフェイス (SVI またはルーテッドポート) が所属できるブリッジグループは 1 つだけです。

スイッチに接続されている個別のブリッジドネットワーク (トポロジの上で区別されるネットワーク) ごとに、1 つのブリッジグループを使用してください。

フォールバックブリッジングをプライベート VLAN が設定されたスイッチに設定しないでください。

IP (バージョン 4 とバージョン 6)、Address Resolution Protocol (ARP; アドレス解決プロトコル)、Reverse ARP (RARP; 逆アドレス解決プロトコル)、LOOPBACK、フレームリレー ARP、共有 STP パケットを除くすべてのプロトコルは、フォールバックブリッジングされます。

ブリッジグループの作成

一連の SVI またはルーテッドポートにフォールバックブリッジングを設定する場合は、これらのインターフェイスをブリッジグループに割り当てる必要があります。同じグループ内のすべてのインターフェイスは、同じブリッジドメインに属します。各 SVI またはルーテッドポートは、1 つのブリッジグループだけに割り当てることができます。



(注)

保護ポート機能とフォールバックブリッジングとの併用はできません。フォールバックブリッジングがイネーブルである場合、スイッチ上の 1 つの保護ポートから、別の VLAN 内にある同じスイッチ上の別の保護ポートにパケットが転送される可能性があります。

ブリッジグループを作成し、そこにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	bridge bridge-group protocol vlan-bridge	ブリッジ グループ番号を割り当て、ブリッジ グループで実行する VLAN ブリッジ スパニングツリー プロトコルを指定します。 ibm および dec キーワードはサポートされていません。 <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。最大 32 個のブリッジ グループを作成できます。フレームは同じグループ内のインターフェイス間でだけブリッジングされます。
ステップ3	interface interface-id	ブリッジ グループを割り当てるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> ルーターポート : no switchport インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 SVI : interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 (注) ルーターポートや SVI に IP アドレスを割り当てることができますが、これは必須ではありません。
ステップ4	bridge-group bridge-group	ステップ 2 で作成したブリッジ グループにインターフェイスを割り当てます。 デフォルトでは、インターフェイスはどのブリッジ グループにも割り当てられていません。インターフェイスは 1 つのブリッジ グループにだけ割り当てることができます。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ブリッジ グループを削除するには、**no bridge bridge-group** グローバル コンフィギュレーション コマンドを使用します。**no bridge bridge-group** コマンドを使用すると、該当するブリッジ グループからすべての SVI およびルーターポートが自動的に削除されます。ブリッジ グループからインターフェイスを削除したり、ブリッジ グループを削除したりするには、**no bridge-group bridge-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 を作成してこのブリッジ グループ内で実行する VLAN ブリッジ STP を指定し、ポートをルーターポートとして定義して、ブリッジ グループにポートを割り当てる例を示します。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# bridge-group 10
```

次に、ブリッジ グループ 10 を作成して、このブリッジ グループで実行する VLAN ブリッジ STP を指定する例を示します。VLAN 2 の SVI を定義し、これをブリッジ グループに割り当てます。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# vlan 2
```

```
Switch(config-vlan)# exit
Switch(config)# interface vlan2
Switch(config-if)# bridge-group 10
Switch(config-if)# exit
```

スパニングツリー パラメータの調整

特定のスパニングツリー パラメータのデフォルト値が不適切な場合は、このパラメータを調整する必要があります。スパニングツリー全体に影響するパラメータを設定する場合は、さまざまなタイプの **bridge** グローバル コンフィギュレーション コマンドを使用します。インターフェイス固有のパラメータを設定する場合は、さまざまなタイプの **bridge-group** インターフェイス コンフィギュレーション コマンドを使用します。

スパニングツリー パラメータを調整するには、次に示す作業のいずれかを実行します。

- 「VLAN ブリッジ スパニングツリー プライオリティの変更」(P.52-6) (任意)
- 「インターフェイス プライオリティの変更」(P.52-7) (任意)
- 「パス コストの割り当て」(P.52-7) (任意)
- 「BPDU インターバルの調整」(P.52-8) (任意)
- 「インターフェイスでのスパニングツリーのディセーブル化」(P.52-10) (任意)



(注)

スパニングツリー パラメータの調整は、スイッチおよび STP の機能に精通しているネットワーク管理者だけが行ってください。計画が不十分なまま調整を行うと、パフォーマンスの低下を招くことがあります。スイッチングに関する資料としては、IEEE 802.1D 仕様が適しています。詳細については、『Cisco IOS Configuration Fundamentals Command Reference』の付録「References and Recommended Reading」を参照してください。

VLAN ブリッジ スパニングツリー プライオリティの変更

ルート スイッチの候補として別のスイッチと同等のレベルにあるスイッチには、VLAN ブリッジ スパニングツリー プライオリティをグローバルに設定できます。このスイッチがルート スイッチとして選択される可能性を設定することもできます。

スイッチ プライオリティを変更するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group priority number	スイッチの VLAN ブリッジ スパニングツリー プライオリティを変更します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>number</i> には、0 ~ 65535 の数字を入力します。デフォルトは 32768 です。この値が低いほど、スイッチがルートとして選択される可能性が高くなります。
ステップ 3	end	特権 EXEC モードに戻ります。

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

デフォルト設定に戻すには、**no bridge bridge-group priority** グローバル コンフィギュレーション コマンドを使用します。ポートのプライオリティを変更するには、**bridge-group priority** インターフェイス コンフィギュレーション コマンドを使用します (次の項を参照)。

次に、ブリッジグループ 10 のスイッチ プライオリティを 100 に設定する例を示します。

```
Switch(config)# bridge 10 priority 100
```

インターフェイス プライオリティの変更

ポートのプライオリティを変更できます。2 つのスイッチがルート スwitch の候補として同等のレベルにある場合は、レベルに差が付くようにポート プライオリティを設定します。インターフェイスのプライオリティ値が低いスイッチが選択されます。

インターフェイス プライオリティを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	プライオリティを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>bridge-group bridge-group priority number</code>	ポート プライオリティを変更します。 <ul style="list-style-type: none"> bridge-group には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。 number には、0 ~ 255 の値を入力します (増分値は 4)。この値が低いほど、スイッチのポートがルートとして選択される可能性が高くなります。デフォルトは 128 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no bridge-group bridge-group priority** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジグループ 10 内のポートのプライオリティを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge-group 10 priority 20
```

パス コストの割り当て

各ポートにはパス コストが割り当てられています。規定では、パス コストは 1000/ (接続された LAN のデータ速度) の値を Mbps 単位で表したものです。

パス コストを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	パス コストを設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bridge-group bridge-group path-cost cost	ポートのパス コストを割り当てます。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>cost</i> には、0 ~ 65535 の数字を入力します。値が大きいほど、コストは大きくなります。 <ul style="list-style-type: none"> - 10 Mb/s の場合、デフォルトのパス コストは 100 です。 - 100 Mb/s の場合、デフォルトのパス コストは 19 です。 - 1000 Mb/s の場合、デフォルトのパス コストは 4 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのパス コストに戻すには、**no bridge-group bridge-group path-cost** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートのパス コストを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge-group 10 path-cost 20
```

BPDU インターバルの調整

ここでは、BPDU インターバルを調整する手順について説明します。

- 「[hello BPDU インターバルの調整](#)」(P.52-9) (任意)
- 「[転送遅延時間の変更](#)」(P.52-9) (任意)
- 「[最大アイドル時間の変更](#)」(P.52-10) (任意)



(注)

スパニングツリーの各スイッチには、個々の設定に関係なく、ルートスイッチの hello BPDU インターバル、転送遅延時間、および最大アイドル時間パラメータが採用されています。

hello BPDU インターバルの調整

hello BPDU インターバルを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	bridge bridge-group hello-time seconds	hello BPDU インターバルを指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、1 ~ 10 の数字を入力します。デフォルトは 2 です。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、ブリッジ グループ 10 内の hello インターバルを 5 秒に変更する例を示します。

```
Switch(config)# bridge 10 hello-time 5
```

転送遅延時間の変更

転送遅延時間は、ポートでスイッチングがアクティブになってから実際に転送を開始するまでの時間です。この間にトポロジ変更情報の受信が行われます。

転送遅延時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	bridge bridge-group forward-time seconds	転送遅延時間を指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、4 ~ 200 の数字を入力します。デフォルトは 20 です。
ステップ3	end	特権 EXEC モードに戻ります。
ステップ4	show running-config	設定を確認します。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、ブリッジ グループ 10 内の転送遅延時間を 10 秒に変更する例を示します。

```
Switch(config)# bridge 10 forward-time 10
```

最大アイドル時間の変更

指定時間内にルートスイッチからBPDUが受信されない場合は、スパニングツリートポロジが再計算されます。

最大アイドル時間（最大エージングタイム）を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group max-age seconds	ルートスイッチからBPDUをヒアリングするために待機する時間を指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、6 ~ 200 の数字を入力します。デフォルトは 30 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、ブリッジグループ 10 内の最大アイドル時間を 30 秒に変更する例を示します。

```
Switch(config)# bridge 10 max-age 30
```

インターフェイスでのスパニングツリーのディセーブル化

2つの任意のスイッチングサブネットワーク間にループのないパスが存在する場合は、一方のスイッチングサブネットワークで生成されたBPDUの影響が他方のサブネットワーク内のデバイスに及ばないようにできます（ただし、ネットワーク全体に及ぶスイッチングは可能です）。たとえば、スイッチング LAN サブネットワークが WAN によって分離されている場合は、BPDU の WAN リンク間移動を禁止できます。

ポート上でスパニングツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bridge-group bridge-group spanning-disabled	ポート上でスパニングツリーをディセーブルにします。 <i>bridge-group</i> には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でスパニングツリーを再びイネーブルにするには、**no bridge-group bridge-group spanning-disabled** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートのスパニングツリーをディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# bridge group 10 spanning-disabled
```

フォールバック ブリッジングのモニタおよびメンテナンス

ネットワークをモニタしてメンテナンスするには、表 52-2 に記載された特権 EXEC コマンドを 1 つまたは複数使用します。

表 52-2 フォールバック ブリッジングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
clear bridge <i>bridge-group</i>	学習したエントリを転送データベースから削除します。
show bridge [<i>bridge-group</i>] group	ブリッジ グループの詳細を表示します。
show bridge [<i>bridge-group</i>] [<i>interface-id</i> <i>mac-address</i> verbose]	ブリッジ グループ内で学習した MAC アドレスを表示します。

これらの表示内のフィールドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択し、『Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2』を参照してください。



CHAPTER 53

トラブルシューティング

この章では、IE 3000 スイッチの Cisco IOS ソフトウェアに関する問題を特定し解決する方法について説明します。問題の性質に応じて、コマンドライン インターフェイス (CLI) やデバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LED の説明など、トラブルシューティングの詳細については、ハードウェア インストレーション ガイドを参照してください。



(注)

この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Commands Master List, Release 12.2』を参照してください。

この章で説明する内容は、次のとおりです。

- 「ソフトウェアで障害が発生した場合の回復」 (P.53-2)
- 「パスワードを忘れた場合の回復」 (P.53-3)
- 「コマンド スイッチで障害が発生した場合の回復」 (P.53-4)
- 「クラスタ メンバ スイッチとの接続の回復」 (P.53-8)



(注) 回復手順を実行するには、スイッチを直接操作しなければなりません。

- 「自動ネゴシエーションの不一致の防止」 (P.53-8)
- 「PoE スイッチ ポートのトラブルシューティング」 (P.53-8)
- 「SFP モジュールのセキュリティと識別」 (P.53-9)
- 「SFP モジュール ステータスのモニタリング」 (P.53-10)
- 「ping の使用」 (P.53-10)
- 「レイヤ 2 traceroute の使用」 (P.53-11)
- 「IP traceroute の使用」 (P.53-13)
- 「TDR の使用」 (P.53-15)
- 「debug コマンドの使用」 (P.53-16)
- 「show platform forward コマンドの使用」 (P.53-17)
- 「crashinfo ファイルの使用」 (P.53-20)
- 「トラブルシューティング表」 (P.53-21)

ソフトウェアで障害が発生した場合の回復

スイッチソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤ったファイルをダウンロードした場合、イメージファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは Power-On Self-Test (POST; 電源投入時セルフテスト) に失敗し、接続できなくなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージファイルまたは間違ったイメージファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多数あり、使用するエミュレーションソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

- ステップ 1** PC 上で、Cisco.com から tar 形式のソフトウェア イメージファイル (*image_filename.tar*) をダウンロードします。
- Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージファイルの検索方法については、リリース ノートを参照してください。
- ステップ 2** tar ファイルから bin ファイルを抽出します。
- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
 - UNIX を使用している場合は、次の手順に従ってください。
 1. **tar -tvf <image_filename.tar>** UNIX コマンドを使用して、tar ファイルの内容を表示します。


```
switch% tar -tvf image_filename.tar
```
 2. **tar -xvf <image_filename.tar> <image_filename.bin>** UNIX コマンドを使用して、bin ファイルを特定し、抽出します。


```
switch% tar -xvf image_filename.tar image_filename.binx
ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.bin, 2928176 bytes, 5720 tape
blocks

x image_name.bin, 3970586 bytes, 7756 tape blocks
```
 3. **ls -l <image_filename.bin>** UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。


```
switch% ls -l image_filename.bin-rwxr-xr-x 1 bschuett eng 6365325 May 19
13:03
ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.bin

-rw-r--r-- 1 boba 3970586 Apr 21 12:00 image_name.bin
```
- ステップ 3** XMODEM プロトコルをサポートする端末エミュレーションソフトウェアを備えた PC を、スイッチのコンソール ポートに接続します。
- ステップ 4** エミュレーションソフトウェアの回線速度を 9600 ボーに設定します。
- ステップ 5** スイッチの電源コードを取り外します。

ステップ 6 [Express Setup] ボタンを押しながら、電源コードをスイッチに再接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、[Express Setup] ボタンを放します。ソフトウェアに関する数行分の情報と指示が表示されます。

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#
```

```
flash_init
load_helper
boot
```

ステップ 7 フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 8 コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 9 ヘルパー ファイルがある場合にはロードします。

```
switch: load_helper
```

ステップ 10 XMODEM プロトコルを使用して、ファイル転送を開始します。

```
switch: copy xmodem: flash:image_filename.bin
```

ステップ 11 XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに適切なコマンドを使用して、転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 12 新規にダウンロードされた Cisco IOS イメージを起動します。

```
switch:boot flash:image_filename.bin
```

ステップ 13 archive download-sw 特権 EXEC コマンドを使用して、スイッチにソフトウェア イメージをダウンロードします。

ステップ 14 reload 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。

ステップ 15 スイッチから、flash:image_filename.bin ファイルを削除します。

パスワードを忘れた場合の回復

パスワードを忘れた場合は、スイッチのパスワードを削除して新しく設定できます。

手順を開始する前に、次の点を確認してください。

- スイッチに物理的にアクセスできること。
- イネーブルになっていて装置に接続されていないスイッチ ポートが 1 つ以上あること。

スイッチのパスワードを削除して新しく設定するには、次の手順を実行します。

ステップ 1 SETUP LED がグリーンに点滅し、使用可能なスイッチ ダウンリンク ポートの LED がグリーンに点滅するまで、[Express Setup] ボタンを押し続けます。

PC またはラップトップの接続に使用できるスイッチ ダウンリンク ポートの空きがない場合は、いずれかのスイッチ ダウンリンク ポートから装置を接続解除します。もう一度、SETUP LED とポートの LED がグリーンに点滅するまで [Express Setup] ボタンを押し続けます。

- ステップ 2** LED がグリーンに点滅しているポートに、PC またはラップトップを接続します。
SETUP LED とスイッチ ダウンリンク ポートの LED が点滅を中止し、グリーンに点灯します。
- ステップ 3** [Express Setup] ボタンを押し続けます。SETUP LED が再度グリーンに点滅し始めます。SETUP LED がグリーンに点灯するまで (約 5 秒間)、ボタンを押したままにします。すぐに [Express Setup] ボタンを放します。
この手順によって、他の設定に影響を与えることなく、パスワードが削除されます。これで、パスワードを入力せずに、コンソール ポートまたはデバイス マネージャからスイッチにアクセスできるようになりました。
- ステップ 4** デバイス マネージャの [Express Setup] ウィンドウを使用するか、コマンドライン インターフェイスで **enable secret** グローバル コンフィギュレーション コマンドを使用して、新しいパスワードを入力します。

コマンドスイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) を使用すると、冗長コマンドスイッチグループを設定できます。詳細については、[第 6 章「スイッチのクラスタ化」](#) および [第 46 章「HSRP および VRRP の設定」](#) を参照してください。また、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』も参照してください。



(注) HSRP は、クラスタを冗長構成にする場合に適しています。

スタンバイ コマンドスイッチが未設定で、かつコマンドスイッチで電源故障などの障害が発生した場合には、メンバスイッチとの管理接続が失われるので、新しいコマンドスイッチに交換する必要があります。ただし、接続されているスイッチ間の接続は影響を受けません。また、メンバスイッチも通常どおりにパケットを転送します。メンバスイッチは、コンソール ポートを介してスタンドアロンのスイッチとして管理できます。また、IP アドレスが与えられている場合は、他の管理インターフェイスを使用して管理できます。

コマンド対応メンバスイッチまたは他のスイッチに IP アドレスを割り当て、コマンドスイッチのパスワードを書き留め、メンバスイッチと交換用コマンドスイッチ間の冗長接続が得られるようにクラスタを配置することにより、コマンドスイッチ障害に備えます。ここでは、故障したコマンドスイッチの交換方法を 2 通り紹介します。

- 「故障したコマンドスイッチをクラスタ メンバと交換する場合」(P.53-5)
- 「故障したコマンドスイッチを他のスイッチと交換する場合」(P.53-6)

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

コマンド対応スイッチについては、リリース ノートを参照してください。

故障したコマンドスイッチをクラスタメンバと交換する場合

故障したコマンドスイッチを同じクラスタ内のコマンド対応メンバスイッチに交換するには、次の手順に従ってください。

- ステップ 1** メンバスイッチからコマンドスイッチを外し、クラスタからコマンドスイッチを物理的に取り外します。
- ステップ 2** 故障したコマンドスイッチの代わりに新しいメンバスイッチを取り付け、コマンドスイッチとクラスタメンバ間の接続を復元します。
- ステップ 3** 新しいコマンドスイッチで CLI セッションを開始します。
CLI にはコンソールポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。コンソールポートの詳しい使用方法については、スイッチのハードウェアインストールガイドを参照してください。
- ステップ 4** スイッチプロンプトで、特権 EXEC モードを開始します。
Switch> **enable**
Switch#
- ステップ 5** 故障したコマンドスイッチのパスワードを入力します。
- ステップ 6** グローバルコンフィギュレーションモードを開始します。
Switch# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
- ステップ 7** クラスタからメンバスイッチを削除します。
Switch(config)# **no cluster commander-address**
- ステップ 8** 特権 EXEC モードに戻ります。
Switch(config)# **end**
Switch#
- ステップ 9** セットアッププログラムを使用して、スイッチの IP 情報を設定します。IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、Return を押します。
Switch# **setup**
--- System Configuration Dialog ---
Continue with configuration dialog?[yes/no]: **y**

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup?[yes/no]:
- ステップ 10** 最初のプロンプトに **Y** を入力します。
セットアッププログラムのプロンプトは、コマンドスイッチとして選択したメンバスイッチによって異なります。
Continue with configuration dialog?[yes/no]: **y**
または
Configuring global parameters:

このプロンプトが表示されなければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

ステップ 11 セットアッププログラムの質問に応答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字、メンバスイッチ上では 31 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (*n* は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されることに注意してください。

ステップ 12 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 13 スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** を押します (要求された場合)。

ステップ 14 クラスタに名前を指定し、**Return** を押します (要求された場合)。

クラスタ名には 1 ~ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 16 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。

情報に誤りがある場合には、**N** を入力し、**Return** を押して、ステップ 9 からやり直します。

ステップ 17 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 18 クラスタ メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンドスイッチを他のスイッチと交換する場合

故障したコマンドスイッチを、クラスタに組み込まれていないコマンド対応スイッチと交換する場合、次の手順に従ってください。

ステップ 1 故障したコマンドスイッチの代わりに新しいスイッチを取り付け、コマンドスイッチとクラスタ メンバ間の接続を復元します。

ステップ 2 新しいコマンドスイッチで CLI セッションを開始します。

CLI にはコンソールポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。コンソールポートの詳しい使用方法については、スイッチのハードウェア インストールガイドを参照してください。

ステップ 3 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 4 故障したコマンドスイッチのパスワードを入力します。

ステップ 5 セットアッププログラムを使用して、スイッチの IP 情報を設定します。

IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、**Return** を押します。

```
Switch# setup
    --- System Configuration Dialog ---
Continue with configuration dialog?[yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup?[yes/no]:
```

ステップ 6 最初のプロンプトに **Y** を入力します。

セットアッププログラムのプロンプトは、コマンドスイッチとして選択したスイッチによって異なります。

```
Continue with configuration dialog?[yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

ステップ 7 セットアッププログラムの質問に応答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (**n** は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されることに注意してください。

ステップ 8 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 9 スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** を押します (要求された場合)。

ステップ 10 クラスタに名前を指定し、**Return** を押します (要求された場合)。

クラスタ名には 1 ~ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 11 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 12 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。

情報に誤りがある場合には、**N** を入力し、**Return** を押して、ステップ 9 からやり直します。

ステップ 13 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 14 クラスタ メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

クラスタ メンバスイッチとの接続の回復

構成によっては、コマンドスイッチとメンバスイッチ間の接続を維持できない場合があります。メンバに対する管理接続を維持できなくなった場合で、かつ、メンバスイッチが正常にパケットを転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバスイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、ネットワーク ポートとして定義されたポートを介してコマンドスイッチに接続することはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバスイッチは、同じ管理 VLAN に所属するポートを介してコマンドスイッチに接続する必要があります。
- セキュア ポートを介してコマンドスイッチに接続するメンバスイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度 (10 Mbps、100 Mbps、および SFP モジュールポート以外の 1000 Mbps) およびデュプレックス (半二重または全二重) に関するスイッチの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。



(注)

接続先装置が自動ネゴシエーションを実行しない場合は、2つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

PoE スイッチ ポートのトラブルシューティング

ここでは、Power over Ethernet (PoE) ポートのトラブルシューティングについて説明します。

電力消失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電デバイス（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは **errdisable** ステートになることがあります。**errdisable** ステートから回復するには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。スイッチで自動回復を設定し、**errdisable** ステートから回復することもできます。**errdisable recovery cause loopback** および **errdisable recovery interval seconds** グローバル コンフィギュレーション コマンドは、指定した期間が経過した後自動的にインターフェイスを **errdisable** ステートから復帰させます。

このリリースのコマンド リファレンスに記載されている次のコマンドを使用すると、PoE ポート ステータスをモニタできます。

- **show controllers power inline** 特権 EXEC コマンド
- **show power inline** 特権 EXEC コマンド
- **debug ilpower** 特権 EXEC コマンド

不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが **errdisable** ステートになることがあります。ポートを **error-disabled** ステートから回復するには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM を備えています。スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを **errdisable** ステートにします。



(注)

セキュリティ エラー メッセージは、GBIC_SECURITY 機能を参照します。スイッチは、SFP モジュールをサポートしていますが、GBIC（ギガビット インターフェイス コンバータ）モジュールはサポートしていません。エラー メッセージ テキストは、GBIC インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、**errdisable** ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチは **errdisable** ステートからインターフェイスを復帰させ、操作を再試行します。**errdisable recovery** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

`show interfaces transceiver` 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンドリファレンスに記載された `show interfaces transceiver` コマンドの説明を参照してください。

ping の使用

ここでは、次の情報について説明します。

- 「ping の概要」(P.53-10)
- 「ping の実行」(P.53-10)

ping の概要

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答 (*hostname* が存在する) は、ネットワーク トラフィックにもよりますが、1 ~ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返ってきます。
- ホスト不明：ホストが存在しない場合、*unknown host* メッセージが返ってきます。
- 宛先に到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返ってきます。
- ネットワークまたはホストに到達不能：ルート テーブルにホストまたはネットワークに関するエントリがない場合、*network or host unreachable* メッセージが返ってきます。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネットワーク間でルーティングされるように IP ルーティングを設定する必要があります。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。IP ルーティングをイネーブルにする場合、または設定する必要がある場合は、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。

スイッチからネットワーク上の別のデバイスに ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
<code>ping ip host address</code>	IP またはホスト名やネットワーク アドレスを指定してリモートホストへ ping を実行します。



(注) ping コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 53-1 で、ping の文字出力について説明します。

表 53-1 ping の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス (デフォルトでは Ctrl+^ X) を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

レイヤ 2 traceroute の使用

ここでは、次の情報について説明します。

- 「レイヤ 2 traceroute の概要」 (P.53-12)
- 「使用上のガイドライン」 (P.53-12)
- 「物理パスの表示」 (P.53-13)

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内にあるスイッチの MAC アドレス テーブルを使用してパスを識別します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパスで検出すると、スイッチはレイヤ 2 トレースクエリを送信し続けてタイムアウトにしまいます。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

使用上のガイドライン

レイヤ 2 traceroute の使用上の注意事項を次に示します。

- Cisco Discovery Protocol (CDP) がネットワーク上のすべてのデバイスでイネーブルでなければなりません。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

レイヤ 2 traceroute をサポートするスイッチの一覧については、「[使用上のガイドライン](#)」(P.53-12) を参照してください。物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通るパスを識別できません。CDP をイネーブルにする場合の詳細については第 32 章「[CDP の設定](#)」を参照してください。

- スイッチは、**ping** 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別される最大ホップ カウントは 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラーメッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラーメッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して、IP アドレスを対応する MAC アドレスおよび VLAN ID に関連付けます。
 - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
 - ARP のエントリが存在しない場合、スイッチは ARP クエリを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。

- 複数のデバイスがハブを介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

物理パスの表示

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを表示できます。

- **traceroute mac** [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]
- **traceroute mac ip** {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]

詳細については、このリリースのコマンドリファレンスを参照してください。

IP traceroute の使用

ここでは、次の情報について説明します。

- 「IP traceroute の概要」 (P.53-13)
- 「IP traceroute の実行」 (P.53-14)

IP traceroute の概要

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。スイッチを **traceroute** の宛先とすると、スイッチは、**traceroute** の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、**traceroute** の出力に中間スイッチは表示されません。ただし、中間スイッチが、特定の packets をルーティングするマルチレイヤスイッチの場合、中間スイッチは **traceroute** の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの Time To Live (TTL; 存続可能時間) フィールドを使用して、ルータおよびサーバで特定のリターンメッセージが生成されるようにします。**traceroute** の実行は、UDP データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージプロトコル (ICMP) **time-to-live-exceeded** メッセージを送信元へ送信します。**traceroute** は、ICMP **time-to-live-exceeded** メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクストホップを識別するために、**traceroute** は TTL 値が 2 の UDP パケットを送信します。1 番目のルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番目のルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、**time-to-live-exceeded** メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、**traceroute** は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に **ICMP ポート到達不能エラー** を送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

IP traceroute の実行

ネットワーク上でパケットが通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip host	ネットワーク上でパケットが通過するパスを追跡します。



(注) **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

 0 172.2.52.1 0 msec 0 msec 4 msec
 1 172.2.1.203 12 msec 8 msec 0 msec
 2 171.9.16.6 4 msec 0 msec 0 msec
 3 171.9.4.5 0 msec 4 msec 0 msec
 4 171.9.121.34 0 msec 4 msec 4 msec
 5 171.9.15.9 120 msec 132 msec 128 msec
 6 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

ディスプレイには、送信される 3 つのプロープごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 53-2 **traceroute の出力表示文字**

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは **Ctrl+^ X**）を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから放し、その後 X キーを押します。

TDR の使用

ここでは、次の情報について説明します。

- 「[TDR の概要](#)」 (P.53-15)
- 「[TDR の実行および結果の表示](#)」 (P.53-15)

TDR の概要

Time Domain Reflector (TDR) 機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR 稼働時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュールポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行および結果の表示

TDR を実行する場合、**test cable-diagnostics tdr interface interface-id** 特権 EXEC コマンドを実行します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface interface-id** 特権 EXEC コマンドを実行します。出力フィールドの説明に関しては、このリリースに対応するコマンドリファレンスを参照してください。

debug コマンドの使用

ここでは、**debug** コマンドを使用してインターネットワーキングの問題を診断し、解決する方法について説明します。

- 「特定機能に関するデバッグのイネーブル化」(P.53-16)
- 「システム全体診断のイネーブル化」(P.53-17)
- 「デバッグおよびエラー メッセージ出力のリダイレクト」(P.53-17)



注意

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することを推奨します。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。



(注)

特定の **debug** コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

特定機能に関するデバッグのイネーブル化

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。たとえば、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) に対するデバッグをイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug span-session
```

スイッチは **no** 形式のコマンドが入力されるまで、出力を生成し続けます。

debug コマンドをイネーブルにしても、出力が表示されない場合は、次の状況が考えられます。

- モニタするトラフィック タイプを生成するようにスイッチが正しく設定されていない可能性があります。**show running-config** コマンドを使用して、設定を確認してください。
- スイッチが正しく設定されていても、デバッグがイネーブルである間にモニタすべきタイプのトラフィックを生成しないことがあります。デバッグする機能によっては、TCP/IP の **ping** コマンドなどを使用すると、ネットワーク トラフィックを生成できます。

SPAN のデバッグをディセーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

また、特権 EXEC モードで **undebug** 形式のコマンドを入力することもできます。

```
Switch# undebug span-session
```

各デバッグ オプションのステータスを表示するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体診断のイネーブル化

システム全体診断をイネーブルにするには、特権 EXEC モードで、次のコマンドを入力します。

```
Switch# debug all
```



注意

デバッグ出力は他のネットワークトラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

デバッグおよびエラーメッセージ出力のリダイレクト

ネットワークサーバはデフォルトで、**debug** コマンドおよびシステムエラーメッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、コンソールポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、および **syslog** サーバを実行している UNIX ホストがあります。**Syslog** フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。



(注)

デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。コンソールでメッセージロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージロギングを行うと、オーバーヘッドが小さくなります。**Syslog** サーバでメッセージロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システムメッセージロギングの詳細については、第 35 章「システムメッセージロギングの設定」を参照してください。

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポートマップ、ビットマップ、および出力側の情報が表示されます。



(注)

show platform forward コマンドの構文および使用方法の詳細については、このリリースに対応するスイッチコマンドリファレンスを参照してください。

このコマンドで出力される情報のほとんどは、主に、スイッチの特定用途向け集積回路 (ASIC) に関する詳細情報を使用するテクニカルサポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

show platform forward コマンドの使用

次に、VLAN 5 のポート 1 に入るパケットが、不明な MAC アドレスにアドレス指定されている場合の **show platform forward** コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべてのポートに対してフラッディングされなければなりません。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
  Lookup                Key-Used                Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000    01FFA  03000000
L2Local  80_00050002_00020002-00_00000000_00000000    00C71  0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

=====
Egress:Asic 2, switch 1
Output Packets:

-----
Packet 1
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000

Port      Vlan      SrcMac          DstMac          Cos  Dscpv
Gi1/1     0005     0001.0001.0001  0002.0002.0002

-----
Packet 2
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000

Port      Vlan      SrcMac          DstMac          Cos  Dscpv
Gi1/1     0005     0001.0001.0001  0002.0002.0002

-----
<output truncated>
-----
Packet 10
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2
Packet dropped due to failed DEJA_VU Check on Gi1/2
```

次に、VLAN 5 のポート 1 に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送信する場合の出力例を示します。パケットは、アドレスを学習したポートから転送する必要がありません。

```
Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
  Lookup                Key-Used                Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000    01FFA  03000000
L2Local  80_00050009_43A80145-00_00000000_00000000    00086  02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003
```

```

=====
Egress:Asic 3, switch 1
Output Packets:

-----
Packet 1
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000

Port          Vlan      SrcMac          DstMac      Cos  Dscp
interface-id  0005 0001.0001.0001  0009.43A8.0145

```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが不明である場合の出力例を示します。デフォルト ルートが設定されていないため、パケットはドロップされます。

```

Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
Lookup                Key-Used                Index-Hit  A-Data
InptACL 40_0D020202_0D010101-00_41000014_000A0000  01FFA  03000000
L3Local 00_00000000_00000000-90_00001400_0D020202  010F0  01880290
L3Scndr 12_0D020202_0D010101-00_40000014_000A0000  034E0  000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000

```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。パケットはルーティング テーブルの指定どおりに転送されます。

```

Switch# show platform forward gigabitethernet1/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
Lookup                Key-Used                Index-Hit  A-Data
InptACL 40_10010A05_0A010505-00_41000014_000A0000  01FFA  03000000
L3Local 00_00000000_00000000-90_00001400_10010A05  010F0  01880290
L3Scndr 12_10010A05_0A010505-00_40000014_000A0000  01D28  30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

```

```

=====
Egress:Asic 3, switch 1
Output Packets:

-----
Packet 1
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000  01FFE  03000000

Port          Vlan      SrcMac          DstMac      Cos  Dscp
Gi1/2        0007 XXXX.XXXX.0246  0009.43A8.0147

```

crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときに使用する情報が保存されています。スイッチは障害発生時にその情報をコンソールに書き込みます。スイッチは次の 2 つのタイプの crashinfo ファイルを作成します。

- 基本 crashinfo ファイル：障害発生後に Cisco IOS イメージを起動すると、スイッチが自動的にこのファイルを作成します。
- 拡張 crashinfo ファイル：システム障害の発生時に、スイッチがこのファイルを自動的に作成します。

基本 crashinfo ファイル

この基本ファイルに保存される情報は、障害が発生した Cisco IOS イメージの名前、バージョン、プロセッサ レジスタのリスト、および他のスイッチ特有の情報です。**show tech-support** 特権 EXEC コマンドを使用することによって、この情報をシスコのテクニカル サポート担当者に提供できます。

基本 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。

```
flash:/crashinfo/
```

ファイル名は `crashinfo_n` になります。`n` には一連の番号が入ります。

新しい crashinfo ファイルが作成されるたびに、前のシーケンス番号より大きいシーケンス番号が使用されるので、シーケンス番号が最大のファイルに、最新の障害が記述されています。タイムスタンプではなく、バージョン番号を使用するのは、スイッチにリアルタイム クロックが組み込まれていないからです。ファイル作成時にシステムが使用するファイル名を変更することはできません。ただし、ファイルが作成されてから、**rename** 特権 EXEC コマンドを使用して名前を変更することもできますが、**show tech-support** 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。**delete** 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示する場合は、**show tech-support** 特権 EXEC コマンドを使用します。**more** 特権 EXEC コマンド、**copy** 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、ファイルにアクセスすることもできます。

拡張 crashinfo ファイル

スイッチは、システム障害の発生時に拡張 crashinfo ファイルを作成します。拡張ファイルに保存される情報は、スイッチの障害となった原因を特定するのに役立つ追加情報です。このファイルに手動でアクセスし、**more** または **copy** 特権 EXEC コマンドを使用すると、シスコのテクニカル サポート担当者にこの情報を提供できます。

拡張 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。

```
flash:/crashinfo_ext/
```

ファイル名は `crashinfo_ext_n` になります。`n` には一連の番号が入ります。

no exception crashinfo グローバル コンフィギュレーション コマンドを使用すると、スイッチが拡張 crashinfo ファイルを作成しないように設定できます。

トラブルシューティング表

次の表は、Cisco.com のトラブルシューティング マニュアルから抽出した内容をまとめたものです。

- 「CPU 使用率に関するトラブルシューティング」(P-21)

CPU 使用率に関するトラブルシューティング

ここでは、CPU 利用の過重が原因で起こりうる問題の症状を一覧し、CPU 使用率の問題の検証方法について説明します。表 53-3 は、CPU 使用率に関する特定可能な主な問題を一覧しています。この表には、考えられる原因と修正措置が示してあり、それぞれに Cisco.com の『[Troubleshooting High CPU Utilization](#)』へのリンクが張られています。

CPU 使用率が高い場合に起こりうる症状

CPU 使用率が高すぎることで次の症状が発生する可能性があります。他の原因で発生する場合があります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求 (ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション) に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

レイヤ 3 スイッチの場合：

- ソフトウェアでルーティングされるパケットのドロップまたは遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

問題と原因の検証

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

■ トラブルシューティング表

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 53-3 CPU 使用率に関する問題のトラブルシューティング

問題のタイプ	原因	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。「 Analyzing Network Traffic 」を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。「 Debugging Active Processes 」を参照してください。

CPU 使用率の詳細および使用率の問題を解決する方法については、Cisco.com の『[Troubleshooting High CPU Utilization](#)』を参照してください。



APPENDIX **A**

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージの操作

この付録では、IE 3000 スイッチ フラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、およびスイッチへのソフトウェア イメージのアーカイブ（アップロードとダウンロード）方法について説明します。



(注) この章で使用しているコマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンド リファレンスおよび Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Configuration Fundamentals Command Reference, Release 12.2』を参照してください。

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェア イメージおよびコンフィギュレーション ファイルの管理に役立つ複数のコマンドも備えています。スイッチのデフォルトのフラッシュ ファイル システムは **flash:** です。

スイッチには、Cisco IOS ソフトウェアのイメージおよびコンフィギュレーション ファイルを格納する リムーバブル コンパクト フラッシュ カードがあります。コンパクト フラッシュ カードを取り外しても、Cisco IOS ソフトウェアのリロードが必要にならない限り、スイッチ動作は中断されません。ただし、コンパクト フラッシュ カードを取り外すと、フラッシュ ファイル システムにアクセスできなくなり、アクセスを試みるとエラー メッセージが生成されます。

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

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

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

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次の例を参照）。

```
Switch# show file systems

File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -          -          -     -     -
* 134086656 117346304  flash rw   flash:
      -          -          -     -     -
      -          -          -     -     system:
      -          -          -     -     tmpsys:
      524288      518334     nvram rw   nvram:
      -          -          -     -     xmodem:
      -          -          -     -     ymodem:
      -          -          -     -     null:
      -          -          -     -     tar:
      -          -          -     -     tftp:
      -          -          -     -     rcp:
      -          -          -     -     http:
      -          -          -     -     ftp:
      -          -          -     -     scp:
      -          -          -     -     https:
      -          -          -     -     cns:

Switch#
```

デフォルト ファイル システムの設定

表 A-1 show file systems フィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ（バイト単位）です。
Free(b)	ファイル システムの空きメモリ サイズ（バイト単位）です。
Type	ファイル システムのタイプです。 flash : ファイル システムはフラッシュ メモリ デバイス用です。 nvram : ファイル システムは NVRAM（不揮発性 RAM） デバイス用です。 opaque : ファイル システムはローカルに生成された <i>pseudo</i> ファイル システム（ <i>system</i> など）、または <i>brimux</i> などのダウンロード インターフェイスです。 unknown : ファイル システムのタイプは不明です。

表 A-1 show file systems フィールドの説明 (続き)

フィールド	値
Flags	<p>ファイル システムの権限です。</p> <p>ro : 読み取り専用です。</p> <p>rw : 読み取り / 書き込みです。</p> <p>wo : 書き込み専用です。</p>
Prefixes	<p>ファイル システムのエイリアスです。</p> <p>flash: : フラッシュ ファイル システムです。</p> <p>nvr : NVRAM です。</p> <p>null: : コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。</p> <p>rcp: : Remote Copy Protocol (RCP) ネットワーク サーバです。</p> <p>system: : 実行コンフィギュレーションを含むシステム メモリが格納されています。</p> <p>tftp: : TFTP ネットワーク サーバです。</p> <p>xmodem: : XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。</p> <p>ymodem: : YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。</p>

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd filesystem:** 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。

ファイル システムのファイルに関する情報を表示するには、表 A-2 に記載された特権 EXEC コマンドのいずれかを使用します。

表 A-2 ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [filesystem:][filename]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。

表 A-2 ファイルに関する情報を表示するためのコマンド（続き）

コマンド	説明
<code>show file information file-url</code>	特定のファイルに関する情報を表示します。
<code>show file descriptors</code>	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <i>filesystem:</i> には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。
ステップ2	<code>cd new_configs</code>	目的のディレクトリに変更します。 コマンド例では、 <i>new_configs</i> という名前のディレクトリに変更する方法を示します。
ステップ3	<code>pwd</code>	作業ディレクトリを表示します。

ディレクトリの作成および削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的
ステップ1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <i>filesystem:</i> には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。
ステップ2	<code>mkdir old_configs</code>	新しいディレクトリを作成します。 コマンド例では、 <i>old_configs</i> という名前のディレクトリの作成方法を示します。 ディレクトリ名では、大文字と小文字が区別されます。 スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ3	<code>dir filesystem:</code>	設定を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force/recursive filesystem:/file-url** 特権 EXEC コマンドを使用します。

名前指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。**file-url** には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

**注意**

ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy source-url destination-url** 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム (**xmodem:**、**ymodem:**) を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、**tftp:** があります。構文は次のとおりです。

- FTP : **ftp:**[[//username [:password]@location]/directory]/filename
- RCP : **rcp:**[[//username@location]/directory]/filename
- TFTP : **tftp:**[[//location]/directory]/filename

ローカルにある書き込み可能なファイル システムには **flash:** があります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ (たとえば、**copy flash: flash:** コマンドは無効)

コンフィギュレーション ファイルによる **copy** コマンドの具体的な使用例については、「[コンフィギュレーション ファイルの操作](#)」(P.A-8) を参照してください。

新しいバージョンをダウンロードするか、または既存のバージョンをアップロードして、ソフトウェア イメージをコピーするには、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドを使用します。詳細については、「[ソフトウェア イメージの操作](#)」(P.A-23) を参照してください。

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**force**] [**recursive**] [**filesystem:**]/**file-url** 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem: オプションを省略すると、**cd** コマンドで指定したデフォルトのデバイスが使用されます。**file-url** には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとする、削除の確認を求めると、プロンプトが表示されます。



注意

ファイルが削除された場合、その内容は回復できません。

次に、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次の項を参照）。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

```
archive tar/create destination-url flash:/file-url
```

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:
- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rpc:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、作成する tar ファイルです。

flash:/file-url には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。次のコマンドを実行すると、ローカルなフラッシュ デバイスのディレクトリ *new-configs* の内容が、172.20.10.30 にある TFTP サーバ上のファイル *saved.tar* に書き込まれます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table source-url

source-url には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:
- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rcp:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、表示する tar ファイルです。

tar ファイルの後ろにオプションのファイルまたはディレクトリ リストを指定して、表示するファイルを制限することもできます。リストを指定すると、リスト内のファイルのみが表示されます。何も指定しないと、すべてのファイルおよびディレクトリが表示されます。

次に、フラッシュ メモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/file.html (0 bytes)
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)
```

次の例では、*/html* ディレクトリおよびその内容だけを表示する方法を示します。

```
Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマンドを使用します。

archive tar/xtract source-url flash:/file-url [dir/file...]

source-url には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:
- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rcp:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、ファイルの抽出元の tar ファイルです。

flash:/file-url [dir/file...] には、tar ファイルが抽出されるローカル フラッシュ ファイル システムの場所を指定します。tar ファイルから抽出されるファイルまたはディレクトリのオプション リストを指定するには、*dir/file...* オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。ここでは、ローカル フラッシュ ファイル システムのルート ディレクトリに単に *new-configs* ディレクトリを抽出しています。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、**more [/ascii | /binary | /ebcdic] file-url** 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumbers
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説明します。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成するには、**setup** プログラムを使用するか、または **setup** 特権 EXEC コマンドを使用します。詳細については、第 4 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップコンフィギュレーションにコンフィギュレーション ファイルをコピー（ダウンロード）できます。次のいずれかの目的でこの操作が必要になります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーション ファイルを別のスイッチに使用するため。たとえば、ネットワークに別のスイッチを追加して、元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連部分を変更できます。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのスイッチに同じコンフィギュレーション コマンドをロードするため。

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（アップロード）するには、TFTP、FTP、または RCP を使用します。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておくと、後でサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要なコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソール ポートから接続することを推奨します。コンソールポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更によっては（スイッチの IP アドレスの変更やポートのディセーブル化など）、スイッチとの接続が切断される可能性があることにご注意ください。
- スイッチにパスワードが設定されていない場合は、**enable secret secret-password** グローバル コンフィギュレーション コマンドを使用して、パスワードを設定することを推奨します。



(注)

copy {ftp: | rcpx: | tftp:} system:running-config 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力した場合と同様に、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定の IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わせられた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成するには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーして (`copy {ftp: | rcp: | tftp:} nvram:startup-config` 特権 EXEC コマンドを使用)、スイッチを再起動します。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した後、`copy running-config startup-config` 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

-
- ステップ 1** スイッチからサーバに既存のコンフィギュレーションをコピーします。
- 詳細については、「[TFTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.A-11)、「[FTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.A-14)、または「[RCP によるコンフィギュレーション ファイルのダウンロード](#)」(P.A-17) を参照してください。
- ステップ 2** UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。
- ステップ 3** 目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出して、新しいファイルに保存します。
- ステップ 4** コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ (UNIX ワークステーションの場合は、通常は /tftpboot) にコピーします。
- ステップ 5** ファイルに関する権限が world-read に設定されていることを確認します。
-

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用してスイッチを設定したり、別のスイッチからダウンロードしたり、TFTP サーバからダウンロードできます。また、コンフィギュレーション ファイルを TFTP サーバにコピー（アップロード）して、格納できます。

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

`/etc/services` ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



(注) `/etc/inetd.conf` および `/etc/services` ファイルを変更した後に、`inetd` デーモンを再起動する必要があります。このデーモンを再起動するには、`inetd` プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) や **reboot** コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。 **ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 `/tftpboot`)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は **world-read** でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch filename** コマンドを入力します。`filename` は、サーバにアップロードするとき使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は **world-write** でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

- ステップ 1** コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。
- ステップ 2** 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (PA-11) を参照して、TFTP サーバが適切に設定されていることを確認します。

- ステップ 3** コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
- ステップ 4** TFTP サーバからコンフィギュレーション ファイルをダウンロードして、スイッチを設定します。TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy tftp:[[[//location]/directory]/filename] system:running-config**
- **copy tftp:[[[//location]/directory]/filename] nvram:startup-config**

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-config* からソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

- ステップ 1** 「[TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備](#)」(P.A-11)を参照して、TFTP サーバが適切に設定されていることを確認します。
- ステップ 2** コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
- ステップ 3** スwitchのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:[[[//location]/directory]/filename]**
- **copy nvram:startup-config tftp:[[[//location]/directory]/filename]**

TFTP サーバにファイルがアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)
- **ip ftp username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- **anonymous**

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password password** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した **username@switchname.domain** パスワード。変数 **username** は現在のセッションに関連付けられているユーザ名、**switchname** は設定されているホスト名、**domain** はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。 **ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。 **show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、 **ip ftp username username** グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、 **copy** コマンド内でユーザ名を指定します。

- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ3	configure terminal	スイッチ上で、グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ4	ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ5	ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	copy ftp:[[//[[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config または copy ftp:[[//[[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvram:startup-config	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-config* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-config* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
```

```

Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101

```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

ステップ	コマンド	目的
ステップ1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ4	ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ5	ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	copy system:running-config ftp:[[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] または copy nvram:startup-config ftp:[[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定場所に格納します。

次に、実行コンフィギュレーション ファイル *switch2-config* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```

Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#

```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```

Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end

```

```
Switch# copy nvram:startup-config ftp:
Remote host[ ]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチ間でコンフィギュレーション ファイルをダウンロード、アップロード、およびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の `copy` コマンドは、リモート システム上の `rsh` サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは `rsh` をサポートするサーバにアクセスするだけですみます（ほとんどの UNIX システムは `rsh` をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- `copy` コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、`username` コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。`ping` コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。`show users` 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に `ip rcmd remote-username username` グローバル コン

フィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、そのユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の **.rhosts** ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の **.rhosts** ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

ステップ	コマンド	目的
ステップ1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-16) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	copy rcp:[[[/[username@]location]/directory]/filename] system:running-config または copy rcp:[[[/[username@]location]/directory]/filename] nvrám:startup-config	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-config* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
```

```

Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101

```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-config* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```

Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101

```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

ステップ	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-16) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	ip rcmd remote-username <i>username</i>	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy system:running-config rcp:[[[[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] または copy nvram:startup-config rcp:[[[[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、実行コンフィギュレーション ファイル *switch2-config* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```

Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101

```

```
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュレーションを使用しないでスイッチを再起動すると、スイッチはセットアッププログラムを開始し、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションを消去するには、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。



注意

削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、**delete flash:filename** 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。**file prompt** コマンドの詳細については、『Cisco IOS Command Reference for Release 12.2』を参照してください。



注意

削除されたファイルは復元できません。

コンフィギュレーションの交換またはロールバック

コンフィギュレーション交換およびロールバック機能を使用すると、実行コンフィギュレーションと保存されている任意の Cisco IOS コンフィギュレーション ファイルを交換できます。ロールバック機能を使用すると以前のコンフィギュレーションに戻すことができます。

コンフィギュレーションの交換およびロールバックの概要

コンフィギュレーションのアーカイブ

コンフィギュレーション アーカイブは、コンフィギュレーション ファイルのアーカイブを保管、構成、管理するメカニズムです。**configure replace** 特権 EXEC コマンドを使用すると、コンフィギュレーション ロールバック機能が向上します。または、**copy running-config destination-url** 特権 EXEC コマンドを使用して実行コンフィギュレーションのコピーを保存し、交換ファイルをローカルまたはリモートで保存することができます。ただし、この方法ではファイルの自動管理を行うことはできません。コンフィギュレーション交換およびロールバック機能を使用すれば、実行コンフィギュレーションのコピーを自動的にコンフィギュレーション アーカイブに保存できます。

archive config 特権 EXEC コマンドを使用して、コンフィギュレーションをコンフィギュレーション アーカイブに保存します。その際は標準のディレクトリとファイル名のプレフィックスが使用され、連続ファイルを保存するたびにバージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。このときのバージョン番号は1つずつ大きくなります。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。保存したファイル数が指定数に達した場合は、次の新しいファイルを保存するときに最も古いファイルが自動的に削除されます。**show archive** 特権 EXEC コマンドを使用すると、コンフィギュレーション アーカイブに保存されたすべてのコンフィギュレーション ファイルを表示できます。

Cisco IOS コンフィギュレーション アーカイブでは、コンフィギュレーション ファイルを保存し、**configure replace** コマンドで使用します。ファイル システムは、FTP、HTTP、RCP、TFTP のいずれかです。

コンフィギュレーションの交換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存されている任意のコンフィギュレーション ファイルを交換できます。**configure replace** コマンドを入力すると実行コンフィギュレーションと指定した交換コンフィギュレーションが比較され、コンフィギュレーションの差分が生成されます。生成された差分がコンフィギュレーションの交換に使用されます。コンフィギュレーション交換は、通常 3 回以下のパスで完了します。ループを防ぐために 6 回以上のパスが実行されることはありません。

copy source-url running-config 特権 EXEC コマンドを使用すると、保存されているコンフィギュレーション ファイルが実行コンフィギュレーションに保存できます。このコマンドを **configure replace target-url** 特権コマンドの代わりに使用する場合は、次のような違いがある点に注意してください。

- **copy source-url running-config** コマンドはマージ動作であり、コピー元ファイルと実行コンフィギュレーションのコマンドをすべて保存します。このコマンドでは、コピー元ファイルに実行コンフィギュレーションのコマンドがない場合でも実行コンフィギュレーションのコマンドを削除しません。**configure replace target-url** コマンドの場合は、交換先のファイルに実行コンフィギュレーションのコマンドがない場合は実行コンフィギュレーションから削除し、実行コンフィギュレーションにないコマンドがある場合はそのコマンドを追加します。
- **copy source-url running-config** コマンドのコピー元ファイルとして、部分コンフィギュレーション ファイルを使用できます。**configure replace target-url** コマンドの交換ファイルとして、完全なコンフィギュレーション ファイルを使用する必要があります。

コンフィギュレーションのロールバック

configure replace コマンドを使用して、前回コンフィギュレーションを保存した後で行った変更をロールバックさせることもできます。コンフィギュレーション ロールバック機能では、コンフィギュレーションを特定の変更時点に戻すのではなく、保存されているコンフィギュレーション ファイルに基づいて特定のコンフィギュレーションに戻します。

コンフィギュレーション ロールバック機能を利用する場合は、コンフィギュレーションを変更する前に実行コンフィギュレーションを保存する必要があります。その後、コンフィギュレーションを変更した後で **configure replace target-url** コマンドを使用し、保存したコンフィギュレーション ファイルを使って変更をロールバックします。

保存されている任意のファイルをロールバック コンフィギュレーションとして指定できます。一部のロールバック モデルと同様、ロールバック回数は無制限です。

設定時の注意事項

コンフィギュレーション交換およびロールバックを設定し実行する場合は、次の注意事項に従ってください。

- スイッチのメモリの空き容量が、2つのコンフィギュレーション ファイル（実行コンフィギュレーションと保存されている交換コンフィギュレーション）の合計容量よりも大きいことを確認します。スイッチのメモリ容量の方が小さい場合、コンフィギュレーション交換は実行されません。
- また、スイッチにコンフィギュレーション交換やロールバック コンフィギュレーション コマンドが実行できるほどの空き容量があることも確認してください。
- ネットワーク デバイスの物理コンポーネント（物理インターフェイスなど）に関連するコンフィギュレーション コマンドを実行コンフィギュレーションに追加または削除することはできません。
 - インターフェイスがデバイス上に物理的に存在する場合、コンフィギュレーション交換を行っても実行コンフィギュレーションから **interface interface-id** コマンド行を削除することはできません。
 - インターフェイスがデバイス上に物理的に存在しない場合、**interface interface-id** コマンド行を実行コンフィギュレーションに追加することはできません。
- **configure replace** コマンドを使用する場合、保存されているコンフィギュレーションを実行コンフィギュレーションの交換コンフィギュレーション ファイルとして指定する必要があります。交換ファイルは Cisco IOS デバイスによって生成された完全なコンフィギュレーションであることが必要です（たとえば **copy running-config destination-url** コマンドで生成したコンフィギュレーション）。



(注) 交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、コンフィギュレーション ロールバックを行うときに大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ3	path url	コンフィギュレーション アーカイブに、ファイルのディレクトリとファイル名プレフィックスを指定します。

■ コンフィギュレーション ファイルの操作

	コマンド	目的
ステップ4	maximum number	(任意) コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を指定します。 <i>number</i> : コンフィギュレーション アーカイブでの実行コンフィギュレーション ファイルの最大数。有効な値は 1 ~ 14 で、デフォルトは 10 です。 (注) このコマンドを使用する前に path アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブのファイルのディレクトリとファイル名プレフィックスを指定しておく必要があります。
ステップ5	time-period minutes	(任意) コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 <i>minutes</i> : コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブを自動保存する間隔を、分単位で指定します。
ステップ6	end	特権 EXEC モードに戻ります。
ステップ7	show running-config	設定を確認します。
ステップ8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

■ コンフィギュレーション 交換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	archive config	(任意) 実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 (注) path アーカイブ コンフィギュレーション コマンドを入力してから、このコマンドを実行します。
ステップ2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3		実行コンフィギュレーションに必要な変更を行います。
ステップ4	exit	特権 EXEC モードに戻ります。

コマンド	目的
ステップ5 configure replace target-url [list] [force] [time seconds] [nolock]	<p>実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換します。</p> <p>target-url : 保存されているコンフィギュレーション ファイルの URL (ファイル システムからアクセス可能)。実行コンフィギュレーション と交換するファイルで、ステップ 2 で archive config 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなどです。</p> <p>list : コンフィギュレーション 交換動作のパスごとにソフトウェア パーサーによって適用されるコマンド エントリのリストを表示します。パスの合計数も表示されます。</p> <p>force : 実行コンフィギュレーション ファイルと指定した保存済みコンフィギュレーション ファイルの交換を確認なしで実行します。</p> <p>time seconds : configure confirm コマンドを入力して実行コンフィギュレーション ファイルとの交換を確認するまでの時間を秒単位で指定します。指定時間内に configure confirm コマンドを入力しない場合、コンフィギュレーション 交換動作が自動的に停止します (つまり、実行コンフィギュレーション ファイルは configure replace コマンドを入力する以前に存在していたコンフィギュレーション に保存されます)。</p> <p>(注) time seconds コマンドライン オプションを使用する前に、コンフィギュレーション アーカイブをイネーブルにしておく必要があります。</p> <p>nolock : コンフィギュレーション 交換動作時に他のユーザが実行コンフィギュレーション を変更できないようにする実行コンフィギュレーション ファイルのロックをディセーブルにします。</p>
ステップ6 configure confirm	<p>(任意) 実行コンフィギュレーション と保存されているコンフィギュレーション ファイルとの交換を確認します。</p> <p>(注) このコマンドは、time seconds キーワードと configure replace コマンドの引数が指定されている場合にだけ使用します。</p>
ステップ7 copy running-config startup-config	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフトウェアを格納するソフトウェア イメージ ファイルをアーカイブ (ダウンロードおよびアップロード) する方法を示します。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

スイッチ ソフトウェアをアップグレードするには、TFTP、FTP、または RCP サーバからスイッチ イメージ ファイルをダウンロードします。TFTP サーバへアクセスできない場合、Web ブラウザ (HTTP) で PC またはワークステーションへ直接ソフトウェア イメージ ファイルをダウンロードします。次にデバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードします。TFTP サーバまたは Web ブラウザ (HTTP) を使用したスイッチのアップグレードについては、リリース ノートを参照してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保存したりできます。

バックアップのために、スイッチ イメージ ファイルを TFTP、FTP、または RCP サーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。



(注)

ソフトウェア イメージ、およびサポートされているアップグレード パスの一覧については、スイッチに付属のリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ (flash:) に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼働しているソフトウェア バージョンを参照できます。画面上で、System image file is... で始まる行を調べます。この行は、イメージが格納されているフラッシュ メモリ内のディレクトリ名を示します。

dir filesystem: 特権 EXEC コマンドを使用して、フラッシュ メモリに格納されている他のソフトウェア イメージのディレクトリ名を調べることもできます。**archive download-sw /directory** 特権 EXEC コマンドを使用して、各 tar ファイルに対してパス全体を指定する代わりに、ディレクトリの後ろにダウンロードする tar ファイルまたは tar ファイルのリストを続けることでディレクトリの指定を 1 回で済ませることが可能です。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- tar ファイルの内容を表形式で示す *info* ファイル
- Cisco IOS イメージや Web 管理用ファイルなど、他のイメージおよびファイルが格納された 1 つまたは複数のサブディレクトリ

次に、*info* ファイルに格納された情報の一部の例を示します。表 A-3 に、この情報の詳細を示します。

```
system_type:0x00000000:image-name
  image_family:xxxx
  stacking_number:x
  info_end:
version_suffix:xxxx
  version_directory:image-name
  image_system_type_id:0x00000000
  image_name:image-nameB.bin
  ios_image_file_size:6398464
  total_image_file_size:8133632
  image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
  image_family:xxxx
  stacking_number:x
```

```
board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
info_end:
```



(注) `stacking_number` フィールドは無視してください。このフィールドはスイッチに適用されません。

表 A-3 info ファイルの説明

フィールド	説明
<code>version_suffix</code>	Cisco IOS イメージ バージョン スtring のサフィックスを指定します。
<code>version_directory</code>	Cisco IOS イメージおよび HTML サブディレクトリがインストールされているディレクトリを指定します。
<code>image_name</code>	<code>tar</code> ファイル内の Cisco IOS イメージの名前を指定します。
<code>ios_image_file_size</code>	<code>tar</code> ファイル内の Cisco IOS イメージのサイズを指定します。このサイズは、Cisco IOS イメージのみを保持するために必要なフラッシュ メモリ サイズの概算値です。
<code>total_image_file_size</code>	<code>tar</code> ファイル内のすべてのイメージ (Cisco IOS イメージおよび Web 管理ファイル) のサイズを指定します。このサイズは、これらのファイルを保持するために必要なフラッシュ メモリ サイズの概算値です。
<code>image_feature</code>	イメージの主な機能に関する説明です。
<code>image_min_dram</code>	このイメージを実行するために必要な DRAM の最小サイズを指定します。
<code>image_family</code>	ソフトウェアをインストールできる製品ファミリに関する説明です。

TFTP によるイメージ ファイルのコピー

TFTP サーバからスイッチ イメージをダウンロードしたり、スイッチから TFTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードするために使用できます。



(注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、`copy` 特権 EXEC コマンドまたは `archive tar` 特権 EXEC コマンドではなく、`archive download-sw` および `archive upload-sw` 特権 EXEC コマンドを使用することを推奨します。

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

/etc/services ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



(注) /etc/inetd.conf および /etc/services ファイルを変更した後に、inetd デーモンを再起動する必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) や **reboot** コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 /tftpboot)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、touch filename コマンドを入力します。filename は、イメージをサーバにアップロードするとき使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 3 を実行します。現在のイメージを保存するには、ステップ 3 へ進みます。

コマンド	目的
ステップ 1	イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します (「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.A-25) を参照)。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

コマンド	目的
ステップ3 archive download-sw /overwrite /reload tftp:[[/location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> • /overwrite オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //location には、TFTP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ4 archive download-sw/leave-old-sw/reload tftp:[[/location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 <ul style="list-style-type: none"> • /leave-old-sw オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //location には、TFTP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (flash:) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は (**/leave-old-sw** キーワードを指定した場合は)、**delete /force/recursive filesystem:/file-url** 特権 EXEC コマンドを入力して、そのイメージを削除できます。**filesystem** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。**file-url** には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

TFTP によるイメージ ファイルのアップロード

スイッチから TFTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	TFTP サーバが適切に設定されていることを確認します（「 TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備 」(P.A-25) を参照）。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	<p>archive upload-sw tftp:[[/location]/directory]/image-name.tar</p> <p>現在稼働中のスイッチ イメージを TFTP サーバにアップロードします。</p> <ul style="list-style-type: none"> <i>//location</i> には、TFTP サーバの IP アドレスを指定します。 <i>/directory/image-name.tar</i> には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。<i>image-name.tar</i> は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのコピー

FTP サーバからスイッチ イメージをダウンロードしたり、スイッチから FTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



(注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)。
- **ip ftp username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- **anonymous**

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password password** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した **username@switchname.domain** パスワード。変数 **username** は現在のセッションに関連付けられているユーザ名、**switchname** は設定されているホスト名、**domain** はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username username** グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセ

スしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。ユーザ名をこの処理のためだけに指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンド内でユーザ名を指定します。

- イメージ ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～7 の手順を実行します。現在のイメージを保存するには、ステップ 7 へ進みません。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4	ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	archive download-sw /overwrite /reload ftp:[[/username[:password]@location]/directory]/ image-name.tar	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> /overwrite オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 //username[:password] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。 @location には、FTP サーバの IP アドレスを指定します。 directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

コマンド	目的
ステップ 8 archive download-sw/leave-old-sw/reload ftp:[[/username[:password]@location]/directory]/ image-name.tar	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 <ul style="list-style-type: none"> • /leave-old-sw オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //username[:password] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。 • @location には、FTP サーバの IP アドレスを指定します。 • directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注)

フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (**flash:**) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、**BOOT** 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は (**/leave-old-sw** キーワードを指定した場合は)、**delete /force/recursive filesystem:/file-url** 特権 EXEC コマンドを入力して、そのイメージを削除できます。**filesystem** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。**file-url** には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのアップロード

スイッチから FTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4	ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	archive upload-sw ftp:[[/[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>image-name.tar</i>	現在稼働中のスイッチ イメージを FTP サーバにアップロードします。 <ul style="list-style-type: none"> • <i>//username:password</i> には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。 • <i>@location</i> には、FTP サーバの IP アドレスを指定します。 • <i>/directory/image-name.tar</i> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 <i>image-name.tar</i> は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのコピー

RCP サーバからスイッチ イメージをダウンロードしたり、スイッチから RCP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の **copy** コマンドは、リモート システム上の **rsh** サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは **rsh** をサポートするサーバにアクセスするだけですみます（ほとんどの UNIX システムは **rsh** をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが **Telnet** を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として **Telnet** ユーザ名がスイッチ ソフトウェアによって送信されます。
- スwitch のホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、**rsh** がサポートされていることを確認します。
- スwitch に RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スウィッチとサーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の **.rhosts** ファイルにエントリを追加する必要があります。

たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の **.rhosts** ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 6 の手順を実行します。現在のイメージを保存するには、ステップ 6 へ進みません。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-16) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。

コマンド	目的
ステップ6 archive download-sw /overwrite /reload rcp:[[//[username@]location]/directory]/image-name.tar]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> • /overwrite オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //username には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • @location には、RCP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ7 archive download-sw/leave-old-sw/reload rcp:[[//[username@]location]/directory]/image-name.tar]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 <ul style="list-style-type: none"> • /leave-old-sw オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //username には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • @location には、RCP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

`/leave-old-sw` を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、稼働中のイメージを保存しようとする、ダウンロードプロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (`flash:`) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete /force/recursive filesystem:file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。`filesystem` には、システム ボードのフラッシュ デバイスを指定する場合は `flash:` を使用します。`file-url` には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが既存のイメージでインストールされている場合に限り、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.A-16) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	<code>ip rcmd remote-username username</code>	(任意) リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	archive upload-sw rep:[[[//[username@]location]/directory]/image-name.tar]	<p>現在稼働中のスイッチ イメージを RCP サーバにアップロードします。</p> <ul style="list-style-type: none"> • <i>//username</i> には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • <i>@location</i> には、RCP サーバの IP アドレスを指定します。 • <i>/directory]/image-name.tar</i> には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • <i>image-name.tar</i> は、サーバに保存するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージファイルが構築されます。これらのファイルがアップロードされた後に、アップロードアルゴリズムによって tar ファイル形式が作成されます。



注意

ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

■ ソフトウェア イメージの操作



APPENDIX **B**

Cisco IOS Release 15.0(1)SE でサポートされていないコマンド

この付録では、IE 3000 スイッチのプロンプトに疑問符 (?) を入力したときに表示されるコマンドライン インターフェイス (CLI) コマンドの中で、まだテストされていないため、またはスイッチのハードウェアの制限により、このリリースではサポートされていないコマンドをいくつか示します。このリストは完全ではありません。これらのサポートされていないコマンドは、ソフトウェア機能およびコマンド モード別に掲載されています。

- 「アクセス コントロール リスト」 (P.B-2)
- 「アーカイブ コマンド」 (P.B-2)
- 「ブートローダ コマンド」 (P.B-3)
- 「組み込まれている Event Manager」 (P.B-3)
- 「Embedded Syslog Manager」 (P.B-4)
- 「debug コマンド」 (P.B-4)
- 「フォールバック ブリッジング」 (P.B-4)
- 「ハイ アベイラビリティ」 (P.B-6)
- 「HSRP」 (P.B-6)
- 「IGMP スヌーピング コマンド」 (P.B-7)
- 「インターフェイス コマンド」 (P.B-7)
- 「IP マルチキャスト ルーティング」 (P.B-7)
- 「IP マルチキャスト ルーティング」 (P.B-7)
- 「IP ユニキャスト ルーティング」 (P.B-9)
- 「IPv6」 (P.B-11)
- 「レイヤ 3」 (P.B-11)
- 「MAC アドレス コマンド」 (P.B-13)
- 「Miscellaneous」 (P.B-14)
- 「MSDP」 (P.B-14)
- 「マルチキャスト」 (P.B-15)
- 「NetFlow コマンド」 (P.B-15)
- 「NAT コマンド」 (P.B-16)
- 「QoS」 (P.B-16)

- 「RADIUS」 (P.B-16)
- 「SNMP」 (P.B-17)
- 「SNMPv3」 (P.B-17)
- 「スパニングツリー」 (P.B-17)
- 「VLAN」 (P.B-17)

アクセスコントロール リスト

サポートされていない特権 EXEC コマンド

```
access-enable [host] [timeout minutes]
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
clear access-template [access-list-number | name] [dynamic-name] [source] [destination]
show access-lists rate-limit [destination]
show accounting
show ip accounting [checkpoint] [output-packets | access violations]
show ip cache [prefix-mask] [type number]
```

サポートされていないグローバル コンフィギュレーション コマンド

```
access-list rate-limit acl-index {precedence | mask prec-mask}
access-list dynamic extended
```

サポートされていないルートマップ コンフィギュレーション コマンド

```
match ip address prefix-list prefix-list-name [prefix-list-name...]
```

アーカイブ コマンド

サポートされていない特権 EXEC コマンド

```
archive config
logging persistent
show archive config
show archive log
```

ARP コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
arp ip-address hardware-address smds
arp ip-address hardware-address srp-a
arp ip-address hardware-address srp-b
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
arp probe
ip probe proxy
```

ブートローダ コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
boot buffersize
```

組み込まれている Event Manager

サポートされていない特権 EXEC コマンド

```
event manager update user policy [policy-filename | group [group name expression] ] | repository [url location]
```

次のコマンドのパラメータはサポートされていません。

```
event manager run [policy name] |<parameter1>|... <parameter15>|
```

サポートされていないグローバル コンフィギュレーション コマンド

```
no event manager directory user repository [url location ]
event manager applet [applet-name] maxrun
```

サポートされていないアプレット コンフィギュレーション モードのコマンド

```
no event interface name [interface-name] parameter [counter-name] entry-val [entry counter value]
entry-op {gt|ge|eq|ne|lt|le} [entry-type {increment | rate | value}] [exit-val [exit value] exit-op
{gt|ge|eq|ne|lt|le} exit-type { increment | rate | value}] [average-factor <average-factor-value>]
no trigger
tag
```

Embedded Syslog Manager

サポートされていないグローバル コンフィギュレーション コマンド

すべて

サポートされていない特権 EXEC コマンド

すべて

debug コマンド

サポートされていない特権 EXEC コマンド

```
debug platform cli-redirection main
debug platform configuration
```

フォールバック ブリッジング

サポートされていない特権 EXEC コマンド

```
clear bridge [bridge-group] multicast [router-ports | groups | counts] [group-address] [interface-unit]
[counts]
clear vlan statistics
show bridge [bridge-group] circuit-group [circuit-group] [src-mac-address] [dst-mac-address]
show bridge [bridge-group] multicast [router-ports | groups] [group-address]
show bridge vlan
show interfaces crb
```

```
show interfaces {ethernet | fastethernet} [interface | slot/port] irb
show subscriber-policy range
```

サポートされていないグローバル コンフィギュレーション コマンド

```
bridge bridge-group acquire
bridge bridge-group address mac-address {forward | discard} [interface-id]
bridge bridge-group aging-time seconds
bridge bridge-group bitswap_l3_addresses
bridge bridge-group bridge ip
bridge bridge-group circuit-group circuit-group pause milliseconds
bridge bridge-group circuit-group circuit-group source-based
bridge cmf
bridge crb
bridge bridge-group domain domain-name
bridge irb
bridge bridge-group mac-address-table limit number
bridge bridge-group multicast-source
bridge bridge-group protocol dec
bridge bridge-group route protocol
bridge bridge-group subscriber policy policy
subscriber-policy policy [[no | default] packet [permit | deny]]
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
bridge-group bridge-group cbus-bridging
bridge-group bridge-group circuit-group circuit-number
bridge-group bridge-group input-address-list access-list-number
bridge-group bridge-group input-lat-service-deny group-list
bridge-group bridge-group input-lat-service-permit group-list
bridge-group bridge-group input-lsap-list access-list-number
bridge-group bridge-group input-pattern-list access-list-number
bridge-group bridge-group input-type-list access-list-number
bridge-group bridge-group lat-compression
bridge-group bridge-group output-address-list access-list-number
bridge-group bridge-group output-lat-service-deny group-list
bridge-group bridge-group output-lat-service-permit group-list
bridge-group bridge-group output-lsap-list access-list-number
```

bridge-group *bridge-group* **output-pattern-list** *access-list-number*
bridge-group *bridge-group* **output-type-list** *access-list-number*
bridge-group *bridge-group* **sse**
bridge-group *bridge-group* **subscriber-loop-control**
bridge-group *bridge-group* **subscriber-trunk**
bridge *bridge-group* **lat-service-filtering**
frame-relay map bridge *dci* **broadcast**
interface bvi *bridge-group*
x25 map bridge *x.121-address* **broadcast** [*options-keywords*]

ハイ アベイラビリティ

サポートされていない SSO 認識 HSRP コマンド

すべて

HSRP

サポートされていないグローバル コンフィギュレーション コマンド

interface Async
interface BVI
interface Dialer
interface Group-Async
interface Lex
interface Multilink
interface Virtual-Template
interface Virtual-Tokenring

サポートされていないインターフェイス コンフィギュレーション コマンド

mtu
standby mac-refresh *seconds*
standby use-bia

IGMP スヌーピング コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
ip igmp snooping tcn
```

インターフェイス コマンド

サポートされていない特権 EXEC コマンド

```
show interfaces [interface-id | vlan vlan-id] [crb | fair-queue | irb | mac-accounting | precedence | irb  
| random-detect | rate-limit | shape]
```

サポートされていないグローバル コンフィギュレーション コマンド

```
interface tunnel
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
transmit-interface type number
```

IP マルチキャスト ルーティング

サポートされていない特権 EXEC コマンド

```
clear ip rtp header-compression [type number]
```

debug ip packet コマンドを実行すると、スイッチの CPU で受信されるパケットが表示されます。ハードウェアでスイッチングされるパケットは表示されません。

debug ip mcache コマンドは、スイッチの CPU で受信されるパケットに影響します。ハードウェアでスイッチングされるパケットは表示されません。

debug ip mpacket [detail] [access-list-number [group-name-or-address]] コマンドは、スイッチの CPU で受信されるパケットにだけ影響します。ほとんどのマルチキャスト パケットはハードウェアでスイッチングされるため、このコマンドは、このルートでパケットが CPU に転送されることがわかっている場合だけ使用してください。

```
debug ip pim atm
```

```
show frame-relay ip rtp header-compression [interface type number]
```

show ip mcache コマンドを実行すると、スイッチの CPU に送信されるパケット用のキャッシュ内のエントリが表示されます。ほとんどのマルチキャスト パケットは CPU で処理されずにハードウェアでスイッチングされるため、このコマンドを使用しても、マルチキャスト パケット情報は表示されません。

show ip mpacket コマンドはサポートされていますが、スイッチの CPU で受信されるパケットに対してだけ効果があります。ルートがハードウェアによってスイッチングされる場合、このコマンドは効果がありません。CPU はパケットを受信せず、パケット情報が表示されないためです。

show ip pim vc [*group-address* | *name*] [*type number*]

show ip rtp header-compression [*type number*] [*detail*]

サポートされていないグローバル コンフィギュレーション コマンド

ip multicast-routing [*vrf vrf-name*]

ip pim accept-rp {*address* | **auto-rp**} [*group-access-list-number*]

ip pim message-interval *seconds*

サポートされていないインターフェイス コンフィギュレーション コマンド

frame-relay ip rtp header-compression [*active* | *passive*]

frame-relay map ip *ip-address dlc* [**broadcast**] **compress**

frame-relay map ip *ip-address dlc* **rtp header-compression** [*active* | *passive*]

ip igmp helper-address *ip-address*

ip multicast helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*}
extended-access-list-number

ip multicast rate-limit {*in* | *out*} [*video* | *whiteboard*] [*group-list access-list*] [*source-list access-list*]
kbps

ip multicast ttl-threshold *ttl-value* (代わりに **ip multicast boundary** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用)

ip multicast use-functional

ip pim minimum-vc-rate *pps*

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count *number*

ip rtp compression-connections *number*

ip rtp header-compression [*passive*]

IP SLA

サポートされていない MPLS ヘルス モニタ コマンド

すべて

サポートされていないイーサネット ゲートキーパー登録コマンド

すべて

サポートされていない VoIP コール セットアップ プローブ コマンド

すべて

IP ユニキャスト ルーティング

サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド

```
clear ip accounting [checkpoint]
clear ip bgp address flap-statistics
clear ip bgp prefix-list
debug ip cef stats
show cef [drop | not-cef-switched]
show ip accounting [checkpoint] [output-packets | access-violations]
show ip bgp dampened-paths
show ip bgp inconsistent-as
show ip bgp regexp regular expression
show ip prefix-list regular expression
```

サポートされていないグローバル コンフィギュレーション コマンド

```
ip accounting precedence {input | output}
ip accounting-list ip-address wildcard
ip accounting-transits count
ip cef traffic-statistics [load-interval seconds] [update-rate seconds]
ip flow-aggregation
ip flow-cache
ip flow-export
ip gratuitous-arps
ip local
ip prefix-list
ip reflexive-list
router egp
router-isis
```

```

router iso-igrp
router mobile
router odr
router static

```

サポートされていないインターフェイス コンフィギュレーション コマンド

```

ip accounting
ip load-sharing [per-packet]
ip mtu bytes
ip ospf dead-interval minimal hello-multiplier multiplier
ip verify
ip unnumbered type number
すべての ip security コマンド

```

サポートされていない BGP ルータ コンフィギュレーション コマンド

```

address-family vpv4
default-information originate
neighbor advertise-map
neighbor allowas-in
neighbor default-originate
neighbor description
network backdoor
table-map

```

サポートされていない VPN コンフィギュレーション コマンド

すべて

サポートされていないルート マップ コマンド

```

ポリシーベース ルーティング (PBR) の match route-type
set as-path {tag | prepend as-path-string}
set automatic-tag
set dampening half-life reuse suppress max-suppress-time
set default interface interface-id [interface-id.....]
set interface interface-id [interface-id.....]
set ip default next-hop ip-address [ip-address.....]

```

set ip destination *ip-address mask*
set ip next-hop verify-availability
set ip precedence *value*
set ip qos-group
set metric-type internal
set origin
set metric-type internal
set tag *tag-value*

IPv6

IPv4/v6 トンネリング コマンド

すべて

レイヤ 3

BGP

次の機能のすべてのコマンド

- ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポート
- グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート
- 名前付き拡張コミュニティ リストに対する BGP サポート
- 拡張コミュニティ リストのシーケンス エントリに対する BGP サポート
- TTL セキュリティ チェックに対する BGP サポート
- BGP ルートマップ ポリシー リストのサポート
- BGP ネクスト ホップ伝播
- BGP ポリシー アカウンティング
- BGP ポリシー アカウンティング出力インターフェイス アカウンティング
- BGP リンク帯域幅
- BGP ハイブリッド CLI サポート
- BGP コスト コミュニティ
- BGP ダイナミック アップデート ピアグループ
- BGP 条件付きルート インジェクション
- ピア テンプレートをを使用した BGP 設定
- AS パス アクセス リスト 500 番までに対する BGP サポートの拡張

その他のサポートされていない BGP コマンド

address-family l2vpn

address-family vpv4

bgp-policyclear bgp nsapaddress-family nsap

clear bgp nsap dampening

clear bgp nsap external

clear bgp nsap flap-statistics

clear bgp nsap peer-group

clear ip bgp ipv6

clear ip bgp l2vpn

clear ip bgp vpv4

clear ip bgp vpv6

ha-mode graceful-restartip extcommunity-list redistribute (BGP から ISO IS-IS)

ip policy-listredistribute (ISO IS-IS から BGP)

match extcommunity

neighbor ha-mode graceful-restart

neighbor sooredistribute dvmrp

neighbor ttl-securityset extcommunity

set extcommunity cost

show bgp nsap

show bgp nsap community

show bgp nsap community-list

show bgp nsap dampening

show bgp nsap dampened-paths

show bgp nsap filter-list

show bgp nsap flap-statistics

show bgp nsap inconsistent-as

show bgp nsap neighbors

show bgp nsap paths

show bgp nsap quote-regexp

show bgp nsap regexp

show bgp nsap summary

show ip bgp ipv4 multicast

show ip bgp ipv4 multicast summary

show ip bgp l2vpn

show ip bgp vpv4

show ip extcommunity-list

```
show ip policy-list
```

OSPF

```
area sham-link
ignore lsa mospf
nsf ietf
nsf ietf helper disable
nsf ietf helper strict-lsa-checking
show ip ospf sham-links
```

VRF 認識 AAA

すべて

MAC アドレス コマンド

サポートされていない特権 EXEC コマンド

```
show mac-address-table
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table multicast
show mac-address-table notification
show mac-address-table static
show mac-address-table vlan
show mac address-table multicast
```



(注) VLAN (仮想 LAN) のレイヤ 2 マルチキャスト アドレス テーブル エントリを表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。

サポートされていないグローバル コンフィギュレーション コマンド

```
mac-address-table aging-time
mac-address-table notification
```

mac-address-table static

Miscellaneous

サポートされていないユーザ EXEC コマンド

verify

サポートされていない特権 EXEC コマンド

file verify auto

remote コマンド

show cable-diagnostics prbs

test cable-diagnostics prbs

サポートされていないグローバル コンフィギュレーション コマンド

errdisable recovery cause unicast flood

l2protocol-tunnel global drop-threshold

memory reserve critical

service compress-config

track *object-number* rtr

stack-mac persistent timer

logging discriminator

MSDP

サポートされていない特権 EXEC コマンド

show access-expression

show exception

show location

show pm LINE

show smf [*interface-id*]

show subscriber-policy [*policy-number*]

show template [*template-name*]

サポートされていないグローバル コンフィギュレーション コマンド

`ip msdp default-peer ip-address | name [prefix-list list]` (BGP/MBGP がサポートされていないため、このコマンドの代わりに、`ip msdp peer` コマンドを使用してください)

マルチキャスト

サポートされていない BiDirectional PIM (bidir-PIM; 双方向 PIM) コマンド

すべて

サポートされていないマルチキャスト ルーティング マネージャ コマンド

すべて

サポートされていない IP マルチキャスト レート制限コマンド

すべて

サポートされていない UDLR コマンド

すべて

サポートされていない GRE でのマルチキャスト コマンド

すべて

NetFlow コマンド

サポートされていないグローバル コンフィギュレーション コマンド

`ip flow-aggregation cache`

`ip flow-cache entries`

`ip flow-export`

NAT コマンド

サポートされていない特権 EXEC コマンド

```
show ip nat statistics
show ip nat translations
```

QoS

サポートされていないグローバル コンフィギュレーション コマンド

```
priority-list
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
priority-group
rate-limit
```

サポートされていないポリシーマップ コンフィギュレーション コマンド

```
class class-default (class-default が class-map-name の場合)
```

RADIUS

サポートされていないグローバル コンフィギュレーション コマンド

```
aaa nas port extended
aaa authentication feature default enable
aaa authentication feature default line
aaa nas port extended
radius-server attribute nas-port
radius-server configure
radius-server extended-portnames
```

SNMP

サポートされていないグローバル コンフィギュレーション コマンド

`snmp-server enable informs`

`snmp-server ifindex persist`

`logging discriminator discr-name [[facility] [mnemonics] [msg-body] {drops string | includes string}] [severity {drops sev-num | includes sev-num}] [rate-limit msglimit]`

`logging buffered discriminator`

SNMPv3

サポートされていない 3DES 暗号化コマンド

すべて

スパンニングツリー

サポートされていないグローバル コンフィギュレーション コマンド

`spanning-tree pathcost method {long | short}`

サポートされていないインターフェイス コンフィギュレーション コマンド

`spanning-tree stack-port`

VLAN

サポートされていないグローバル コンフィギュレーション コマンド

`vlan internal allocation policy {ascending | descending}`

サポートされていないユーザ EXEC コマンド

`show running-config vlan`

`show vlan ifindex`

vlan database

サポートされていない VLAN データベース コマンド

vtp

vlan

VTP

サポートされていない特権 EXEC コマンド

vtp {password *password* | pruning | version *number*}

このコマンドは、vtp グローバル コンフィギュレーション コマンドに置き換えられています。



INDEX

A

AAA ダウン ポリシー、NAC レイヤ 2 IP 検証 [1-11](#)

ABR [41-26](#)

access-class コマンド [38-20](#)

ACE

IP [38-2](#)

QoS と [39-8](#)

イーサネット [38-2](#)

定義済み [38-2](#)

ACL

ACE [38-2](#)

IP

暗黙の拒否 [38-10, 38-15, 38-17](#)

暗黙のマスク [38-10](#)

一致基準 [38-7](#)

作成する [38-7](#)

フラグメントと QoS の注意事項 [39-34](#)

未定義 [38-22](#)

IPv4

一致基準 [38-7](#)

インターフェイスに対して適用する [38-20](#)

数 [38-8](#)

作成する [38-7](#)

端末回線、設定する [38-20](#)

名前付き [38-15](#)

非サポート機能 [38-7](#)

IPv6

一致条件 [45-3](#)

インターフェイスへの適用 [45-7](#)

サポートしない機能 [45-3](#)

サポート対象 [45-2](#)

制限 [45-3](#)

設定 [45-3, 45-4](#)

名前付き [45-3](#)

表示 [45-8](#)

他の機能との相互作用 [45-4](#)

優先 [45-2](#)

MAC 拡張 [38-28, 39-46](#)

QoS [39-8, 39-44](#)

QoS クラス マップごとの数 [39-34](#)

QoS のトラフィックを分類する [39-44](#)

VLAN マップ

設定時の注意事項 [38-32](#)

設定する [38-31](#)

VLAN マップでルータ ACL を使用する [38-38](#)

エントリの並べ替え [38-15](#)

拡張 IP、QoS 分類を設定する [39-45](#)

拡張 IPv4

一致基準 [38-7](#)

作成する [38-10](#)

コメント [38-19](#)

コンパイルする [38-24](#)

サポート [1-9](#)

サポートされない機能、IPv6 [45-3](#)

サポートされるタイプ [38-2](#)

時間範囲 [38-17](#)

照合 [38-7, 38-21, 45-3](#)

すべてのキーワード [38-13](#)

定義済み [38-1, 38-7](#)

適用

IPv6 インターフェイス [45-7](#)

適用する

QoS に対する [39-8](#)

インターフェイスに対する [38-20, 45-7](#)

時間範囲 [38-17](#)

スイッチドパケットでの [38-39](#)
 ブリッジドパケットでの [38-40](#)
 マルチキャストパケットでの [38-41](#)
 ルーテッドパケットでの [38-41](#)

名前 [45-4](#)

名前付き、IPv4 [38-15](#)

名前付き、IPv6 [45-3](#)

ハードウェアでのサポート [38-22](#)

ハードウェアとソフトウェアの処理 [38-22](#)

非サポート機能、IPv4 [38-7](#)

標準 IP、QoS 分類を設定する [39-44](#)

標準 IPv4

一致基準 [38-7](#)

作成する [38-9](#)

ポート [38-2, 45-1](#)

ホスト キーワード [38-13](#)

モニタリング [38-43, 45-8](#)

優先順位 [38-2](#)

ルータ [38-2, 45-1](#)

ルータ ACL と VLAN マップの設定時の注意事項 [38-38](#)

例 [38-24, 39-44](#)

レイヤ 4 情報 [38-39](#)

ロギング メッセージ [38-8](#)

AC (コマンドスイッチ) [6-11](#)

ARP

カプセル化 [41-10](#)

スタティック キャッシュの設定 [41-9](#)

設定 [41-9](#)

定義済み [1-5, 7-24, 41-9](#)

テーブル

アドレス解決 [7-24](#)

管理する [7-24](#)

ASBR [41-26](#)

AS パス フィルタ、BGP [41-55](#)

Auto-MDIX

設定する [14-21](#)

説明 [14-20](#)

Auto Smartports マクロ

表示 [15-5](#)

B

BackboneFast

イネーブルにする [23-14](#)

説明 [23-5](#)

ディセーブルにする [23-15](#)

Berkeley r-tool の置換 [11-57](#)

BGP

CIDR [41-61](#)

clear コマンド [41-64](#)

Multi-VRF CE によるルーティングセッション [41-85](#)

show コマンド [41-64](#)

イネーブル化 [41-48](#)

コミュニティ フィルタリング [41-57](#)

サポート [1-13](#)

集約アドレス [41-61](#)

集約ルート、設定 [41-61](#)

スーパーネット [41-61](#)

セッションのリセット [41-51](#)

説明 [41-44](#)

デフォルト設定 [41-45](#)

ネイバー、タイプ [41-48](#)

ネイバーの設定 [41-59](#)

バージョン 4 [41-45](#)

パス選択 [41-52](#)

ピア、設定 [41-59](#)

プレフィックス フィルタリング [41-56](#)

マルチパス サポート [41-52](#)

モニタリング [41-64](#)

ルーティング ドメイン連合 [41-62](#)

ルート ダンプニング [41-63](#)

ルート マップ [41-54](#)

ルート リフレクタ [41-62](#)

BPDU

errdisable ステート [23-2](#)

RSTP 形式 [22-12](#)

- フィルタリング [23-3](#)
 - BPDU ガード
 - イネーブルにする [23-11](#)
 - サポート [1-7](#)
 - 説明 [23-2](#)
 - ディセーブルにする [23-12](#)
 - BPDU フィルタリング
 - イネーブルにする [23-12](#)
 - サポート [1-7](#)
 - 説明 [23-3](#)
 - ディセーブルにする [23-13](#)
 - broadcast storm-control コマンド [29-4](#)
-
- C**
- Catalyst 6000 スイッチ
 - 認証の互換性 [12-8](#)
 - CA トラストポイント
 - 設定する [11-54](#)
 - 定義済み [11-52](#)
 - CDP
 - LLDP での定義 [31-1](#)
 - アップデート [32-3](#)
 - イネーブルとディセーブル
 - インターフェイス上で [32-4](#)
 - スイッチ上で [32-4](#)
 - 概要 [32-1](#)
 - サポート [1-5](#)
 - 信頼境界と [39-40](#)
 - スイッチ クラスタでの自動検出 [6-4](#)
 - 設定 [32-2](#)
 - 説明 [32-1](#)
 - 送信タイマーとホールドタイム、設定する [32-3](#)
 - デフォルト設定 [32-2](#)
 - モニタリング [32-5](#)
 - ルーティング デバイスをディセーブルにする [32-4](#)
 - レイヤ 2 プロトコル トンネリング [20-8](#)
 - CEF
 - IPv6 [42-20](#)
 - イネーブル化 [41-91](#)
 - 定義 [41-90](#)
 - CE デバイス内の Multi-VRF
 - 「Multi-VRF CE」を参照
 - CGMP
 - IGMP スヌーピング ラーニング方式としての [28-9](#)
 - 概要 [50-9](#)
 - キャッシュに格納されたグループ エントリのクリア [50-64](#)
 - サーバ サポート機能 [50-9](#)
 - サーバ サポートのイネーブル化 [50-46](#)
 - スイッチ サポート [1-3](#)
 - マルチキャスト グループに加入する [28-3](#)
 - CIDR [41-61](#)
 - CipherSuite [11-53](#)
 - Cisco 7960 IP 電話 [18-1](#)
 - Cisco Discovery Protocol
 - 「CDP」を参照
 - Cisco Group Management Protocol
 - 「CGMP」を参照
 - Cisco IOS DHCP サーバ
 - 「DHCP、Cisco IOS DHCP サーバ データベース」を参照
 - Cisco IOS File System
 - 「IFS」を参照
 - Cisco IOS IP SLA [47-1](#)
 - Cisco Secure ACS
 - ダウンロード可能な ACL の属性と値のペア [12-20](#)
 - リダイレクト URL の属性と値のペア [12-20](#)
 - Cisco Secure ACS 設定ガイド [12-60](#)
 - CiscoWorks 2000 [1-4, 36-4](#)
 - CISP [12-30](#)
 - CIST リージョナル ルート
 - 「MSTP」を参照
 - CIST ルート
 - 「MSTP」を参照
 - CLI
 - エラー メッセージ [2-5](#)
 - クラスタを管理する [6-16](#)

コマンド出力のフィルタリング 2-10
 コマンドの no 形式と default 形式 2-4
 コマンドの短縮形 2-4
 コマンド モード 2-1
 コンフィギュレーション ロギング 2-5
 説明 1-4
 ヘルプを使用する 2-3
 編集機能

イネーブルとディセーブル 2-7
 キーストロック編集 2-8
 ラップされた行 2-9

履歴

コマンドを呼び出す 2-6
 説明 2-6
 ディセーブルにする 2-7
 バッファ サイズを変更する 2-6

Client Information Signalling Protocol

「CISP」を参照

CLNS

「ISO CLNS」を参照

CNS 1-4

Configuration Engine

イベント サービス 5-3
 コンフィギュレーション サービス 5-2
 設定 ID、デバイス ID、ホスト名 5-3
 説明 5-1

管理機能 1-4

組み込みエージェント

イベント エージェントをイネーブルにする 5-7
 自動設定をイネーブルにする 5-7
 設定エージェントをイネーブルにする 5-9
 説明 5-5

CoA 要求コマンド 11-25

config.text 4-18

configure terminal コマンド 14-9

config-vlan モード 2-2

CoS

オーバーライド プライオリティ 18-6
 信頼のプライオリティ 18-6

CoS/DSCP マップ、QoS での 39-63
 CoS 出力キューしきい値マップ、QoS の 39-19
 CPU 使用率、トラブルシューティング 53-21
 crashinfo ファイル 53-20
 Customer Edge デバイス 41-76

D

DAACL

「ダウンロード可能 ACL」を参照

Default Router Preference

「DRP」を参照

default コマンド 2-4

description コマンド 14-21

DHCP

Cisco IOS サーバ データベース

設定する 26-15
 説明 26-7
 デフォルト設定 26-9

IPv6 用 DHCP

「DHCPv6」を参照

イネーブルにする

リレー エージェント 26-11

DHCP Option 82

回線 ID サブオプション 26-5

概要 26-4

設定時の注意事項 26-10

デフォルト設定 26-9

転送アドレス、指定する 26-11

パケット形式、サブオプション

回線 ID 26-5

リモート ID 26-5

表示する 26-16

ヘルパー アドレス 26-11

リモート ID サブオプション 26-5

DHCPv6

DHCPv6 サーバ機能をイネーブルにする 42-17

クライアント機能をイネーブルにする 42-19

サポート 1-14

- 設定ガイドライン [42-16](#)
- 説明 [42-6](#)
- デフォルト設定 [42-16](#)
- DHCP オブジェクト トラッキング、プライマリ インターフェイスの設定 [48-11](#)
- DHCP サーバ ポートベースのアドレス割り当て
 - イネーブルにする [26-29](#)
 - サポート [1-5](#)
 - 設定時の注意事項 [26-29](#)
 - 説明 [26-28](#)
 - デフォルト設定 [26-29](#)
 - 表示する [26-31](#)
 - 予約アドレス [26-30](#)
- DHCP スヌーピング
 - Option 82 データ挿入 [26-4](#)
 - 信頼済みインターフェイス [26-3](#)
 - 設定時の注意事項 [26-10](#)
 - デフォルト設定 [26-9](#)
 - バインディング データベース
 - 「DHCP スヌーピング バインディング データベース」を参照
 - バインディング テーブルの表示 [26-16](#)
 - 非信頼インターフェイス [26-3](#)
 - 非信頼パケット形式エッジ スイッチを受信する [26-3, 26-13](#)
 - 非信頼メッセージ [26-2](#)
 - プライベート VLAN の [26-14](#)
 - メッセージ交換プロセス [26-4](#)
- DHCP スヌーピング バインディング データベース
 - イネーブルにする [26-15](#)
 - エージェント統計情報をクリアする [26-16](#)
 - エントリ [26-7](#)
 - 削除する
 - データベース エージェント [26-16](#)
 - バインディング [26-16](#)
 - バインディング ファイル [26-16](#)
 - 設定時の注意事項 [26-10](#)
 - 設定する [26-15](#)
 - 説明 [26-7](#)
 - データベースを更新する [26-16](#)
 - デフォルト設定 [26-9](#)
 - バインディング [26-7](#)
 - バインディング ファイル
 - 形式 [26-8](#)
 - 場所 [26-7](#)
 - バインディングを追加する [26-15](#)
 - 表示
 - ステータスと統計情報 [26-16](#)
 - バインディング エントリ [26-16](#)
 - 表示する [26-16](#)
 - リセットする
 - タイムアウト値 [26-16](#)
 - 遅延値 [26-16](#)
- DHCP スヌーピング バインディング テーブル
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP バインディング データベース
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP バインディング テーブル
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP ベースの自動設定
 - BOOTP との関係 [4-4](#)
 - 概要 [4-4](#)
 - クライアント要求メッセージの交換 [4-4](#)
 - サポート [1-5](#)
 - 設定する
 - DNS [4-8](#)
 - TFTP サーバ [4-8](#)
 - クライアント側 [4-4](#)
 - サーバ側 [4-7](#)
 - リレー デバイス [4-9](#)
 - リース オプション
 - IP アドレス情報 [4-7](#)
 - 設定ファイルを受信する [4-7](#)
 - リレー サポート [1-5, 1-14](#)
 - 例 [4-10](#)
- DHCP ベースの自動設定とイメージ アップデート
 - 概要 [4-5 ~ 4-6](#)

- 設定する [4-12 ~ 4-15](#)
 - distributed-list コマンド [41-103](#)
 - DNS
 - DHCP ベースの自動設定と [4-8](#)
 - IPv6 での [42-4](#)
 - 概要 [7-8](#)
 - サポート [1-5](#)
 - 設定する [7-9](#)
 - 設定を表示する [7-10](#)
 - デフォルト設定 [7-9](#)
 - DNS ベースの SSM マッピング [50-19, 50-21](#)
 - dot1q-tunnel switchport モード [16-16](#)
 - DRP
 - IPv6 [42-4](#)
 - サポート [1-14](#)
 - 設定 [42-14](#)
 - 説明 [42-4](#)
 - DSCP [1-12, 39-2](#)
 - DSCP/CoS マップ、QoS での [39-66](#)
 - DSCP/DSCP 変換マップ、QoS での [39-67](#)
[1-12, 39-2](#)
 - DSCP 出力キューしきい値マップ、QoS の [39-19](#)
 - DSCP 透過性 [39-41](#)
 - DTP [1-8, 16-15](#)
 - DUAL 有限状態マシン、EIGRP [41-36](#)
 - DVMRP
 - DVMRP ルータへの PIM ドメインの接続 [50-53](#)
 - mrinfo 要求、応答 [50-55](#)
 - 概要 [50-9](#)
 - サポート [1-14](#)
 - 自動サマライズ
 - サマリー アドレスの設定 [50-60](#)
 - ディセーブル化 [50-62](#)
 - 相互運用性
 - Cisco IOS ソフトウェアとの [50-9](#)
 - シスコ デバイスとの [50-51](#)
 - 送信元配信ツリー、構築 [50-9](#)
 - トンネル
 - 設定 [50-53](#)
 - ネイバー情報の表示 [50-55](#)
 - ネイバー
 - 情報の表示 [50-55](#)
 - デフォルト ルートのアドバタイズ [50-55](#)
 - 非ブルーニングとのピアリングの禁止 [50-58](#)
 - 非ブルーニングの拒否 [50-57](#)
 - プローブ メッセージによる検出 [50-51](#)
 - ユニキャスト ルーティングのイネーブル化 [50-56](#)
 - ルーティング テーブル [50-9](#)
 - ルート
 - MBONE に入る個数の制限 [50-59](#)
 - Syslog メッセージのしきい値の変更 [50-59](#)
 - 削除 [50-64](#)
 - すべてのアドバタイズ [50-62](#)
 - ネイバーへのデフォルト ルートのアドバタイズ [50-55](#)
 - 表示 [50-64](#)
 - メトリック オフセットの追加 [50-62](#)
 - 優先度 [50-62](#)
 - ユニキャスト ルート アドバタイズの制限 [50-51](#)
 - レポート メッセージで取得された DVMRP ルートのキャッシュへの格納 [50-56](#)
 - dynamic auto trunking モード [16-16](#)
 - dynamic desirable trunking モード [16-16](#)
 - Dynamic Host Configuration Protocol
 - 「DHCP ベースの自動設定」を参照
 - Dynamic Trunking Protocol (ダイナミック トランキング プロトコル)
 - 「DTP」を参照
-
- ## E
- EBGP [41-43](#)
 - 「EBGP」を参照
 - EIGRP
 - インターフェイス パラメータ、設定 [41-40](#)
 - コンポーネント [41-36](#)
 - スタブ ルーティング [41-42](#)
 - 設定 [41-39](#)

- 定義 [41-35](#)
 - デフォルト設定 [41-37](#)
 - 認証 [41-40](#)
 - モニタリング [41-43](#)
 - ELIN ロケーション [31-3](#)
 - enable secret password [11-4](#)
 - errdisable ステート、BPDU [23-2](#)
 - EtherChannel
 - IEEE 802.3ad、説明 [40-6](#)
 - LACP
 - システム プライオリティ [40-20](#)
 - ステータスを表示する [40-21](#)
 - 説明 [40-6](#)
 - ポート プライオリティ [40-20](#)
 - 他の機能との相互動作 [40-7](#)
 - ホットスタンバイ ポート [40-19](#)
 - モード [40-6](#)
 - PAGP
 - Catalyst 1900 との互換性 [40-18](#)
 - 学習方式とプライオリティの設定 [40-18](#)
 - 仮想スイッチとの相互動作 [40-5](#)
 - サポート [1-3](#)
 - 集約ポート ラーナー [40-18](#)
 - ステータスを表示する [40-21](#)
 - 説明 [40-4](#)
 - デュアルアクションの検出での [40-5](#)
 - 他の機能との相互動作 [40-6](#)
 - モード [40-5](#)
 - サポート [1-3](#)
 - 自動作成 [40-4, 40-6](#)
 - ステータスを表示する [40-21](#)
 - 設定時の注意事項 [40-10](#)
 - 設定する
 - レイヤ 2 インターフェイス [40-11](#)
 - レイヤ 3 物理インターフェイス [40-15](#)
 - レイヤ 3 ポートチャンネル論理インターフェイス [40-14](#)
 - 説明 [40-2](#)
 - 相互動作
 - STP での [40-10](#)
 - VLAN での [40-11](#)
 - チャンネル グループ
 - 番号付け [40-3](#)
 - 物理インターフェイスと論理インターフェイスのバインディング [40-3](#)
 - デフォルト設定 [40-10](#)
 - 転送方式 [40-7, 40-17](#)
 - ポート グループ [14-6](#)
 - ポートチャンネル インターフェイス
 - 説明 [40-3](#)
 - レイヤ 3 インターフェイス [41-4](#)
 - ロード バランシング [40-7, 40-17](#)
 - 論理インターフェイス、説明 [40-3](#)
 - EtherChannel ガード
 - イネーブルにする [23-15](#)
 - 説明 [23-7](#)
 - ディセーブルにする [23-15](#)
 - EUI [42-3](#)
 - Express Setup [1-2](#)
 - 「スタートアップ ガイド」も参照
 - Extensible Authentication Protocol over LAN [12-1](#)
-
- ## F
- fa0 インターフェイス [1-6](#)
 - FCS Bit Error Rate アラーム
 - 設定 [3-10](#)
 - 定義 [3-3](#)
 - FCS エラー ヒステリシスしきい値 [3-2](#)
 - FIB [41-91](#)
 - Flex Link
 - VLAN [25-2](#)
 - VLAN ロード バランシングを設定する [25-11](#)
 - 設定 [25-9](#)
 - 設定時の注意事項 [25-8](#)
 - 説明 [25-1](#)
 - デフォルト設定 [25-8](#)
 - モニタリング [25-15](#)

優先 VLAN の設定 [25-12](#)

リンク ロード バランシング [25-2](#)

Flex Link マルチキャスト高速コンバージェンス [25-3](#)

FTP

イメージ ファイル

アップロードする [A-32](#)

サーバを準備する [A-29](#)

ダウンロードする [A-30](#)

古いイメージを削除する [A-31](#)

設定ファイル

アップロードする [A-15](#)

概要 [A-13](#)

サーバを準備する [A-13](#)

ダウンロードする [A-14](#)

コマンド スイッチの冗長性 [1-7](#)

自動クラスタ回復 [6-13](#)

設定 [46-4](#)

タイマー [46-11](#)

注意事項 [46-6](#)

定義 [46-1](#)

デフォルト設定 [46-5](#)

トラッキング [46-8](#)

認証ストリング [46-11](#)

プライオリティ [46-8](#)

モニタリング [46-13](#)

ルーティングの冗長性 [1-13](#)

「クラスタ」、「クラスタ スタンバイ グループ」、「スタンバイ コマンド スイッチ」も参照

HTTP over SSL

「HTTPS」を参照

HTTPS [11-51](#)

自己署名証明書 [11-52](#)

設定する [11-55](#)

HTTP セキュア サーバ [11-51](#)

G

get-bulk-request オペレーション [36-3](#)

get-next-request オペレーション [36-3, 36-4](#)

get-request オペレーション [36-3, 36-4](#)

get-response オペレーション [36-3](#)

GUI

「デバイス マネージャと Network Assistant」を参照

H

hello タイム

MSTP [22-23](#)

STP [21-21](#)

Hot Standby Router Protocol (ホットスタンバイ ルータ プロトコル)

「HSRP」を参照

HP OpenView [1-4](#)

HSRP

ICMP リダイレクト メッセージのサポート [46-12](#)

オブジェクト トラッキング [48-7](#)

概要 [46-1](#)

クラスタ グループにバインド [46-12](#)

クラスタ スタンバイ グループの考慮事項 [6-12](#)

I

IBGP

「IBGP」を参照

IBPG [41-43](#)

ICMP

IPv6 [42-4](#)

traceroute と [53-13](#)

サポート [1-13](#)

時間超過メッセージ [53-13](#)

到達不能と ACL [38-22](#)

到達不能メッセージ [38-21](#)

到達不能メッセージおよび IPv6 [45-4](#)

リダイレクト メッセージ [41-12](#)

ICMP ping

概要 [53-10](#)

実行する [53-10](#)

ICMP Router Discovery Protocol

- 「IRDP」を参照
- ICMPv6 [42-4](#)
- ICMP エコー動作
 - IP SLA [47-11](#)
 - 設定する [47-12](#)
- IDS 装置
 - 入力 RSPAN と [30-20](#)
 - 入力 SPAN と [30-13](#)
- IEEE 802.1D
 - 「STP」を参照
- IEEE 802.1p [18-1](#)
- IEEE 802.1Q
 - カプセル化 [16-15](#)
 - 設定の制限 [16-17](#)
 - その他の機能を含むトンネル ポート [20-6](#)
 - タグなしトラフィック用ネイティブ VLAN [16-22](#)
 - トランク ポートと [14-3](#)
 - トンネリング
 - 説明 [20-1](#)
 - デフォルト [20-4](#)
 - 他の機能との互換性 [20-6](#)
- IEEE 802.1s
 - 「MSTP」を参照
- IEEE 802.1w
 - 「RSTP」を参照
- IEEE 802.1x
 - 「ポートベース認証」を参照
- IEEE 802.3ad
 - 「EtherChannel」を参照
- IEEE 802.3x フロー制御 [14-19](#)
- ifIndex 値、SNMP [36-6](#)
- IFS [1-5](#)
- IGMP
 - join メッセージ [28-3](#)
 - 概要 [50-3](#)
 - キャッシュ エントリの削除 [50-64](#)
 - クエリー [28-4](#)
 - グループの表示 [50-64](#)
 - グループへのアクセスの制御 [50-42](#)
 - 高速スイッチング [50-46](#)
 - サポート [1-3](#)
 - サポートされるバージョン [28-3](#)
 - スイッチの設定
 - グループのメンバーとして [50-41](#)
 - 静的に接続されたメンバー [50-45](#)
 - 設定可能な脱退タイマー
 - イネーブルにする [28-11](#)
 - 説明 [28-6](#)
 - 脱退処理、イネーブルにする [28-11, 44-9](#)
 - デフォルト設定 [50-41](#)
 - バージョン 1
 - 説明 [50-3](#)
 - バージョン 2 への変更 [50-43](#)
 - バージョン 2
 - クエリー タイムアウト値 [50-44](#)
 - グループのプルーニング [50-45](#)
 - 最大クエリー応答時間値 [50-45](#)
 - 説明 [50-4](#)
 - バージョン 1 への変更 [50-43](#)
 - フラッディングしたマルチキャスト トラフィック
 - インターフェイス上でディセーブルにする [28-14](#)
 - クエリー送信要求 [28-13](#)
 - グローバルな脱退 [28-13](#)
 - 時間の長さを制御する [28-12](#)
 - フラッディング モードから回復する [28-13](#)
 - ホストクエリー インターバル、変更 [50-43](#)
 - マルチキャスト グループから脱退する [28-5](#)
 - マルチキャスト グループに加入する [28-3](#)
 - マルチキャストの到達可能性 [50-41](#)
 - レポート抑制
 - 説明 [28-6](#)
 - ディセーブルにする [28-16, 44-11](#)
- IGMP グループ
 - 最大番号を設定する [28-28](#)
 - フィルタリングを設定する [28-29](#)
- IGMP スヌーピング
 - VLAN の設定 [28-8](#)

- アドレス エイリアス設定 [28-2](#)
- イネーブルとディセーブル [28-7, 44-6](#)
- クエリア
 - 設定時の注意事項 [28-14](#)
 - 設定する [28-14](#)
- グローバル設定 [28-8](#)
- サポート [1-3](#)
- サポートされるバージョン [28-3](#)
- 設定 [28-7](#)
- 即時脱退 [28-5](#)
- 定義 [28-2](#)
- デフォルト設定 [28-7, 44-5, 44-6](#)
- 方式 [28-8](#)
- モニタリング [28-16, 44-12](#)
- IGMP スロットリング
 - アクションを表示する [28-30](#)
 - 設定する [28-29](#)
 - 説明 [28-25](#)
 - デフォルト設定 [28-26](#)
- IGMP 即時脱退
 - イネーブルにする [28-11](#)
 - 設定時の注意事項 [28-11](#)
 - 説明 [28-5](#)
- IGMP フィルタリング
 - サポート [1-3](#)
 - 設定する [28-26](#)
 - 説明 [28-25](#)
 - デフォルト設定 [28-26](#)
 - モニタリング [28-30](#)
- IGMP プロファイル
 - コンフィギュレーション モード [28-26](#)
 - 設定する [28-26](#)
 - 適用する [28-27](#)
- IGMP ヘルパー [1-3, 50-6](#)
- IGP [41-26](#)
- interfaces range macro コマンド [14-12](#)
- Interior Gateway Protocol
 - 「IGP」を参照
- Internet Group Management Protocol (インターネットグループ管理プロトコル)
 - 「IGMP」を参照
- IP ACL
 - QoS 分類の [39-8](#)
 - 暗黙の拒否 [38-10, 38-15](#)
 - 暗黙のマスク [38-10](#)
 - 名前付き [38-15](#)
 - 未定義 [38-22](#)
- ip cef distributed コマンド [41-91](#)
- ip igmp profile コマンド [28-26](#)
- IP precedence [39-2](#)
- IP precedence/DSCP マップ、QoS での [39-64](#)
- IP SLA
 - ICMP エコー動作 [47-11](#)
 - SNMP サポート [47-2](#)
 - UDP ジッタ動作 [47-9](#)
 - 応答側
 - イネーブルにする [47-8](#)
 - 説明 [47-4](#)
 - 応答時間 [47-4](#)
 - オブジェクト トラッキング [48-9](#)
 - オブジェクト トラッキングの設定 [48-9](#)
 - オブジェクト モニタリング エージェントの追跡、設定 [48-11](#)
 - サポートされるメトリック [47-2](#)
 - しきい値のモニタリング [47-6](#)
 - スケジューリング [47-5](#)
 - 制御プロトコル [47-4](#)
 - 設定時の注意事項 [47-6](#)
 - 定義 [47-1](#)
 - デフォルト設定 [47-6](#)
 - 動作 [47-3](#)
 - 到達可能性トラッキング [48-9](#)
 - トラック ステート [48-9](#)
 - ネットワーク パフォーマンスを測定する [47-3](#)
 - マルチオペレーションのスケジューリング [47-5](#)
 - モニタリング [47-13](#)
 - 利点 [47-2](#)

IP traceroute

- 概要 [53-13](#)
- 実行する [53-14](#)

IPv4 ACL

- インターフェイスに対して適用する [38-20](#)
- 拡張、作成する [38-10](#)
- 名前付き [38-15](#)
- 標準、作成する [38-9](#)

IPv4 と IPv6

- デュアルプロトコルスタック [42-5](#)

IPv6

ACL

- precedence [45-2](#)
- 一致条件 [45-3](#)
- サポート対象 [45-2](#)
- 制限 [45-3](#)
- 表示 [45-8](#)
- ポート [45-1](#)
- ルータ [45-1](#)

CEFv6 [42-20](#)Default Router Preference (DRP) [42-4](#)Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 [42-8](#)

- EIGRP IPv6 コマンド [42-8](#)
- ルータ ID [42-8](#)

ICMP [42-4](#)OSPF [42-7](#)SDM テンプレート [10-2, 44-1, 45-1](#)

- アドレス [42-2](#)
- アドレスフォーマット [42-2](#)
- アドレスを割り当てる [42-11](#)
- アプリケーション [42-5](#)
- 機能の制限 [42-10](#)
- サポート機能 [42-2](#)
- 自動設定 [42-5](#)
- スイッチの制限 [42-10](#)
- スタティック ルートの概要 [42-7](#)
- スタティック ルートを設定する [42-21](#)
- ステートレス自動設定 [42-5](#)

定義済み [42-1](#)

- デフォルト設定 [42-11](#)
- 転送する [42-11](#)
- ネイバー探索 [42-4](#)
- パス MTU ディスカバリ [42-4](#)
- 非サポート機能 [42-9](#)
- モニタリング [42-28](#)

IPv6 の HSRP

- 設定 [42-26](#)
- 注意事項 [42-25](#)

IP アドレス

- 128 ビット [42-2](#)
- IPv6 [42-2](#)
- IP ルーティング [41-4](#)
- MAC アドレス アソシエーション [41-8](#)
- クラス [41-5](#)
- クラスタ アクセス [6-2](#)
- 検出する [7-24](#)
- 候補またはメンバ [6-3, 6-14](#)
- コマンド スイッチ [6-3, 6-12, 6-14](#)
- 冗長クラスタ [6-12](#)
- スタンバイ コマンド スイッチ [6-12, 6-14](#)
- デフォルト設定 [41-4](#)
- モニタリング [41-18](#)
- 「IP 情報」も参照

IP サービス レベル契約

- 「IP SLA」を参照

IP サービス レベル、分析する [47-1](#)

IP 情報

- デフォルト設定 [4-3](#)
- 割り当て
 - DHCP ベースの自動設定を介して [4-4](#)
 - 手動で [4-16](#)

IP 送信元ガード

- イネーブル化 [26-20, 26-21](#)
- ディセーブル化 [26-20](#)

IP ソース ガード

- 802.1x と [26-19](#)
- DHCP スヌーピングと [26-17](#)

- EtherChannels と [26-19](#)
- TCAM エントリと [26-20](#)
- VRF と [26-19](#)
- スタティック バインディング
 - 削除する [26-20](#)
 - 追加する [26-20, 26-21](#)
- スタティック ホスト [26-21](#)
- 設定時の注意事項 [26-19](#)
- 説明 [26-17](#)
- 送信元 IP アドレスと MAC アドレスのフィルタリング [26-17](#)
- 送信元 IP アドレスのフィルタリング [26-17](#)
- デフォルト設定 [26-19](#)
- トランク インターフェイスと [26-19](#)
- バインディング設定
 - 自動的な [26-17](#)
 - 手動での [26-17](#)
- バインディング テーブル [26-17](#)
- 表示する
 - アクティブ IP バインディングまたは MAC バインディング [26-28](#)
 - 設定 [26-28](#)
 - バインディング [26-28](#)
- フィルタリング
 - 送信元 IP アドレス [26-17](#)
 - 送信元 IP アドレスと MAC アドレス [26-17](#)
- プライベート VLAN の [26-19](#)
- ポート セキュリティと [26-19](#)
- ルーテッド ポートと [26-19](#)
- IP ダイレクト ブロードキャスト [41-14](#)
- IP 電話
 - QoS でポート セキュリティを確立する [39-39](#)
 - QoS と [18-1](#)
 - QoS の信頼境界 [39-39](#)
 - 自動分類とキューイング [39-21](#)
 - 設定する [18-4](#)
- IP ブロードキャスト アドレス [41-16](#)
- IP プロトコル
 - ACL での [38-12](#)
 - ルーティング [1-13](#)
- IP ポート セキュリティ、スタティック ホスト用
 - PVLAN ホスト ポートでの [26-25](#)
 - レイヤ 2 アクセス ポート [26-21](#)
- IP マルチキャスト ルーティング
 - IGMP スヌーピングと [28-2](#)
- MBONE
 - sdr キャッシュ エントリの削除 [50-64](#)
 - sdr キャッシュ エントリの存在期間の制限 [50-48](#)
 - sdr キャッシュの表示 [50-65](#)
 - sdr リスナー サポート機能のイネーブル化 [50-48](#)
 - Session Directory (sdr) ツール、説明 [50-47](#)
 - アドバタイズされる DVMRP ルートの制限 [50-59](#)
 - 会議セッション アナウンスメント用の SAP パケット [50-48](#)
 - 説明 [50-47](#)
- PIMv1 および PIMv2 の相互運用性 [50-11](#)
- RP
 - PIMv2 BSR の設定 [50-31](#)
 - 自動 RP および BSR の使用 [50-35](#)
 - 自動 RP の設定 [50-27](#)
 - 手動での割り当て [50-25](#)
 - マッピング情報のモニタリング [50-36](#)
- アドレス
 - すべてのマルチキャスト ルータ [50-3](#)
 - 全ホスト [50-3](#)
 - ホスト グループ アドレス範囲 [50-3](#)
- イネーブル化
 - PIM モード [50-13](#)
 - マルチキャスト転送 [50-13](#)
- 管理用スコープの境界、説明 [50-49](#)
- 逆経路チェック (RPF) [50-8](#)
- グループ /RP マッピング
 - BSR [50-7](#)
 - 自動 RP [50-7](#)
- シスコの実装 [50-1](#)
- 自動 RP

- BSR による使用 [50-35](#)
- 概要 [50-7](#)
- 既存の SM クラウドへの追加 [50-27](#)
- キャッシュのクリア [50-64](#)
- 候補 RP スプーフィングの禁止 [50-30](#)
- 新規インターネットワークでの設定 [50-27](#)
- 設定時の注意事項 [50-12](#)
- 着信 RP アナウンスメント メッセージのフィルタリング [50-30](#)
- 問題のある RP への Join メッセージの送信禁止 [50-29](#)
- 利点 [50-27](#)
- 設定
 - IP マルチキャスト境界 [50-49](#)
 - 基本的なマルチキャスト ルーティング [50-12](#)
- デフォルト設定 [50-10](#)
- 統計情報、システムおよびネットワークの表示 [50-64](#)
- ブート ストラップ ルータ
 - IP マルチキャスト境界の定義 [50-32](#)
 - PIM ドメイン境界の定義 [50-31](#)
- 概要 [50-7](#)
- 候補 BSR の設定 [50-33](#)
- 候補 RP の設定 [50-34](#)
- 自動 RP による使用 [50-35](#)
- 設定時の注意事項 [50-12](#)
- プロトコルの動作 [50-2](#)
- マルチキャスト転送、説明 [50-8](#)
- モニタリング
 - パケット速度および損失情報 [50-65](#)
 - パスのトレース [50-65](#)
 - ピアリング デバイス [50-65](#)
- ルーティング テーブル
 - 削除 [50-64](#)
 - 表示 [50-64](#)
- 「CGMP」も参照
- 「DVMRP」も参照
- 「IGMP」も参照
- 「PIM」も参照
- IP ユニキャスト ルーティング
 - ARP [41-9](#)
 - EtherChannel レイヤ 3 インターフェイス [41-4](#)
 - IGP [41-26](#)
 - IP アドレス指定
 - クラス [41-5](#)
 - 設定 [41-4](#)
 - IRDP [41-12](#)
 - MAC アドレスおよび IP アドレス [41-8](#)
 - SVI を使用 [41-3](#)
 - UDP [41-16](#)
 - VLAN 間 [41-2](#)
 - アドミニストレーティブ ディスタンス [41-93](#), [41-104](#)
 - アドレス解決 [41-8](#)
 - イネーブル化 [41-19](#)
 - 逆アドレス解決 [41-8](#)
 - クラスレス ルーティング [41-7](#)
 - 再配信 [41-95](#)
 - サブネットゼロ [41-6](#)
 - サブネットマスク [41-6](#)
 - 受動インターフェイス [41-103](#)
 - スーパーネット [41-7](#)
 - スタティック ルーティング [41-3](#)
 - スタティック ルートの設定 [41-92](#)
 - 設定する手順 [41-4](#)
 - ダイナミック ルーティング [41-3](#)
 - ダイレクトブロードキャスト [41-14](#)
 - ディセーブル化 [41-19](#)
 - デフォルト
 - アドレス指定の設定 [41-4](#)
 - ゲートウェイ [41-12](#)
 - ネットワーク [41-94](#)
 - ルーティング [41-3](#)
 - ルート [41-94](#)
 - 認証キー [41-105](#)
 - ブロードキャスト
 - アドレス [41-16](#)
 - ストーム [41-14](#)
 - パケット [41-14](#)

フラッディング **41-17**

プロキシ ARP **41-9**

プロトコル

- ダイナミック **41-3**
- ディスタンスベクトル **41-3**
- リンクステート **41-3**

ルーテッドポート **41-3**

レイヤ 3 インターフェイス **41-3**

レイヤ 3 インターフェイスへの IP アドレスの割り当て **41-6**

「BGP」も参照

「EIGRP」も参照

「OSPF」も参照

「RIP」も参照

IP ルーティング

- イネーブル化 **41-19**
- インターフェイスを接続する **14-8**
- ディセーブル化 **41-19**

IP ルート、モニタリング **41-106**

IRDP

- サポート **1-13**
- 設定 **41-13**
- 定義 **41-12**

IS-IS

- show コマンド **41-75**
- アドレス **41-66**
- エリアルーティング **41-65**
- システムルーティング **41-65**
- デフォルト設定 **41-67**
- モニタリング **41-75**

ISO CLNS

- clear コマンド **41-75**
- NET **41-65**
- NSAP **41-65**
- OSI 標準 **41-65**
- ダイナミックルーティングプロトコル **41-65**
- モニタリング **41-75**

ISO IGRP

- エリアルーティング **41-65**

システムルーティング **41-65**

J

join メッセージ、IGMP **28-3**

K

KDC

説明 **11-42**

「Kerberos」も参照

Kerberos

KDC **11-42**

TGT **11-44**

暗号化ソフトウェア イメージ **11-41**

クレデンシヤル **11-42**

サーバ **11-43**

サポート **1-11**

信頼済みサードパーティとしてのスイッチ **11-42**

設定する **11-45**

設定例 **11-42**

説明 **11-42**

操作 **11-44**

チケット **11-42**

認証する

KDC **11-44**

境界スイッチ **11-44**

ネットワーク サービス **11-45**

用語 **11-43**

レルム **11-43**

L

l2protocol-tunnel コマンド **20-13**

LACP

「EtherChannel」を参照

レイヤ 2 プロトコル トンネリング **20-9**

LDAP **5-2**

LED、スイッチ

「ハードウェア インストレーション ガイド」を参照

Lightweight Directory Access Protocol

「LDAP」を参照

Link Aggregation Control Protocol

「EtherChannel」を参照

Link Fault アラーム 3-3

Link Layer Discovery Protocol

「CDP」を参照

Link State Advertisement (LSA) 41-31

LLDP

イネーブルにする 31-5

概要 31-1

サポートされる TLV 31-1

スイッチ スタックの考慮事項 31-2

設定

デフォルト設定 31-4

設定する 31-4

特性 31-6

送信タイマーとホールドタイム、設定する 31-6

モニタリングとメンテナンス 31-10

LLDP-MED

概要 31-1, 31-2

サポートされる TLV 31-2

設定する

TLV 31-6

手順 31-4

モニタリングとメンテナンス 31-10

LLDP Media Endpoint Discovery

「LLDP-MED」を参照

LRE プロファイル、スイッチ クラスタでの考慮事項 6-16

M

MAB

「MAC 認証バイパス」を参照

MAB エージング タイム 1-9

MAB 非アクティビティ タイマー

デフォルト設定 12-33

範囲 12-36

MAC/PHY コンフィギュレーション ステータス TLV 31-2

MAC アドレス

ACL での 38-28

IP アドレス アソシエーション 41-8

IP ソース バインディング テーブルで表示する 26-28

VLAN でのラーニングをディセーブルにする 7-23

VLAN との対応付け 7-13

アドレス テーブルを構築する 7-13

エージング タイム 7-14

検出する 7-24

スタティック

許可する 7-22, 7-24

削除する 7-21

追加する 7-21

特性 7-20

ドロップする 7-22

ダイナミック

削除する 7-15

ラーニング 7-13

デフォルト設定 7-14

表示する 7-24

MAC アドレス /VLAN マッピング 16-26

MAC アドレス通知、サポート 1-14

MAC アドレス テーブル移動更新

設定時の注意事項 25-8

設定する 25-12

説明 25-6

デフォルト設定 25-8

モニタリング 25-15

MAC アドレス ラーニング 1-5

MAC アドレス ラーニング、VLAN でディセーブルにする 7-23

MAC 拡張アクセス リスト

QoS 分類の 39-5

QoS を設定する 39-46

作成する 38-28

- 定義済み [38-28](#)
- レイヤ 2 インターフェイスに対して適用する [38-30](#)
- MAC 認証バイパス [12-36](#)
 - 「MAB」を参照
 - 概要 [12-16](#)
 - 設定する [12-56](#)
- maximum-paths コマンド [41-52, 41-92](#)
- MDA
 - 設定時の注意事項 [12-12 ~ 12-13](#)
 - 説明 [1-10, 12-12](#)
 - 認証プロセスでの例外 [12-5](#)
- MHSRP [46-4](#)
- MIB
 - SNMP の相互作用 [36-4](#)
- MIBs
 - 概要 [36-1](#)
- mrouter ポート [25-3, 25-5](#)
- MSDP
 - MSDP 接続および統計情報のクリア [51-18](#)
 - SA メッセージ
 - キャッシュ エントリのクリア [51-18](#)
 - モニタリング [51-18](#)
 - Source-Active メッセージ
 - TTL によるデータの制限 [51-13](#)
 - アドバタイズされる送信元の制限 [51-9](#)
 - キャッシング [51-6](#)
 - 着信のフィルタリング [51-14](#)
 - 定義 [51-2](#)
 - ピアからのフィルタリング [51-10](#)
 - ピアへのフィルタリング [51-12](#)
 - 概要 [51-1](#)
 - 加入遅延、定義 [51-6](#)
 - サポート [1-14](#)
 - 送信元情報の制御
 - スイッチから発信 [51-8](#)
 - スイッチで受信 [51-13](#)
 - スイッチによる転送 [51-11](#)
 - デフォルト設定 [51-4](#)
 - デンス モード領域
 - SA メッセージの送信 [51-16](#)
 - 発信元アドレスの指定 [51-17](#)
- 発信元アドレス、変更 [51-17](#)
- ピア
 - シャットダウン [51-15](#)
 - 送信元情報の要求 [51-8](#)
 - デフォルトの設定 [51-4](#)
 - ピアリング関係、概要 [51-1](#)
 - モニタリング [51-18](#)
- ピア RPF フラッドイング [51-2](#)
- フィルタリング
 - 着信 SA メッセージ [51-14](#)
 - ピアからの SA 要求 [51-10](#)
 - ピアへの SA メッセージ [51-12](#)
- メッシュグループ
 - 設定 [51-15](#)
 - 定義 [51-15](#)
- 利点 [51-3](#)
- MSTP
 - BPDU ガード
 - イネーブルにする [23-11](#)
 - 説明 [23-2](#)
 - BPDU フィルタリング
 - イネーブルにする [23-12](#)
 - 説明 [23-3](#)
 - CIST、説明 [22-3](#)
 - CIST リージョナル ルート [22-3, 22-5](#)
 - CIST ルート [22-5](#)
 - CST
 - 定義 [22-3](#)
 - リージョン間の動作 [22-4](#)
 - EtherChannel ガード
 - イネーブルにする [23-15](#)
 - 説明 [23-7](#)
 - IEEE 802.1D との相互運用性
 - 移行プロセスの再起動 [22-26](#)
 - 説明 [22-8](#)
 - IEEE 802.1s
 - 実装 [22-6](#)

- ポートの役割名の変更 [22-7](#)
- 用語 [22-5](#)
- IST
 - 定義 [22-2](#)
 - マスター [22-3](#)
 - リージョン内の動作 [22-3](#)
- MST リージョン
 - CIST [22-3](#)
 - IST [22-2](#)
 - サポートされるスパンニングツリー インスタンス [22-2](#)
 - 設定 [22-16](#)
 - 説明 [22-2](#)
 - ホップ カウント メカニズム [22-5](#)
- Port Fast
 - イネーブルにする [23-10](#)
 - 説明 [23-2](#)
- Port Fast 対応ポートのシャットダウン [23-2](#)
- VLAN と MST インスタンスのマッピング [22-16](#)
- インターフェイスの状態、転送のブロッキング [23-2](#)
- 概要 [22-2](#)
- 拡張システム ID
 - 異常動作 [22-18](#)
 - セカンダリ ルート スイッチへの影響 [22-19](#)
 - ルート スイッチへの影響 [22-18](#)
- 境界ポート
 - 設定時の注意事項 [22-16](#)
 - 説明 [22-6](#)
- サポートされるインスタンス [21-10](#)
- サポートされるオプション機能 [1-7](#)
- ステータスの表示 [22-27](#)
- ステータス、表示 [22-27](#)
- 設定
 - MST リージョン [22-16](#)
 - 高速コンバージェンス用リンク タイプ [22-25](#)
 - 最大エージング タイム [22-24](#)
 - 最大ホップ カウント [22-25](#)
 - スイッチ プライオリティ [22-22](#)
 - セカンダリ ルート スイッチ [22-19](#)
 - 転送遅延時間 [22-24](#)
 - ネイバー タイプ [22-26](#)
 - パス コスト [22-21](#)
 - ポート プライオリティ [22-20](#)
 - ルート スイッチ [22-18](#)
 - 設定時の注意事項 [22-15, 23-10](#)
 - 設定する
 - hello タイム [22-23](#)
 - デフォルト設定 [22-15](#)
 - デフォルトのオプション機能設定 [23-10](#)
 - モード間での相互運用性と互換性 [21-10](#)
 - モードのイネーブル化 [22-16](#)
 - ルート ガード
 - イネーブルにする [23-16](#)
 - 説明 [23-8](#)
 - ルート スイッチ
 - 異常動作 [22-18](#)
 - 拡張システム ID の影響 [22-18](#)
 - 設定 [22-18](#)
 - ルート スイッチ選択を防止する [23-8](#)
 - ループ ガード
 - イネーブルにする [23-16](#)
 - 説明 [23-9](#)
- multiauth
 - アクセス不能認証バイパスのサポート [12-23](#)
- multiauth モード
 - 「複数認証モード」を参照
- Multicast Source Discovery Protocol
 - 「MSDP」を参照
- multicast storm-control コマンド [29-4](#)
- Multiple HSRP
 - 「MHSRP」を参照
- Multiple VPN Routing/Forwarding、カスタマー エッジ デバイスでの
 - 「Multi-VRF CE」を参照
- Multi-VRF CE
 - サポート [1-13](#)
 - 設定 [41-78](#)

設定時の注意事項 [41-79](#)

設定例 [41-86](#)

定義 [41-76](#)

デフォルト設定 [41-78](#)

ネットワーク コンポーネント [41-78](#)

パケット転送処理 [41-78](#)

MVR

IGMPv3 と [28-21](#)

アドレスのエイリアス [28-21](#)

アプリケーション例 [28-18](#)

インターフェイスの設定 [28-23](#)

グローバル パラメータを設定する [28-21](#)

サポート [1-3](#)

設定時の注意事項 [28-21](#)

説明 [28-18](#)

デフォルト設定 [28-20](#)

マルチキャスト TV アプリケーション [28-18](#)

モード [28-22](#)

モニタリング [28-24](#)

Network Assistant

スイッチをアップグレードする [A-23](#)

説明 [1-4](#)

利点 [1-2](#)

no switchport コマンド [14-4](#)

Not-So-Stubby-Area

「NSSA」を参照

no コマンド [2-4](#)

NSAP、ISO IGRP アドレスとして [41-65](#)

NSF 認識

IS-IS [41-68](#)

NSM [5-3](#)

NSSA、OSPF [41-31](#)

NTP

アソシエーション

定義済み [7-2](#)

概要 [7-2](#)

サポート [1-5](#)

時刻

サービス [7-2](#)

同期をとる [7-2](#)

層 [7-2](#)

N

NAC

AAA ダウン ポリシー [1-11](#)

RADIUS サーバを使用した IEEE 802.1x 検証 [12-57](#)

RADIUS サーバを使用した IEEE 802.1x 認証 [12-57](#)

アクセス不能認証バイパス [1-11, 12-52](#)

クリティカル認証 [12-23, 12-52](#)

レイヤ 2 IEEE 802.1x 検証 [1-10, 12-28, 12-57](#)

レイヤ 2 IP 検証 [1-10](#)

NameSpace Mapper

「NSM」を参照

NEAT

概要 [12-29](#)

設定する [12-58](#)

Network Admission Control

NAC

O

Open1x

設定する [12-63](#)

Open1x 認証

概要 [12-29](#)

Open Shortest Path First

「OSPF」を参照

OSPF

IPv6 用 [42-7](#)

LSA グループ ペーシング [41-34](#)

インターフェイス パラメータ、設定 [41-29](#)

エリア パラメータ、設定 [41-31](#)

仮想リンク [41-32](#)

経路集約 [41-32](#)

サポート [1-13](#)

設定 [41-28](#)
 説明 [41-26](#)
 デフォルト設定
 設定 [41-27](#)
 メトリック [41-32](#)
 ルート [41-32](#)
 モニタリング [41-35](#)
 ルータ ID [41-34](#)

P

PAgP

「EtherChannel」を参照

レイヤ 2 プロトコル トンネリング [20-9](#)

PBR

イネーブル化 [41-100](#)

高速スイッチングされたポリシーベース ルーティング [41-102](#)

定義 [41-98](#)

ローカル ポリシーベース ルーティング [41-102](#)

PC (パッシブ コマンド スイッチ) [6-11](#)

PE/CE ルーティング、設定 [41-85](#)

Per-VLAN Spanning-Tree plus

「PVST+」を参照

PIM

Shortest Path Tree、使用の延期 [50-38](#)

概要 [50-4](#)

共有ツリーおよび送信元ツリー、概要 [50-37](#)

サポート [1-14](#)

スタブ ルーティング

 イネーブル化 [50-24](#)

 概要 [50-5](#)

 設定時の注意事項 [50-23](#)

 表示 [50-65](#)

スパス モード

 RPF 検索 [50-9](#)

 概要 [50-5](#)

 加入メッセージおよび共有ツリー [50-5](#)

 プルーニング メッセージ [50-5](#)

デフォルト設定 [50-10](#)

デンス モード

 RPF 検索 [50-9](#)

 概要 [50-5](#)

 ランデブー ポイント (RP)、説明 [50-5](#)

ネイバーの表示 [50-65](#)

バージョン

 v2 の改善点 [50-4](#)

 相互運用性 [50-11](#)

 相互運用性に関するトラブルシューティング [50-36](#)

モードのイネーブル化 [50-13](#)

ルータ クエリー メッセージ インターバル、変更 [50-39](#)

PIM-DVMRP、スヌーピング方式としての ping [28-9](#)

 概要 [53-10](#)

 実行する [53-10](#)

 文字出力の説明 [53-11](#)

PoE

 トラブルシューティング [53-8](#)

Port Aggregation Protocol

「EtherChannel」を参照

Port Fast

 イネーブルにする [23-10](#)

 サポート [1-7](#)

 説明 [23-2](#)

 モード、スパニングツリー [16-27](#)

Port not Forwarding アラーム [3-3](#)

Port not Operating アラーム [3-3](#)

PROFINET [9-1](#)

 設定 [9-5](#)

 設定の表示 [9-5](#)

 デフォルト設定 [9-4](#)

Protocol-Independent Multicast Protocol

「PIM」を参照

PTP

 設定 [8-3](#)

 設定の表示 [8-4](#)

デフォルト設定 [8-2](#)

PVST+

IEEE 802.1Q トランキングの相互運用性 [21-11](#)

サポートされるインスタンス [21-10](#)

説明 [21-9](#)

Q

QoS

DSCP 透過 [39-41](#)

IP 電話

検出と信頼済みの設定 [39-21, 39-39](#)

自動分類とキューイング [39-21](#)

MQC コマンドと [39-1](#)

QoS ラベル、定義済み [39-4](#)

暗黙の拒否 [39-8](#)

概要 [39-2](#)

基本モデル [39-4](#)

キュー

SRR、説明 [39-15](#)

WTD、説明 [39-14](#)

出力特性を設定する [39-72](#)

高優先順位（緊急） [39-20, 39-78](#)

入力特性を設定する [39-68](#)

場所 [39-14](#)

クラス マップ

設定する [39-47](#)

表示 [39-80](#)

グローバルにイネーブルにする [39-36](#)

再書き込み [39-20](#)

サポート [1-12](#)

自動 QoS

VoIP 用にイネーブル化 [39-27](#)

実行コンフィギュレーションでの影響 [39-26](#)

出力キューのデフォルト [39-22](#)

初期設定を表示する [39-30](#)

生成コマンドのリスト [39-23](#)

生成コマンドを表示する [39-28](#)

設定時の注意事項 [39-26](#)

設定とデフォルト表示 [39-30](#)

設定例 [39-29](#)

説明 [39-21](#)

ディセーブルにする [39-28](#)

入力キューのデフォルト [39-22](#)

出力インターフェイスで帯域幅を制限する [39-79](#)

出力キュー

DSCP 値または CoS 値のマッピング [39-75](#)

SRR の共有重みを設定する [39-77](#)

SRR のシェーピング重みを設定する [39-76](#)

WTD しきい値の設定 [39-73](#)

WTD、説明 [39-19](#)

しきい値マップを表示する [39-76](#)

スケジューリング、説明 [39-4](#)

説明 [39-4](#)

バッファ領域を割り当てる [39-73](#)

バッファ割り当てスキーム、説明 [39-18](#)

フローチャート [39-18](#)

信頼状態

信頼済みデバイス [39-39](#)

説明 [39-5](#)

ドメイン内 [39-37](#)

別のドメインとの境界 [39-41](#)

設定時の注意事項

自動 QoS [39-26](#)

標準 QoS [39-34](#)

設定する

DSCP の透過性 [39-41](#)

DSCP マップ [39-62](#)

IP 拡張 ACL [39-45](#)

IP 標準 ACL [39-44](#)

MAC ACL [39-46](#)

自動 QoS [39-21](#)

集約ポリシング機能 [39-60](#)

出力キューの特性 [39-72](#)

信頼境界 [39-39](#)

デフォルト ポート CoS 値 [39-39](#)

ドメイン内のポートの信頼状態 [39-37](#)

入力キューの特性 [39-68](#)

- 別のドメインとの境界での DSCP 信頼状態 **39-41**
 - ポリシー マップ、階層型 **39-53**
 - デフォルト自動設定 **39-21**
 - デフォルトの標準設定 **39-31**
 - 統計情報を表示する **39-80**
 - 入力キュー
 - DSCP 値または CoS 値のマッピング **39-69**
 - SRR の共有重みを設定する **39-71**
 - WTD しきい値の設定 **39-69**
 - WTD、説明 **39-17**
 - しきい値マップを表示する **39-69**
 - スケジューリング、説明 **39-4**
 - 説明 **39-4**
 - 帯域幅を割り当てる **39-71**
 - バッファと帯域幅の割り当て、説明 **39-17**
 - バッファ領域を割り当てる **39-70**
 - プライオリティ キュー、説明 **39-17**
 - プライオリティ キューを設定する **39-71**
 - フローチャート **39-16**
 - パケットの変更 **39-20**
 - フローチャート
 - 出力キューイングとスケジューリング **39-18**
 - 入力キューイングとスケジューリング **39-16**
 - 分類 **39-7**
 - ポリシングとマーキング **39-11**
 - 分類
 - DSCP の透過性、説明 **39-41**
 - IP ACL、説明 **39-6, 39-8**
 - IP トラフィックのオプション **39-6**
 - MAC ACL、説明 **39-5, 39-8**
 - クラス マップ、説明 **39-8**
 - 信頼 DSCP、説明 **39-5**
 - 信頼 IP precedence、説明 **39-5**
 - 信頼済み CoS、説明 **39-5**
 - 定義済み **39-4**
 - 転送処理 **39-3**
 - 非 IP トラフィックのオプション **39-5**
 - フレームとパケットでの **39-3**
 - フローチャート **39-7**
 - ポリシー マップ、説明 **39-8**
 - ポリサー
 - 設定 **39-52, 39-57, 39-61**
 - ポリシー、インターフェイスに接続する **39-9**
 - ポリシー マップ
 - SVI での階層 **39-53**
 - 階層 **39-9**
 - 特性 **39-49**
 - 表示する **39-80**
 - 物理ポートでの非階層 **39-49**
 - ポリシング
 - 説明 **39-4, 39-9**
 - トークン バケット アルゴリズム **39-10**
 - ポリシング機能
 - 数 **39-35**
 - 説明 **39-9**
 - タイプ **39-10**
 - 表示する **39-80**
 - マーキング、説明 **39-4, 39-9**
 - マークダウン アクション **39-52, 39-57**
 - マッピング テーブル
 - CoS/DSCP **39-63**
 - DSCP/CoS **39-66**
 - DSCP/DSCP 変換 **39-67**
 - IP precedence/DSCP **39-64**
 - タイプ **39-13**
 - 表示する **39-80**
 - ポリシング済み DSCP **39-65**
 - QoS の CoS 入力キューしきい値マップ **39-17**
 - QoS の DSCP 入力キューしきい値マップ **39-17**
 - Quality Of Service
 - 「QoS」を参照
 - Quality of Service
 - 「QoS」を参照
-
- ## R
- RADIUS

- AAA サーバ グループを定義する **11-33**
- 概要 **11-19**
- クラスタでの **6-15**
- サーバ ロード バランシング **11-41**
- サーバを指定する **11-29**
- サポート **1-11**
- 設定する
 - アカウントिंग **11-36**
 - 通信、グローバル **11-29, 11-37**
 - 通信、サーバ単位 **11-29**
 - 認可 **11-35**
 - 認証 **11-31**
 - 複数 UDP ポート **11-29**
- 設定を表示する **11-41**
- 操作 **11-21**
- 属性
 - ベンダー固有 **11-37**
 - ベンダー専用 **11-39**
- デフォルト設定 **11-28**
- ネットワーク環境の提案 **11-20**
- 方式リスト、定義済み **11-28**
- ユーザに対するサービスを制限する **11-35**
- ユーザによってアクセスされるサービスをトラッキングする **11-36**
- RADIUS 許可の変更 **11-21**
- Rapid Per-VLAN Spanning-Tree plus
 - 「Rapid PVST+」を参照
- Rapid PVST+
 - IEEE 802.1Q トランッキングの相互運用性 **21-11**
 - サポートされるインスタンス **21-10**
 - 説明 **21-9**
- RARP **41-9**
- rcommand コマンド **6-16**
- RCP
 - イメージファイル
 - アップロードする **A-36**
 - サーバを準備する **A-33**
 - ダウンロードする **A-34**
 - 古いイメージを削除する **A-36**
 - 設定ファイル
 - アップロードする **A-18**
 - 概要 **A-16**
 - サーバを準備する **A-16**
 - ダウンロードする **A-17**
- Remote Authentication Dial-In User Service
 - 「RADIUS」を参照
- Remote SPAN **30-2**
- REP
 - SNMP トラップ、設定 **24-14**
 - VLAN ブロッキング **24-13**
 - VLAN ロード バランシング **24-4**
 - VLAN ロード バランシングのトリガー **24-5**
 - インターフェイスの設定 **24-10**
 - エージング タイマー **24-8**
 - オープン セグメント **24-2**
 - および STP **24-6**
 - 管理 VLAN **24-9**
 - 管理 VLAN、設定 **24-9**
 - コンバージェンス **24-4**
 - サポートされるインターフェイス **24-1**
 - 手動によるプリエンブション、設定 **24-14**
 - セカンダリ エッジ ポート **24-4**
 - セグメント **24-1**
 - 特性 **24-2**
 - 設定時の注意事項 **24-7**
 - デフォルト設定 **24-7**
 - ネイバー オフセット番号 **24-4**
 - プライマリ エッジ ポート **24-4**
 - プリエンブション遅延時間 **24-5**
 - ポート **24-6**
 - モニタリング **24-15**
 - リンク完全性の確認 **24-3**
 - リング セグメント **24-2**
- Resilient Ethernet Protocol
 - 「REP」を参照
- RFC
 - 1058、RIP **41-20**
 - 1112、IP マルチキャストと IGMP **28-2**

- 1157、SNMPv1 [36-2](#)
- 1163、BGP [41-43](#)
- 1166、IP アドレス [41-5](#)
- 1253、OSPF [41-26](#)
- 1267、BGP [41-43](#)
- 1305、NTP [7-2](#)
- 1587、NSSA [41-26](#)
- 1757、RMON [34-2](#)
- 1771、BGP [41-43](#)
- 1901、SNMPv2C [36-2](#)
- 1902 ~ 1907、SNMPv2 [36-2](#)
- 2236、IP マルチキャストと IGMP [28-2](#)
- 2273-2275、SNMPv3 [36-2](#)
- RFC 5176 規定 [11-23](#)
- RIP
 - IPv6 用 [42-7](#)
 - アドバタイズメント [41-20](#)
 - サポート [1-13](#)
 - サマリー アドレス [41-24](#)
 - スプリット ホライズン [41-24](#)
 - 設定 [41-21](#)
 - 説明 [41-20](#)
 - デフォルト設定 [41-20](#)
 - 認証 [41-23](#)
 - ホップ カウント [41-20](#)
- RMON
 - アラームとイベントをイネーブルにする [34-3](#)
 - 概要 [34-1](#)
 - サポート [1-14](#)
 - サポートされるグループ [34-2](#)
 - ステータスを表示する [34-6](#)
 - デフォルト設定 [34-3](#)
 - 統計情報
 - グループ イーサネットを収集する [34-6](#)
 - グループ履歴を収集する [34-5](#)
- route-map コマンド [41-101](#)
- Routing Information Protocol
 - 「RIP」を参照
- RSPAN
 - VLAN ベース [30-6](#)
 - 宛先ポート [30-7](#)
 - 概要 [1-14, 30-1](#)
 - 受信トラフィック [30-4](#)
 - ステータスを表示する [30-23](#)
 - セッション
 - 作成する [30-17](#)
 - 定義済み [30-3](#)
 - 特定の VLAN に対する送信元トラフィックを制限する [30-22](#)
 - 入力トラフィックをイネーブルにする [30-20](#)
 - モニタリングされるポートを指定する [30-17](#)
 - 設定時の注意事項 [30-16](#)
 - 送信トラフィック [30-5](#)
 - 送信元ポート [30-5](#)
 - 定義済み [30-2](#)
 - デフォルト設定 [30-9](#)
 - 特性 [30-8](#)
 - 他の機能との相互動作 [30-8](#)
 - モニタリングされるポート [30-5](#)
 - モニタリング ポート [30-7](#)
- RSTP
 - BPDU
 - 形式 [22-12](#)
 - 処理 [22-13](#)
 - IEEE 802.1D との相互運用性
 - 移行プロセスの再起動 [22-26](#)
 - 説明 [22-8](#)
 - トポロジの変更 [22-13](#)
 - 「MSTP」も参照
 - アクティブ トポロジ [22-9](#)
 - 概要 [22-9](#)
 - 高速コンバージェンス
 - エッジ ポートおよび Port Fast [22-10](#)
 - 説明 [22-10](#)
 - ポイントツーポイント リンク [22-10, 22-25](#)
 - ルート ポート [22-10](#)
 - 指定スイッチ、定義 [22-9](#)
 - 指定ポート、定義 [22-9](#)

提案合意ハンドシェイク プロセス [22-10](#)

ポートの役割

説明 [22-9](#)

同期 [22-11](#)

ルート ポート、定義 [22-9](#)

S

SCP

SSH と [11-58](#)

設定する [11-58](#)

「SCP」を参照

SC (スタンバイ コマンド スイッチ) [6-11](#)

SDM

テンプレート

数 [10-1](#)

設定する [10-4](#)

SDM テンプレート [45-3](#)

設定時の注意事項 [10-3](#)

設定する [10-3](#)

タイプ [10-1](#)

デュアル IPv4/IPv6 [10-2](#)

Secure Copy Protocol

Secure Socket Layer

「SSL」を参照

set-request オペレーション [36-4](#)

SFP

ステータス、表示する [53-10](#)

セキュリティと識別情報 [53-9](#)

モニタリング ステータス [14-27, 53-10](#)

show access-lists hw-summary コマンド [38-22](#)

show alarm コマンド [3-13](#)

show cdp traffic コマンド [32-6](#)

show cluster members コマンド [6-16](#)

show configuration コマンド [14-21](#)

show forward コマンド [53-17](#)

show interfaces switchport [25-4](#)

show interfaces コマンド [14-19, 14-21](#)

show l2protocol コマンド [20-14, 20-16, 20-17](#)

show lldp traffic コマンド [31-11](#)

show platform forward コマンド [53-17](#)

show running-config コマンド

ACL を表示する [38-20, 38-21, 38-33, 38-35](#)

インターフェイスの説明 [14-21](#)

show コマンドと more コマンドの出力、フィルタリング [2-10](#)

shutdown コマンド、インターフェイスでの [14-28](#)

SmartPort マクロ

グローバル パラメータ値の適用 [15-3](#)

シスコのデフォルト マクロの適用 [15-3](#)

設定時の注意事項 [15-2](#)

デフォルト設定 [15-1](#)

トレース [15-2](#)

表示 [15-5](#)

SNAP [32-1](#)

SNMP

CPU しきい値通知を設定する [36-17](#)

ifIndex 値 [36-6](#)

IP SLA と [47-2](#)

MIB 変数にアクセスする [36-4](#)

TFTP サーバによるアクセスを制限する [36-18](#)

エージェント

説明 [36-4](#)

ディセーブルにする [36-8](#)

エンジン ID [36-7](#)

概要 [36-1, 36-4](#)

クラスタでの [6-15](#)

クラスタを管理する [6-17](#)

グループ [36-7, 36-10](#)

コミュニティ ストリング

概要 [36-4](#)

クラスタ スイッチの [36-4](#)

設定する [36-8](#)

サポートされるバージョン [36-2](#)

システム接点と場所 [36-17](#)

システム ログ メッセージを NMS に対して制限する [35-10](#)

情報

- イネーブルにする **36-16**
- 説明 **36-5**
- ディセーブルにする **36-16**
- トラップ キーワードと **36-13**
- トラップとの違い **36-5**
- ステータス、表示する **36-19**
- セキュリティ レベル **36-3**
- 設定例 **36-18**
- 帯域内管理 **1-6**
- 通知 **36-5**
- デフォルト設定 **36-7**
- トラップ
 - MAC アドレス通知をイネーブルにする **7-15, 7-17, 7-19**
 - イネーブルにする **36-13**
 - 概要 **36-1, 36-4**
 - 情報との違い **36-5**
 - 説明 **36-3, 36-5**
 - タイプ **36-13**
 - ディセーブルにする **36-16**
 - トラップ マネージャ、設定する **36-14**
 - 認証レベル **36-11**
 - ホスト **36-7**
 - マネージャ機能 **1-4, 36-3**
 - ユーザ **36-7, 36-10**
- SNMPv1 **36-2**
- SNMPv2C **36-2**
- SNMPv3 **36-2**
- SNMP と Syslog、IPv6 による **42-8**
- SNMP トラップ
 - REP **24-14**
- Source-Specific Multicast
 - 「SSM」を参照
- SPAN
 - VLAN ベース **30-6**
 - 宛先ポート **30-7**
 - 概要 **1-14, 30-1**
 - 受信トラフィック **30-4**
 - ステータスを表示する **30-23**
- セッション
 - 宛先（モニタリング）ポートを削除する **30-12**
 - 作成する **30-11**
 - 定義済み **30-3**
 - 特定の VLAN に対する送信元トラフィックを制限する **30-15**
 - 入力転送を設定する **30-14, 30-21**
 - 入力トラフィックをイネーブルにする **30-13**
 - モニタリングされるポートを指定する **30-11**
- 設定時の注意事項 **30-10**
- 送信トラフィック **30-5**
- 送信元ポート **30-5**
- デフォルト設定 **30-9**
- ポート、制約事項 **29-13**
- 他の機能との相互動作 **30-8**
- モニタリングされるポート **30-5**
- モニタリング ポート **30-7**
- SPAN トラフィック **30-4**
- SRR
 - 共有モード **39-15**
 - サポート **1-12, 1-13**
 - シェーピング モード **39-15**
 - 設定する
 - 出力キューでの共有重み **39-77**
 - 出力キューでのシェーピング重み **39-76**
 - 入力キューでの共有重み **39-71**
 - 説明 **39-15**
- SSH
 - 暗号化ソフトウェア イメージ **11-47**
 - 暗号化方式 **11-48**
 - 設定 **11-48**
 - 説明 **1-6, 11-47**
 - ユーザ認証方式、サポートされる **11-48**
- SSL
 - 暗号化ソフトウェア イメージ **11-51**
 - セキュア HTTP クライアントを設定する **11-56**
 - セキュア HTTP サーバを設定する **11-55**
 - 設定時の注意事項 **11-54**
 - 説明 **11-51**

- モニタリング [11-57](#)
- SSM
 - CGMP の制限 [50-16](#)
 - IGMPv3 [50-14](#)
 - IGMPv3 ホスト シグナリング [50-16](#)
 - IGMP スヌーピング [50-16](#)
 - Internet Standard Multicast との違い [50-14](#)
 - IP アドレス範囲 [50-15](#)
 - PIM [50-14](#)
 - アドレス管理に関する制約 [50-16](#)
 - コンポーネント [50-14](#)
 - ステート維持の制限 [50-17](#)
 - 設定 [50-14, 50-17](#)
 - 設定時の注意事項 [50-16](#)
 - 動作 [50-15](#)
 - モニタリング [50-17](#)
- SSM マッピング [50-17](#)
 - DNS ベース [50-19, 50-21](#)
 - 概要 [50-18](#)
 - スタティック [50-19, 50-21](#)
 - スタティック トラフィック転送 [50-22](#)
 - 制限 [50-18](#)
 - 設定 [50-17, 50-20](#)
 - 設定時の注意事項 [50-18](#)
 - モニタリング [50-23](#)
- standby ip コマンド [46-6](#)
- STP
 - BackboneFast
 - イネーブルにする [23-14](#)
 - 説明 [23-5](#)
 - ディセーブルにする [23-15](#)
 - BPDU ガード
 - イネーブルにする [23-11](#)
 - 説明 [23-2](#)
 - ディセーブルにする [23-12](#)
 - BPDU フィルタリング
 - イネーブルにする [23-12](#)
 - 説明 [23-3](#)
 - ディセーブルにする [23-13](#)
 - BPDU メッセージ交換 [21-3](#)
 - EtherChannel ガード
 - イネーブルにする [23-15](#)
 - 説明 [23-7](#)
 - ディセーブルにする [23-15](#)
 - IEEE 802.1D とブリッジ ID [21-4](#)
 - IEEE 802.1D とマルチキャスト アドレス [21-8](#)
 - IEEE 802.1Q トランクでの制限 [21-10](#)
 - IEEE 802.1t と VLAN 識別情報 [21-4](#)
 - Port Fast
 - イネーブルにする [23-10](#)
 - 説明 [23-2](#)
 - Port Fast 対応ポートのシャットダウン [23-2](#)
 - UplinkFast
 - イネーブルにする [23-14](#)
 - 説明 [23-3](#)
 - VLAN ブリッジ [21-11](#)
 - インターフェイスの状態
 - 概要 [21-4](#)
 - ディセーブル [21-7](#)
 - 転送する [21-5, 21-7](#)
 - ブロッキング [21-6](#)
 - ラーニング [21-6](#)
 - リスニング [21-6](#)
 - インターフェイスの状態、転送のブロッキング [23-2](#)
 - および REP [24-6](#)
 - 下位 BPDU [21-3](#)
 - 概要 [21-2](#)
 - カウンタ、クリア [21-24](#)
 - 拡張システム ID
 - 概要 [21-4](#)
 - セカンダリ ルート スイッチの影響 [21-17](#)
 - 予期しない動作 [21-16](#)
 - ルート スイッチの影響 [21-15](#)
 - 間接リンク障害を検出する [23-5](#)
 - サポートされるインスタンス [21-10](#)
 - サポートされるオプション機能 [1-7](#)
 - サポートされる機能 [1-7](#)

- サポートされるプロトコル [21-9](#)
 - サポートされるモード [21-9](#)
 - 指定スイッチ、定義済み [21-4](#)
 - 指定ポート、定義済み [21-4](#)
 - 冗長接続性 [21-8](#)
 - ステータス、表示する [21-23](#)
 - ステータスを表示する [21-23](#)
 - 設定
 - hello タイム [21-21](#)
 - 最大エージング タイム [21-22](#)
 - セカンダリ ルート スイッチ [21-17](#)
 - 転送遅延時間 [21-22](#)
 - ポート プライオリティ [21-17](#)
 - 設定時の注意事項 [21-12, 23-10](#)
 - 設定する
 - スイッチ プライオリティ [21-20](#)
 - スパニングツリー モード [21-14](#)
 - 転送保留カウント [21-23](#)
 - パス コスト [21-19](#)
 - ルート スイッチ [21-15](#)
 - タイマー、説明 [21-21](#)
 - ディセーブルにする [21-15](#)
 - デフォルト設定 [21-12](#)
 - デフォルトのオプション機能設定 [23-10](#)
 - パス コスト [16-24, 16-25](#)
 - ポート プライオリティ [16-23](#)
 - マルチキャスト アドレス、影響 [21-8](#)
 - モード間での相互運用性と互換性 [21-10](#)
 - 優位 BPDU [21-3](#)
 - ルート ガード
 - イネーブルにする [23-16](#)
 - 説明 [23-8](#)
 - ルート スイッチ
 - 拡張システム ID の影響 [21-4, 21-15](#)
 - 設定する [21-15](#)
 - 選択 [21-3](#)
 - 予期しない動作 [21-16](#)
 - ルート スイッチ 選択を防止する [23-8](#)
 - ルート ポート 選択のアクセラレーション [23-4](#)
 - ルート ポート、定義済み [21-3](#)
 - ループ ガード
 - イネーブルにする [23-16](#)
 - 説明 [23-9](#)
 - レイヤ 2 プロトコル トネリング [20-8](#)
 - ロード シェアリング
 - 概要 [16-22](#)
 - パス コストを使用する [16-24](#)
 - ポート プライオリティを使用する [16-23](#)
 - SunNet Manager [1-4](#)
 - SVI
 - IP ユニキャスト ルーティング [41-3](#)
 - VLAN 間でのルーティング [16-2](#)
 - VLAN の接続 [14-7](#)
 - 定義 [14-5](#)
 - ルータ ACL [38-4](#)
 - SVI 自動ステート除外
 - 設定する [14-24](#)
 - 定義 [14-6](#)
 - SVI リンク ステート [14-6](#)
 - Switch Database Management
 - 「SDM」を参照
 - switchport backup interface [25-4, 25-5](#)
 - switchport block multicast コマンド [29-8](#)
 - switchport block unicast コマンド [29-8](#)
 - switchport mode dot1q-tunnel コマンド [20-7](#)
 - switchport protected コマンド [29-7](#)
 - switchport コマンド [14-14](#)
 - Syslog
 - 「システム メッセージ ロギング」を参照
-
- ## T
- TACACS+
 - アカウンティング、定義済み [11-12](#)
 - 概要 [11-11](#)
 - クラスタでの [6-15](#)
 - サーバを指定する [11-14](#)
 - サポート [1-11](#)

- 設定する
 - アカウントティング [11-18](#)
 - 認可 [11-17](#)
 - 認証キー [11-14](#)
 - ログイン認証 [11-15](#)
 - 設定を表示する [11-19](#)
 - 操作 [11-13](#)
 - デフォルト設定 [11-14](#)
 - 認可、定義済み [11-12](#)
 - 認証、定義済み [11-12](#)
 - ユーザに対するサービスを制限する [11-17](#)
 - ユーザによってアクセスされるサービスをトラッキングする [11-18](#)
 - tar ファイル
 - イメージファイルの形式 [A-24](#)
 - 作成する [A-6](#)
 - 抽出する [A-7](#)
 - 内容を表示する [A-7](#)
 - TCL スクリプト、組み込みイベント マネージャによる登録と定義 [37-6](#)
 - TDR [1-15](#)
 - Telnet
 - 管理インターフェイスにアクセスする [2-10](#)
 - 接続数 [1-6](#)
 - パスワードを設定する [11-6](#)
 - Terminal Access Controller Access Control System Plus
 - 「TACACS+」を参照
 - TFTP
 - イメージファイル
 - アップロードする [A-28](#)
 - サーバを準備する [A-25](#)
 - 削除する [A-27](#)
 - ダウンロードする [A-26](#)
 - サーバによるアクセスを制限する [36-18](#)
 - 自動設定を設定する [4-8](#)
 - 設定ファイル
 - アップロードする [A-12](#)
 - サーバを準備する [A-11](#)
 - ダウンロードする [A-11](#)
 - ベース ディレクトリの設定ファイル [4-8](#)
 - TFTP サーバ [1-5](#)
 - time-range コマンド [38-17](#)
 - TLV
 - LLDP [31-1](#)
 - LLDP-MED [31-2](#)
 - 定義済み [31-1](#)
 - ToS [1-12](#)
 - traceroute コマンド [53-14](#)
 - 「IP traceroute」も参照
 - traceroute、レイヤ 2
 - 1 ポートに複数のデバイス [53-13](#)
 - ARP [53-12](#)
 - CDP [53-12](#)
 - IP アドレスおよびサブネット [53-12](#)
 - MAC アドレスおよび VLAN [53-12](#)
 - 説明 [53-12](#)
 - ブロードキャスト トラフィック [53-12](#)
 - マルチキャスト トラフィック [53-12](#)
 - ユニキャスト トラフィック [53-12](#)
 - tracerout、レイヤ 2
 - 使用上の注意事項 [53-12](#)
-
- ## U
- UDLD
 - イネーブル化
 - グローバル [33-5](#)
 - イネーブルにする
 - インターフェイスごとの [33-5](#)
 - インターフェイスをリセットする [33-6](#)
 - 概要 [33-1](#)
 - 検出メカニズムをエコーする [33-3](#)
 - サポート [1-7](#)
 - ステータス、表示する [33-7](#)
 - 設定時の注意事項 [33-4](#)
 - ディセーブルにする
 - インターフェイスごとの [33-5](#)
 - グローバルに [33-5](#)

- 光ファイバインターフェイスでの **33-5**
 - デフォルト設定 **33-4**
 - ネイバー データベース **33-2**
 - リンク検出メカニズム **33-1**
 - レイヤ 2 プロトコル トンネリング **20-11**
 - UDLD シャットダウン インターフェイスをリセットする **33-6**
 - UDP ジッタ、設定する **47-9**
 - UDP ジッタ動作、IP SLA **47-9**
 - UDP、設定 **41-16**
 - unicast storm control コマンド **29-4**
 - UNIX Syslog サーバ
 - サポートされる機能 **35-14**
 - デーモンの設定 **35-13**
 - メッセージ ロギング設定 **35-13**
 - UplinkFast
 - イネーブルにする **23-14**
 - 説明 **23-3**
 - ディセーブルにする **23-14**
-
- ## V
- VLAN
 - 1006 ~ 4094 の ID を設定する **16-11**
 - RSPAN での送信元トラフィックを制限する **30-22**
 - SPAN での送信元トラフィックを制限する **30-15**
 - STP と IEEE 802.1Q トランク **21-10**
 - SVI による接続 **14-7**
 - VLAN データベースに追加する **16-8**
 - VLAN ブリッジ STP **21-11, 52-2**
 - VTP モード **17-3**
 - 拡張範囲 **16-1, 16-11**
 - 機能 **1-8**
 - サービス プロバイダー ネットワーク内のカスタマー番号 **20-3**
 - 削除する **16-9**
 - 作成する **16-9**
 - サポートされる **16-2**
 - サポートされる番号 **1-8**
 - 図示 **16-2**
 - スタティック アクセス ポート **16-10**
 - スパンニングツリー インスタンスと **16-3, 16-7, 16-12**
 - 設定 **16-1**
 - 設定時の注意事項、拡張範囲 VLAN **16-11**
 - 設定時の注意事項、標準範囲 VLAN **16-6**
 - 説明 **14-2, 16-1**
 - ダイナミック アドレスのエージング **21-9**
 - 追加 **16-8**
 - デフォルト設定 **16-7**
 - トークンリング **16-6**
 - トラフィック **16-2**
 - トランク上で許可される **16-20**
 - 内部 **16-12**
 - ネイティブ、設定する **16-22**
 - パラメータ **16-5**
 - 表示する **16-15**
 - 標準範囲 **16-1, 16-5**
 - 変更する **16-8**
 - ポート メンバーシップ モード **16-3**
 - マルチキャスト **28-18**
 - vlan.dat ファイル **16-5**
 - VLAN 1、トランク ポート上でディセーブルにする **16-20**
 - VLAN 1 の最小化 **16-20**
 - VLAN ACL
 - 「VLAN マップ」を参照
 - vlan dot1q tag native コマンド **20-5**
 - VLAN ID、検出する **7-24**
 - VLAN Query Protocol
 - 「VQP」を参照
 - VLAN 間ルーティング **1-13, 41-2**
 - VLAN 管理ドメイン **17-2**
 - vlan グローバル コンフィギュレーション コマンド **16-7**
 - VLAN コンフィギュレーション モード **2-2**
 - VLAN 設定
 - 起動時 **16-7**
 - 保存 **16-7**

VLAN データベース

VLAN の保存 [16-5](#)VTP と [17-1](#)スタートアップ コンフィギュレーション ファイル
と [16-7](#)保存されている VLAN 設定 [16-7](#)

VLAN トランッキング プロトコル

「VTP」を参照

VLAN トランク [16-15](#)VLAN の削除 [16-9](#)VLAN フィルタリングと SPAN [30-6](#)VLAN ブロッキング、REP [24-13](#)

VLAN マップ

ACL と VLAN マップの例 [38-33](#)一般的な使用方法 [38-36](#)サーバに対するアクセス拒否の例 [38-37](#)削除する [38-35](#)作成 [38-33](#)サポート [1-9](#)設定時の注意事項 [38-32](#)設定する [38-31](#)定義済み [38-2](#)適用 [38-35](#)パケットの拒否と許可 [38-33](#)表示 [38-43](#)ワイヤリング クローゼットの設定例 [38-36](#)VLAN マップ エントリ、順序 [38-32](#)

VLAN マネジメント ポリシー サーバ

「VMPS」を参照

VLAN メンバーシップ

確認する [16-29](#)モード [16-3](#)VLAN リンク ステート [14-6](#)

VLAN ロード バランシング

REP [24-4](#)VLAN ロード バランシング、Flex Link の [25-2](#)設定時の注意事項 [25-8](#)VLAN ロード バランシング、トリガー [24-5](#)VLAN 割り当て応答、VMPS [16-26](#)

VMPS

MAC アドレスの VLAN へのマッピング [16-26](#)管理する [16-31](#)サーバ アドレスを入力する [16-28](#)再確認間隔、変更する [16-30](#)設定時の注意事項 [16-27](#)設定例 [16-32](#)説明 [16-26](#)

ダイナミック ポート メンバーシップ

再確認する [16-30](#)説明 [16-27](#)トラブルシューティング [16-31](#)デフォルト設定 [16-27](#)メンバーシップを再確認する [16-29](#)モニタリング [16-31](#)リトライ回数、変更する [16-30](#)Voice over IP [18-1](#)

VPN

サービス プロバイダー ネットワーク内 [41-76](#)フォワーディング [41-78](#)ルーティングの設定 [41-85](#)ルート [41-77](#)

VPN ルーティングおよび転送テーブル

「VRF」を参照

VQP [1-8, 16-26](#)

VRF

定義 [41-78](#)テーブル [41-76](#)

VRF 認識サービス

ARP [41-82](#)ftp [41-84](#)HSRP [41-83](#)ping [41-82](#)SNMP [41-82](#)syslog [41-83](#)tftp [41-84](#)traceroute [41-84](#)設定 [41-81](#)

VTP

アドバタイズメント [16-17, 17-3, 17-4](#)

拡張範囲 VLAN と [16-3, 17-1](#)

クライアント モード、設定する [17-12](#)

クライアントをドメインに追加する [17-16](#)

サーバ モード、設定する [17-10, 17-14](#)

サポート [1-8](#)

使用する [17-1](#)

整合性検査 [17-4](#)

設定

- 注意事項 [17-8](#)
- 保存する [17-8](#)
- 要件 [17-10](#)

設定の要件 [17-10](#)

設定リビジョン番号

- 注意事項 [17-16](#)
- リセットする [17-17](#)

説明 [17-1](#)

デフォルト設定 [17-8](#)

統計情報 [17-18](#)

トークンリングのサポート [17-4](#)

ドメイン [17-2](#)

ドメイン名 [17-9](#)

トランスペアレント モード、設定 [17-11](#)

バージョン

- イネーブルにする [17-14](#)

バージョン 1 [17-4](#)

バージョン 2

- 概要 [17-4](#)
- 設定時の注意事項 [17-9](#)

バージョン 3

- 概要 [17-5](#)

バージョン、注意事項 [17-9](#)

パスワード [17-9](#)

標準範囲 VLAN と [16-3, 17-1](#)

プルーニング

- イネーブルにする [17-15](#)
- 概要 [17-5](#)
- サポート [1-8](#)
- ディセーブルにする [17-15](#)

例 [17-6](#)

プルーニング適格リスト、変更する [16-21](#)

モード

- オフ [17-3](#)
- クライアント [17-3](#)
- サーバ [17-3](#)
- トランスペアレント [17-3](#)
- 変遷 [17-3](#)

モニタリング [17-18](#)

レイヤ 2 プロトコル トンネリング [20-8](#)

W

WCCP

MD5 セキュリティ [49-3](#)

イネーブル化 [49-6](#)

クライアントから受信したトラフィックのリダイレクト [49-6](#)

サポートしない WCCPv2 機能 [49-4](#)

サポートしない機能 [49-4](#)

設定時の注意事項 [49-5](#)

説明 [49-1](#)

ダイナミック サービス グループ [49-3](#)

デフォルト設定 [49-5](#)

転送方式 [49-3](#)

認証 [49-3](#)

ネゴシエーション [49-3](#)

パケットのリダイレクト [49-3](#)

パケット戻し方式 [49-3](#)

パスワードの設定 [49-7](#)

表示 [49-10](#)

メッセージ交換 [49-2](#)

モニタリングおよびメンテナンス [49-10](#)

レイヤ 2 ヘッダー書き換え [49-3](#)

Web Cache Communication Protocol

「WCCP」を参照

Web 認証 [12-16](#)

- 設定する [13-16 ~ ??](#)
- 説明 [1-8](#)

Web ベース認証

カスタマイズ可能な Web ページ [13-6](#)

説明 [13-1](#)

Web ベース認証、他の機能との相互作用 [13-7](#)

Weighted Tail Drop

「WTD」を参照

WTD

サポート [1-12](#), [1-13](#)

しきい値を設定する

出力キュー セット [39-73](#)

入力キュー [39-69](#)

説明 [39-14](#)

X

Xmodem プロトコル [53-2](#)

あ

アカウントティング

802.1x での [12-48](#)

IEEE 802.1x での [12-14](#)

RADIUS での [11-36](#)

TACACS+ での [11-12](#), [11-18](#)

アクセス拒否応答、VMPS [16-26](#)

アクセス グループ

IPv4 ACL をインターフェイスに対して適用する [38-21](#)

レイヤ 2 [38-21](#)

レイヤ 3 [38-21](#)

アクセス コントロール エントリ

「ACE」を参照

アクセス コントロール エントリ (ACE) [45-3](#)

アクセスする

クラスタ、スイッチ [6-14](#)

コマンドスイッチ [6-12](#)

スイッチ クラスタ [6-14](#)

メンバ スイッチ [6-14](#)

アクセス不能認証バイパス [12-23](#)

multiauth ポートのサポート [12-23](#)

アクセス ポート

スイッチ クラスタでの [6-10](#)

定義済み [14-3](#)

レイヤ 2 プロトコル トンネリング [20-11](#)

アクセス リスト

「ACL」を参照

アクティブ トラフィック モニタリング、IP SLA [47-1](#)

アクティブ リンク [25-2](#), [25-4](#), [25-5](#), [25-6](#)

アクティブ ルータ [46-2](#)

アップグレードする、ソフトウェア イメージを

「ダウンロードする」を参照

アップロードする

イメージ ファイル

FTP を使用する [A-32](#)

RCP を使用する [A-36](#)

TFTP を使用する [A-28](#)

準備する [A-25](#), [A-29](#), [A-33](#)

理由 [A-24](#)

設定ファイル

FTP を使用する [A-15](#)

RCP を使用する [A-18](#)

TFTP を使用する [A-12](#)

準備する [A-11](#), [A-13](#), [A-16](#)

理由 [A-9](#)

宛先 IP アドレス ベース転送、EtherChannel [40-8](#)

宛先 MAC アドレス転送、EtherChannel [40-8](#)

宛先アドレス

IPv4 ACL での [38-12](#)

IPv6 ACL [45-5](#)

アドバタイズメント

CDP [32-1](#)

LLDP [31-1](#), [31-2](#)

RIP [41-20](#)

VTP [16-17](#), [17-3](#), [17-4](#)

アドミニストレーティブ ディスタンス

OSPF [41-32](#)

定義 [41-104](#)

ルーティング プロトコルのデフォルト [41-93](#)

アドレス

- IPv6 [42-2](#)
- MAC アドレス テーブルを表示する [7-24](#)
- MAC、検出する [7-24](#)
- スタティック
 - 追加と削除 [7-20](#)
 - 定義済み [7-12](#)
- ダイナミック
 - エージング タイムを変更する [7-14](#)
 - エージングのアクセラレーション [21-9](#)
 - 削除する [7-15](#)
 - 定義済み [7-12](#)
 - デフォルト エージング [21-9](#)
 - ラーニング [7-13](#)
- マルチキャスト
 - STP アドレス管理 [21-8](#)
 - グループ アドレス範囲 [50-3](#)
- アドレス解決 [7-24, 41-8](#)
- アドレス解決プロトコル
 - 「ARP」を参照
- アドレスのエイリアス [28-2](#)
- アプリケーション エンジン、トラフィックのリダイレクト [49-1](#)
- アベイラビリティ、機能 [1-7](#)
- アラーム
 - 温度 [3-2](#)
 - 電源装置 [3-2](#)
 - 表示 [3-13](#)
- アラーム、RMON [34-4](#)
- アラーム発生オプション
 - SNMP トラップ [3-4](#)
 - Syslog メッセージ [3-4](#)
 - 方法 [3-3](#)
 - リレー設定 [3-3](#)
- アラーム プロファイル
 - 作成または変更 [3-11](#)
 - 設定 [3-12](#)
- 暗号化、CipherSuite [11-53](#)
- 暗号化ソフトウェア イメージ

Kerberos [11-41](#)SSH [11-47](#)SSL [11-51](#)暗号化、パスワードの [11-4](#)

い

- イーサネット VLAN
 - 追加する [16-8](#)
 - デフォルトと範囲 [16-8](#)
 - 変更する [16-8](#)
- 一時的な自己署名証明書 [11-52](#)
- 一致する、IPv4 ACL [38-7](#)
- 一般クエリー [25-5](#)
- イネーブル化、SNMP トラップの [3-13](#)
- イネーブル パスワード [11-4](#)
- イベント、RMON [34-4](#)
- イベント検出器、組み込みイベント マネージャ [37-2](#)
- インターネット制御メッセージ プロトコル
 - 「ICMP」を参照
- インターネット プロトコル バージョン 6
 - 「IPv6」を参照
- インターフェイス
 - Auto-MDIX、設定する [14-20](#)
 - カウンタ、クリアする [14-27](#)
 - 管理 [1-4](#)
 - 再起動 [14-28](#)
 - サポートされる [14-8](#)
 - シャットダウンする [14-28](#)
 - 情報を表示する [14-26](#)
 - ステータス [14-26](#)
 - 設定時の注意事項
 - デュプレックスと速度 [14-17](#)
 - 設定する
 - 手順 [14-9](#)
 - 説明 [14-21](#)
 - タイプ [14-1](#)
 - デフォルト設定 [14-14](#)
 - デュプレックスと速度、設定する [14-18](#)

範囲 **14-10**
 範囲マクロ **14-12**
 物理、指定する **14-8**
 フロー制御 **14-19**
 命名する **14-21**
 モニタリング **14-26**
 わかりやすい名前、追加 **14-21**
 インターフェイス コマンド **14-8 ~ 14-9**
 インターフェイス コンフィギュレーション
 REP **24-10**
 インターフェイス コンフィギュレーション モード **2-3**
 インターフェイス タイプ **14-8**
 インベントリ管理 TLV **31-2, 31-7**

え

永続的な自己署名証明書 **11-52**
 エージング タイマー、REP **24-8**
 エージング タイム
 MAC アドレス テーブル **7-14**
 アクセラレーション
 MSTP の **22-24**
 STP での **21-9, 21-22**
 最大
 MSTP **22-24, 22-25**
 STP での **21-22, 21-23**
 エージング、短縮 **21-9**
 エラー メッセージ、コマンド入力中の **2-5**
 エリア ボーダ ルータ
 「ABR」を参照
 エリア ルーティング
 IS-IS **41-65**
 ISO IGRP **41-65**

お

応答側、IP SLA
 イネーブルにする **47-8**
 説明 **47-4**

応答時間、IP SLA で測定する **47-4**
 オブジェクト トラッキング
 HSRP **48-7**
 IP SLA **48-9**
 IP SLA、設定 **48-9**
 モニタリング **48-13**
 オブジェクト トラッキングのプライマリ インターフェイス、DHCP、設定 **48-11**
 オブジェクトのトラッキング **48-2**
 オプション、管理 **1-4**
 オフ モード、VTP **17-3**
 音声 VLAN
 Cisco 7960 Phone、ポート接続 **18-1**
 IP 電話音声トラフィック、説明 **18-2**
 IP 電話データトラフィック、説明 **18-2**
 IP 電話への接続 **18-4**
 音声トラフィックに対してポートを設定する
 802.1p プライオリティ タグ付きフレーム **18-5**
 音声トラフィック用のポート設定
 802.1Q フレーム **18-5**
 設定時の注意事項 **18-3**
 説明 **18-1**
 データトラフィックに対して IP 電話を設定する
 着信フレームの CoS のオーバーライド **18-6**
 着信フレームの CoS プライオリティの信頼 **18-6**
 デフォルト設定 **18-3**
 表示する **18-7**
 音声認識 802.1x セキュリティ
 ポートベース認証
 設定する **12-37**
 説明 **12-29, 12-37**
 温度アラーム、設定 **3-7, 3-8**

か

階層、NTP **7-2**
 階層型ポリシー マップ
 設定時の注意事項 **39-34**

- 設定する [39-53](#)
 - 説明 [39-12](#)
 - 階層ポリシー マップ [39-9](#)
 - 回復手順 [53-1](#)
 - 外部ネイバー、BGP [41-48](#)
 - カウンタ、インターフェイスをクリアする [14-27](#)
 - 拡散更新アルゴリズム (DUAL) [41-35](#)
 - 拡張 crashinfo ファイル [53-20](#)
 - 拡張 IGRP
 - 「EIGRP」を参照
 - 拡張オブジェクト トラッキング
 - DHCP プライマリ インターフェイス [48-11](#)
 - HSRP [48-7](#)
 - IP SLA [48-9](#)
 - IP SLA でのネットワーク モニタリング [48-11](#)
 - IP ルーティング ステート [48-2](#)
 - コマンド [48-1](#)
 - スタティック ルート プライマリ インターフェイス [48-11](#)
 - 追跡リスト [48-3](#)
 - 定義 [48-1](#)
 - バックアップ スタティック ルーティング [48-12](#)
 - ラインプロトコル ステート [48-2](#)
 - ルーティング ポリシー、設定 [48-12](#)
 - 拡張オブジェクト トラッキングのスタティック ルーティング [48-10](#)
 - 拡張システム ID
 - MSTP [22-18](#)
 - STP [21-4, 21-15](#)
 - 拡張範囲 VLAN
 - 作成する [16-12](#)
 - 設定 [16-11](#)
 - 設定時の注意事項 [16-11](#)
 - 定義済み [16-1](#)
 - 内部 VLAN ID を指定した作成 [16-14](#)
 - 拡張ユニバーサル識別情報
 - 「EUI」を参照
 - カスタマイズ可能な Web ページ、Web ベース認証 [13-6](#)
 - 仮想 IP アドレス
 - クラスタ スタンバイ グループ [6-12](#)
 - コマンド スイッチ [6-12](#)
 - 仮想スイッチと PAgP [40-5](#)
 - 仮想ルータ [46-1, 46-2](#)
 - 簡易ネットワーク管理プロトコル
 - 「SNMP」を参照
 - 環境変数、機能 [4-21](#)
 - 環境変数、組み込みイベント マネージャ [37-4](#)
 - 管理 VLAN
 - REP、設定 [24-9](#)
 - 異なる管理 VLAN での検出 [6-8](#)
 - スイッチ クラスタでの考慮事項 [6-8](#)
 - 管理 VLAN、REP [24-9](#)
 - 管理アクセス
 - 帯域外コンソール ポート接続 [1-6](#)
 - 帯域内
 - CLI セッション [1-6](#)
 - SNMP [1-6](#)
 - デバイス マネージャ [1-6](#)
 - ブラウザ セッション [1-6](#)
 - 管理アドレス TLV [31-2](#)
 - 管理オプション
 - CLI [2-1](#)
 - CNS [5-1](#)
 - 概要 [1-4](#)
 - クラスタリング [1-2](#)
 - 管理の簡易性に関する機能 [1-4](#)
 - 関連付け、温度アラームのリレーへの [3-8](#)
-
- ## き
- キー発行局
 - 「KDC」を参照
 - 起動
 - 手動 [4-19](#)
 - 機能、非互換 [29-13](#)
 - 逆アドレス解決 [41-8](#)
 - 逆アドレス解決プロトコル
 - 「RARP」を参照

許可 VLAN リスト [16-20](#)

許可ポート、IEEE 802.1x での [12-10](#)

緊急キュー、QoS の [39-78](#)

<

クエリー、IGMP [28-4](#)

クエリー送信要求、IGMP [28-13](#)

組み込みイベント マネージャ

TCL スクリプトの登録と定義 [37-6](#)

アクション [37-4](#)

アプレットの登録と定義 [37-5](#)

イベント検出器 [37-2](#)

概要 [37-1](#)

環境変数 [37-4](#)

情報の表示 [37-7](#)

設定 [37-1, 37-5](#)

ポリシー [37-4](#)

クライアント プロセス、トラッキング [48-1](#)

クライアント モード、VTP [17-3](#)

クラスター グループおよび HSRP グループのバインド [46-12](#)

クラスター、スイッチ

LRE プロファイルの考慮事項 [6-16](#)

アクセスする [6-14](#)

管理する

CLI を使用して [6-16](#)

SNMP を介して [6-17](#)

互換性 [6-4](#)

自動回復 [6-11](#)

自動検出 [6-4](#)

説明 [6-1](#)

プランニング [6-4](#)

プランニングの考慮事項

CLI [6-16](#)

IP アドレス [6-14](#)

LRE プロファイル [6-16](#)

RADIUS [6-15](#)

SNMP [6-15, 6-17](#)

TACACS+ [6-15](#)

自動回復 [6-11](#)

自動検出 [6-4](#)

パスワード [6-15](#)

ホスト名 [6-14](#)

利点 [1-2](#)

「候補スイッチ」、「コマンドスイッチ」、「クラスタースタンバイグループ」、「メンバースイッチ」、「スタンバイコマンドスイッチ」も参照

クラスタースタンバイグループ

HSRP グループ [46-12](#)

仮想 IP アドレス [6-12](#)

考慮事項 [6-12](#)

自動回復 [6-13](#)

定義済み [6-2](#)

要件 [6-3](#)

「HSRP」も参照

クラス マップ、QoS の

設定する [39-47](#)

説明 [39-8](#)

表示する [39-80](#)

クラスレス ドメイン間ルーティング

「CIDR」を参照

クラスレス ルーティング [41-7](#)

クリアする、インターフェイスを [14-27](#)

クリティカル VLAN [12-23](#)

クリティカル認証、IEEE 802.1x [12-52](#)

グローバル コンフィギュレーション モード [2-2](#)

グローバル ステータス モニタリング アラーム [3-2](#)

グローバルな脱退、IGMP [28-13](#)

クロック

「システム クロック」を参照

け

経路集約、OSPF [41-32](#)

ケーブル、単方向リンクのモニタリング [33-1](#)

ゲスト VLAN と 802.1x [12-21](#)

権限レベル

回線に対するデフォルトを変更する **11-10**
 概要 **11-2, 11-9**
 既存の **11-11**
 コマンド スイッチ **6-16**
 コマンドを設定する **11-9**
 メンバスイッチでのマッピング **6-16**
 ログイング **11-11**
 検出、クラスタ
 「自動検出」を参照
 検出する、間接リンク障害を、STP **23-5**

こ

構成設定、保存する **4-16**
 高速コンバージェンス **22-10**
 高速スパンニングツリー プロトコル
 「RSTP」を参照
 候補スイッチ
 自動検出 **6-4**
 定義済み **6-3**
 要件 **6-3**
 「コマンド スイッチ」、「クラスタ スタンバイ グループ」、「メンバスイッチ」も参照
 互換性、機能 **29-13**
 コマンド
 no 形式と default 形式 **2-4**
 短縮形 **2-4**
 コマンド、権限レベルを設定する **11-9**
 コマンド スイッチ
 アクセスする **6-12**
 アクティブ (AC) **6-11**
 置き換える
 クラスタ メンバでの **53-5**
 別のスイッチとの **53-6**
 回復
 失われたメンバ接続性からの **53-8**
 コマンド スイッチの障害からの **6-11, 53-4**
 冗長 **6-11**
 スタンバイ (SC) **6-11**

設定の矛盾 **53-8**
 定義済み **6-1**
 パスワード権限レベル **6-16**
 パッシブ (PC) **6-11**
 プライオリティ **6-11**
 要件 **6-3**
 「候補スイッチ」、「クラスタ スタンバイ グループ」、「メンバスイッチ」、「スタンバイ コマンド スイッチ」も参照
 コマンド モード **2-1**
 コマンドライン インターフェイス
 「CLI」を参照
 コミュニティ VLAN **19-2, 19-3**
 コミュニティ ストリング
 SNMP **6-15**
 概要 **36-4**
 クラスタ スイッチの **36-4**
 クラスタでの **6-15**
 設定する **6-15, 36-8**
 コミュニティ ポート **19-2**
 コミュニティ リスト、BGP **41-58**
 壊れたソフトウェア、Xmodem での回復手順 **53-2**
 コンソール ポート、接続する **2-10**
 コンテンツ ルーティング テクノロジー
 「WCCP」を参照
 コンバージェンス
 REP **24-4**
 コンフィギュレーション ファイル
 パスワード回復のディセーブル時の考慮事項 **11-5**
 コンフィギュレーション ログイング **2-5**

さ

サーバ モード、VTP **17-3**
 サービス拒絶攻撃 **29-1**
 サービス クラス
 「CoS」を参照
 サービス プロバイダー ネットワーク
 EtherChannel のレイヤ 2 プロトコル トンネリング **20-9**

IEEE 802.1Q トンネリング [20-1](#)
 カスタマー VLAN [20-2](#)
 レイヤ 2 プロトコル [20-8](#)

サービス プロバイダー ネットワーク、MSTP および RSTP [22-1](#)

再確認間隔、VMPS、変更する [16-30](#)

再確認する、ダイナミック VLAN メンバーシップを [16-29](#)

最大エージング タイム

- MSTP [22-24](#)
- STP [21-22](#)

最大数、ポートあたりのデバイスの、ポートベース認証 [12-36](#)

最大ホップ カウント、MSTP [22-25](#)

最適化する、システム リソースを [10-1](#)

サブドメイン、プライベート VLAN [19-1](#)

サブネット ゼロ [41-6](#)

サブネット マスク [41-6](#)

サポートされるポートベース認証方式 [12-7](#)

し

シーケンス番号、ログ メッセージの [35-8](#)

シェイプド ラウンド ロビン

- 「SRR」を参照

時間帯 [7-5](#)

時間範囲、ACL での [38-17](#)

しきい値、トラフィック レベル [29-2](#)

しきい値のモニタリング、IP SLA [47-6](#)

時刻

- 「NTP とシステム クロック」を参照

シスコ エクスプレス フォワーディング

- 「CEF」を参照

システム MTU

- IS-IS LSP [41-70](#)

システム MTU および IEEE 802.1Q トンネリング [20-5](#)

システム記述 TLV [31-2](#)

システム機能 TLV [31-2](#)

システム クロック

- 概要 [7-1](#)

設定する

- 時間帯 [7-5](#)
- 手動で [7-4](#)
- 夏時間 [7-6](#)
- 日時を表示する [7-5](#)
- 「NTP」も参照

システム プロンプト、デフォルト設定 [7-7, 7-8](#)

システム名

- 手動での設定 [7-8](#)
- デフォルト設定 [7-8](#)
- 「DNS」も参照

システム名 TLV [31-1](#)

システム メッセージ ロギング

- Syslog 機能 [1-14](#)
- UNIX Syslog サーバ

 - サポートされる機能 [35-14](#)
 - デーモンを設定する [35-13](#)
 - ロギング機能を設定する [35-13](#)

- イネーブルにする [35-4](#)
- エラー メッセージの重大度を定義する [35-9](#)
- 概要 [35-1](#)
- 機能キーワード、説明 [35-14](#)
- シーケンス番号、イネーブルとディセーブル [35-8](#)
- 設定を表示する [35-14](#)
- タイム スタンプ、イネーブルとディセーブル [35-8](#)
- ディセーブルにする [35-4](#)
- デフォルト設定 [35-3](#)
- 表示宛先デバイスを設定する [35-5](#)
- メッセージの形式 [35-2](#)
- メッセージを制限する [35-10](#)
- レベル キーワード、説明 [35-10](#)
- ログ メッセージの同期をとる [35-6](#)

システム リソース、最適化する [10-1](#)

システム ルーティング

- IS-IS [41-65](#)
- ISO IGRP [41-65](#)

実行コンフィギュレーション

- 置き換える [A-19, A-20](#)
- ロール バックする [A-19, A-20](#)

- 実行コンフィギュレーション、保存する **4-16**
 - 自動 QoS
 - 「QoS」を参照
 - 自動 RP、説明 **50-7**
 - 自動イネーブル化 **12-30**
 - 自動回復、クラスタ **6-11**
 - 自動検出
 - 考慮事項
 - CDP 非対応デバイス **6-7**
 - 管理 VLAN **6-8**
 - クラスタ非対応デバイス **6-7**
 - 異なる VLAN **6-7**
 - 最新のスイッチ **6-10**
 - 接続性 **6-4**
 - 非候補デバイスの先 **6-8**
 - ルーテッドポート **6-9**
 - スイッチ クラスタでの **6-4**
 - 「CDP」も参照
 - 自動検知、ポート速度 **1-2**
 - 自動ステート除外 **14-6**
 - 自動設定 **4-4**
 - 自動ネゴシエーション
 - インターフェイス設定時の注意事項 **14-18**
 - デュプレックス モード **1-2**
 - 不一致 **53-8**
 - 自動復旧、クラスタ
 - 「HSRP」も参照
 - 重大度、システム メッセージで定義する **35-9**
 - 柔軟な認証の順序設定
 - 概要 **12-28**
 - 設定する **12-63**
 - 集約アドレス、BGP **41-61**
 - 集約グローバルユニキャストアドレス **42-3**
 - 集約ポート
 - 「EtherChannel」を参照
 - 集約ポリシング **1-12**
 - 集約ポリシング機能 **39-60**
 - 受動インターフェイス
 - OSPF **41-32**
 - 設定 **41-103**
 - 手動によるプリエンブション、REP、設定 **24-14**
 - 準備状態チェック
 - ポートベース認証
 - 設定する **12-36**
 - 説明 **12-16, 12-36**
 - 照合
 - IPv6 ACL **45-3**
 - 冗長性
 - EtherChannel **40-3**
 - HSRP **46-1**
 - STP
 - パス コスト **16-24**
 - バックボーン **21-8**
 - ポートプライオリティ **16-23**
 - 冗長リンクと UplinkFast **23-14**
 - 初期設定
 - Express Setup **1-2**
 - デフォルト **1-15**
 - 自律システム、BGP 内 **41-48**
 - 自律システム境界ルータ
 - 「ASBR」を参照
 - 侵入検知システム
 - 「IDS 装置」を参照
 - 信頼される境界、QoS の **39-39**
 - 信頼状態、ポートの
 - IP 電話のポート セキュリティを確立する **39-39**
 - QoS ドメイン間 **39-41**
 - QoS ドメイン内 **39-37**
 - 分類オプション **39-5**
 - 信頼できるトランスポート プロトコル、EIGRP **41-36**
-
- す**
- スイッチ仮想インターフェイス
 - 「SVI」を参照
 - スイッチ コンソール ポート **1-6**
 - スイッチ ソフトウェア機能 **1-1**
 - スイッチド パケット、ACL **38-39**

- スイッチドポート **14-2**
 - スイッチドポート アナライザ
 - 「SPAN」を参照
 - スイッチのクラスタ化テクノロジー **6-1**
 - 「クラスタ、スイッチ」も参照
 - スイッチプライオリティ
 - MSTP **22-22**
 - STP **21-20**
 - スーパーネット **41-7**
 - スケジューリング、IP SLA 動作 **47-5**
 - スケジュール、リロードの **4-22**
 - スタートアップ コンフィギュレーション
 - 起動のデフォルト設定 **4-18**
 - クリアする **A-19**
 - 設定ファイル
 - 自動的にダウンロードする **4-18**
 - ファイル名を指定する **4-18**
 - ブーティング
 - 手動で **4-19**
 - 特定のイメージ **4-20**
 - スタティック IP ルーティング **1-13**
 - スタティック MAC アドレッシング **1-9**
 - スタティック SSM マッピング **50-19, 50-21**
 - スタティック VLAN メンバーシップ **16-2**
 - スタティック アクセス ポート
 - VLAN に割り当てる **16-10**
 - 定義済み **14-3, 16-3**
 - スタティック アドレス
 - 「アドレス」を参照
 - スタティック トラフィック転送 **50-22**
 - スタティック ルーティング **41-3**
 - スタティック ルーティング サポート、拡張オブジェクト
トラッキング **48-10**
 - スタティック ルーティングのプライマリ インターフェイス、設定 **48-11**
 - スタティック ルート
 - IPv6 で設定する **42-21**
 - 概要 **42-7**
 - 設定 **41-92**
 - スタティック ルートのプライマリ インターフェイス、設定 **48-11**
 - スタブ エリア、OSPF **41-31**
 - スタブ ルーティング、EIGRP **41-42**
 - スタンバイ グループ、クラスタ
 - 「クラスタ スタンバイ グループ」と「HSRP」も参照
 - スタンバイ コマンド スイッチ
 - 仮想 IP アドレス **6-12**
 - 考慮事項 **6-12**
 - 設定する
 - 定義済み **6-2**
 - プライオリティ **6-11**
 - 要件 **6-3**
 - 「クラスタ スタンバイ グループ」と「HSRP」も参照
 - スタンバイ タイマー、HSRP **46-11**
 - スタンバイ リンク **25-2**
 - スタンバイ ルータ **46-2**
 - スティッキ ラーニング **29-10**
 - ストーム制御
 - サポート **1-3**
 - しきい値 **29-2**
 - 設定する **29-3**
 - 説明 **29-1**
 - ディセーブルにする **29-5**
 - 表示する **29-23**
 - スヌーピング、IGMP **28-2**
 - スパニングツリーとネイティブ VLAN **16-17**
 - スパニングツリー プロトコル
 - 「STP」を参照
 - スプリット ホライズン、RIP **41-24**
 - スモールフレーム着信レート、設定する **29-5**
-
- せ**
- 正規の時刻源、説明 **7-2**
 - 制御プロトコル、IP SLA **47-4**
 - 制限する、アクセスを
 - RADIUS **11-19**
 - TACACS+ **11-11**

- 概要 [11-1](#)
- パスワードと権限レベル [11-2](#)
- 制限付き VLAN
 - IEEE 802.1x で使用する [12-22](#)
 - 設定する [12-50](#)
 - 説明 [12-22](#)
- 整合性検査、VTP バージョン 2 での [17-4](#)
- 正常終了応答、VMPS [16-26](#)
- 生成する、IGMP レポートを [25-4](#)
- セカンダリ VLAN [19-2](#)
- セカンダリ エッジ ポート、REP [24-4](#)
- セキュア HTTP クライアント
 - 設定する [11-56](#)
 - 表示する [11-57](#)
- セキュア HTTP サーバ
 - 設定する [11-55](#)
 - 表示する [11-57](#)
- セキュア MAC アドレス
 - 最大数 [29-10](#)
 - 削除する [29-17](#)
 - タイプ [29-10](#)
- セキュア シェル
 - 「SSH」を参照
- セキュア ポート、設定する [29-9](#)
- セキュア リモート接続 [11-47](#)
- セキュリティ機能 [1-8](#)
- セキュリティ、ポート [29-9](#)
- 設計する、ネットワークを、例 [1-18](#)
- 接続性の問題 [53-10, 53-11, 53-13](#)
- 接続、セキュア リモート [11-47](#)
- 設定、FCS エラー ヒステリシスしきい値の [3-10](#)
- 設定可能な脱退タイマー、IGMP [28-6](#)
- 設定時の注意事項
 - REP [24-7](#)
- 設定時の注意事項、Multi-VRF CE [41-79](#)
- 設定、初期
 - Express Setup [1-2](#)
 - デフォルト [1-15](#)
- 設定する、802.1x ユーザ ディストリビューションを [12-56](#)
- 設定する、スモールフレーム着信レートを [29-5](#)
- 設定する、ポートベース認証の違反モードを [12-38 ~ 12-39](#)
- 設定、セカンダリ温度しきい値の [3-7, 3-8](#)
- 設定、電源装置アラーム オプションの [3-7](#)
- 設定の置換 [A-19](#)
- 設定の変更、ロギング [35-11](#)
- 設定の矛盾、失われたメンバ接続性から回復する [53-8](#)
- 設定のロールバック [A-19, A-20](#)
- 設定ファイル
 - DHCP で取得する [4-9](#)
 - TFTP サーバアクセスを制限する [36-18](#)
 - アーカイブする [A-20](#)
 - アップロードする
 - FTP を使用する [A-15](#)
 - RCP を使用する [A-18](#)
 - TFTP を使用する [A-12](#)
 - 準備する [A-11, A-13, A-16](#)
 - 理由 [A-9](#)
 - コピー時の無効な組み合わせ [A-5](#)
 - 作成時と使用上の注意事項 [A-9](#)
 - システム接点と場所の情報 [36-17](#)
 - 実行コンフィギュレーションを置き換える [A-19, A-20](#)
 - 実行コンフィギュレーションをロールバックする [A-19, A-20](#)
 - スタートアップ コンフィギュレーションを消去する [A-19](#)
 - 説明 [A-8](#)
 - タイプと場所 [A-10](#)
 - ダウンロードする
 - FTP を使用する [A-14](#)
 - RCP を使用する [A-17](#)
 - TFTP を使用する [A-11](#)
 - 自動的に [4-18](#)
 - 準備する [A-11, A-13, A-16](#)
 - 理由 [A-9](#)
 - 置換とロールバックの注意事項 [A-21](#)

テキスト エディタを使用して作成する [A-10](#)

デフォルト名 [4-18](#)

ファイル名を指定する [4-18](#)

保存された設定を削除する [A-19](#)

設定例、ネットワーク [1-18](#)

設定ロガー [35-11](#)

セットアップ プログラム

障害が発生したコマンド スイッチの置換 [53-6](#)

障害が発生したコマンド スイッチを置き換える [53-5](#)

そ

送信元 IP アドレス ベース転送、EtherChannel [40-8](#)

送信元 IP アドレス ベース転送と宛先 IP アドレス ベース転送、EtherChannel [40-8](#)

送信元 MAC アドレス転送、EtherChannel [40-8](#)

送信元 MAC アドレス転送と宛先 MAC アドレス転送、EtherChannel [40-8](#)

送信元アドレス

IPv4 ACL での [38-12](#)

IPv6 ACL [45-5](#)

即時脱退、IGMP [28-5](#)

イネーブルにする [44-9](#)

属性、RADIUS

ベンダー固有 [11-37](#)

ベンダー専用 [11-39](#)

属性と値のペア [12-12, 12-15, 12-20](#)

ソフトウェア イメージ

tar ファイル形式、説明 [A-24](#)

回復手順 [53-2](#)

フラッシュ内での場所 [A-24](#)

リロードのスケジューリング [4-22](#)

「ダウンロードとアップロード」も参照

た

ダイナミック ARP インспекション

ARP ACL と DHCP スヌーピング エントリのプライオリティ [27-5](#)

ARP キャッシュ ポイズニング [27-1](#)

ARP スプーフィング攻撃 [27-1](#)

ARP パケットのレート制限

errdisable ステート [27-5](#)

設定 [27-11](#)

説明 [27-4](#)

ARP 要求、説明 [27-1](#)

DHCP スヌーピング バインディング データベース [27-2](#)

DoS 攻撃、回避 [27-11](#)

man-in-the middle 攻撃、説明 [27-2](#)

インターフェイス信頼状態 [27-3](#)

機能 [27-2](#)

クリア

統計情報 [27-16](#)

ログ バッファ [27-16](#)

設定

着信 ARP パケットのレート制限 [27-4, 27-11](#)

ログ バッファ [27-13](#)

設定時の注意事項 [27-6](#)

設定する

DHCP 環境での [27-7](#)

非 DHCP 環境の ACL [27-9](#)

説明 [27-1](#)

妥当性チェック、実行 [27-12](#)

デフォルト設定 [27-6](#)

統計情報

クリア [27-16](#)

表示 [27-16](#)

ドロップされたパケットのロギング、説明 [27-5](#)

ネットワーク セキュリティ問題とインターフェイス信頼状態 [27-3](#)

表示

ARP ACL [27-15](#)

信頼状態およびレート制限 [27-15](#)

設定および動作状態 [27-15](#)

統計情報 [27-16](#)

ログ バッファ [27-16](#)

レート制限を超過した場合の errdisable ステート [27-5](#)

ログ バッファ

- クリア [27-16](#)
- 設定 [27-13](#)
- 表示 [27-16](#)

ダイナミック アクセス ポート

- 設定する [16-29](#)
- 定義済み [14-3](#)
- 特性 [16-4](#)

ダイナミック アドレス

「アドレス」を参照

ダイナミック ポート VLAN メンバーシップ

- 再確認する [16-29, 16-30](#)
- 接続のタイプ [16-29](#)
- 説明 [16-27](#)
- トラブルシューティング [16-31](#)

ダイナミック ルーティング [41-3](#)

ISO CLNS [41-65](#)

タイプ オブ サービス

「ToS」を参照

タイム スタンプ、ログ メッセージの [35-8](#)

タイム ドメイン 反射率計

「TDR」を参照

ダウンロード可能 ACL [12-19, 12-21, 12-60](#)

ダウンロードする

イメージ ファイル

- FTP を使用する [A-30](#)
- HTTP を使用する [A-23](#)
- RCP を使用する [A-34](#)
- TFTP を使用する [A-26](#)
- 準備する [A-25, A-29, A-33](#)
- デバイス マネージャまたは Network Assistant を使用する [A-23](#)
- 古いイメージを削除する [A-27](#)
- 理由 [A-24](#)

設定ファイル

- FTP を使用する [A-14](#)
- RCP を使用する [A-17](#)
- TFTP を使用する [A-11](#)
- 準備する [A-11, A-13, A-16](#)

理由 [A-9](#)

タグ付きパケット

- IEEE 802.1Q [20-3](#)
- レイヤ 2 プロトコル [20-8](#)

単一方向リンク検出プロトコル

「UDLD」を参照

短時間でのコンバージェンス [25-3](#)

短縮形、コマンドの [2-4](#)

端末回線、パスワードを設定する [11-6](#)

つ

ツイストペア イーサネット、単方向リンクを検出する [33-1](#)

追跡対象オブジェクト

- しきい値重みによる [48-5](#)
- しきい値パーセントによる [48-6](#)
- ブール式の使用 [48-4](#)

追跡リスト

- 設定 [48-3](#)
- タイプ [48-3](#)

追跡リスト内の重みしきい値 [48-5](#)

追跡リスト内のパーセントしきい値 [48-6](#)

追跡リスト内のブール式 [48-4](#)

て

ディスタンスベクトル プロトコル [41-3](#)

ディスタンス ベクトル マルチキャスト ルーティング プロトコル

「DVMRP」を参照

ディスタンスベクトル マルチキャスト ルーティング プロトコル

「DVMRP」を参照

ディファレンシエーテッド サービス アーキテクチャ、QoS [39-2](#)

ディファレンシエーテッド サービス コード ポイント [39-2](#)

ディレクトリ

作業ディレクトリを表示する [A-4](#)

- 作成と削除 [A-4](#)
- 変更する [A-4](#)
- デバイス検出プロトコル [31-1, 32-1](#)
- デバイス マネージャ
 - スイッチをアップグレードする [A-23](#)
 - 説明 [1-2, 1-4](#)
 - 帯域内管理 [1-6](#)
 - 利点 [1-2](#)
- デバッグする
 - エラー メッセージ出力をリダイレクトする [53-17](#)
 - コマンドを使用する [53-16](#)
 - すべてのシステム診断をイネーブルにする [53-17](#)
 - 特定機能に対してイネーブルにする [53-16](#)
- デフォルト ゲートウェイ [4-16, 41-12](#)
- デフォルト設定
 - 802.1x [12-33](#)
 - BGP [41-45](#)
 - CDP [32-2](#)
 - DHCP [26-9](#)
 - DHCP Option 82 [26-9](#)
 - DHCP スヌーピング [26-9](#)
 - DHCP スヌーピング バインディング データベース [26-9](#)
 - DNS [7-9](#)
 - EIGRP [41-37](#)
 - EtherChannel [40-10](#)
 - Flex Link [25-8](#)
 - HSRP [46-5](#)
 - IEEE 802.1Q トンネリング [20-4](#)
 - IGMP [50-41](#)
 - IGMP スヌーピング [28-7, 44-5, 44-6](#)
 - IGMP フィルタリング [28-26](#)
 - IP SLA [47-6](#)
 - IPv6 [42-11](#)
 - IP アドレス指定、IP ルーティング [41-4](#)
 - IP ソース ガード [26-19](#)
 - IP マルチキャスト ルーティング [50-10](#)
 - IS-IS [41-67](#)
 - LLDP [31-4](#)
 - MAC アドレス テーブル [7-14](#)
 - MAC アドレス テーブル移動更新 [25-8](#)
 - MSDP [51-4](#)
 - MSTP [22-15](#)
 - Multi-VRF CE [41-78](#)
 - MVR [28-20](#)
 - OSPF [41-27](#)
 - PIM [50-10](#)
 - PROFINET [9-4](#)
 - PTP [8-2](#)
 - RADIUS [11-28](#)
 - REP [24-7](#)
 - RIP [41-20](#)
 - RMON [34-3](#)
 - RSPAN [30-9](#)
 - SDM テンプレート [10-3](#)
 - SNMP [36-7](#)
 - SPAN [30-9](#)
 - SSL [11-54](#)
 - STP [21-12](#)
 - TACACS+ [11-14](#)
 - UDLD [33-4](#)
 - VLAN [16-7](#)
 - VLAN、レイヤ 2 イーサネット インターフェイス [16-17](#)
 - VMPS [16-27](#)
 - VTP [17-8](#)
 - WCCP [49-5](#)
 - イーサネット インターフェイス [14-14](#)
 - オプションのスパニングツリー設定 [23-10](#)
 - 音声 VLAN [18-3](#)
 - 起動 [4-18](#)
 - システム名とプロンプト [7-8](#)
 - システム メッセージ ロギング [35-3](#)
 - 自動 QoS [39-21](#)
 - 初期スイッチ情報 [4-3](#)
 - ダイナミック ARP インスペクション [27-6](#)
 - パスワードと権限レベル [11-3](#)
 - バナー [7-11](#)

- 標準 QoS [39-31](#)
 - フォールバックブリッジング [52-3](#)
 - プライベート VLAN [19-6](#)
 - レイヤ 2 インターフェイス [14-14](#)
 - レイヤ 2 プロトコルトンネリング [20-12](#)
 - デフォルト ネットワーク [41-94](#)
 - デフォルトの Web ベース認証の設定
 - 802.1X [13-9](#)
 - デフォルト ルーティング [41-3](#)
 - デフォルト ルート [41-94](#)
 - デュアル IPv4/IPv6 テンプレート [10-2, 42-6](#)
 - デュアルアクションの検出 [40-5](#)
 - デュアルパーパス アップリンク
 - LED [14-7](#)
 - タイプを設定する [14-15](#)
 - 定義済み [14-7](#)
 - リンクの選択 [14-7, 14-15](#)
 - デュアルプロトコルスタック
 - IPv4 と IPv6 [42-6](#)
 - SDM テンプレートのサポート [42-6](#)
 - 電源管理 TLV [31-2, 31-7](#)
 - 転送情報ベース
 - 「FIB」を参照
 - 転送遅延時間
 - MSTP [22-24](#)
 - STP [21-22](#)
 - 転送保留カウント
 - 「STP」を参照
-
- と**
- 同期化、BGP [41-48](#)
 - 統計情報
 - 802.1x [12-65, 13-17](#)
 - CDP [32-5](#)
 - IP マルチキャスト ルーティング [50-64](#)
 - LLDP [31-10](#)
 - LLDP-MED [31-10](#)
 - NMSP [31-10](#)
 - OSPF [41-35](#)
 - QoS の入力と出力 [39-80](#)
 - RMON グループ イーサネット [34-6](#)
 - RMON グループ履歴 [34-5](#)
 - SNMP 入力と出力 [36-19](#)
 - VTP [17-18](#)
 - インターフェイス [14-27](#)
 - 到達可能性、IP SLA IP ホストのトラッキング [48-9](#)
 - トークンリング VLAN
 - VTP サポート [17-4](#)
 - サポート [16-6](#)
 - 独立 VLAN [19-2, 19-3](#)
 - 独立ポート [19-2](#)
 - 都市ロケーション [31-2](#)
 - 特権 EXEC モード [2-2](#)
 - ドメイン、ISO IGRP ルーティング [41-65](#)
 - ドメイン ネーム システム
 - 「DNS」を参照
 - ドメイン名
 - DNS [7-8](#)
 - VTP [17-9](#)
 - トラストポイント、CA [11-52](#)
 - トラッキング、IP ルーティング ステートの [48-2](#)
 - トラッキング、インターフェイス ラインプロトコル ステートの [48-2](#)
 - トラッキング プロセス [48-1](#)
 - トラック ステート、IP SLA のトラッキング [48-9](#)
 - トラップ
 - MAC アドレス通知を設定する [7-15, 7-17, 7-19](#)
 - 概要 [36-1, 36-4](#)
 - 通知タイプ [36-13](#)
 - 定義済み [36-3](#)
 - マネージャを設定する [36-13](#)
 - 有効化 [7-15, 7-17, 7-19, 36-13](#)
 - トラップ ドア メカニズム [4-2](#)
 - トラフィック
 - 非フラグメント化 [38-5](#)
 - フラグメント化 [38-5](#)
 - フラッドのブロッキング [29-8](#)

分割 IPv6 [45-2](#)
 トラフィックの抑制 [29-2](#)
 トラフィック ポリシング [1-12](#)
 トラブルシューティング
 CiscoWorks での [36-4](#)
 CPU 使用率 [53-21](#)
 debug コマンド [53-16](#)
 PIMv1 および PIMv2 の相互運用性の問題 [50-36](#)
 ping による [53-10](#)
 SFP セキュリティと識別情報 [53-9](#)
 show forward コマンド [53-17](#)
 traceroute での [53-13](#)
 クラッシュ情報を表示する [53-20](#)
 システム メッセージ ログイングでの [35-1](#)
 接続性の問題 [53-10, 53-11, 53-13](#)
 単方向リンクを検出する [33-1](#)
 パケット転送を設定する [53-17](#)
 トランキングのカプセル化 [1-8](#)
 トランク
 DTP をサポートしないデバイス [16-15](#)
 許可 VLAN リスト [16-20](#)
 タグなしトラフィック用ネイティブ VLAN [16-22](#)
 パラレル [16-24](#)
 ブルーニング適格リスト [16-21](#)
 ロードシェアリング
 STP パス コストを設定する [16-24](#)
 STP ポートプライオリティを使用する [16-23](#)
 トランク フェールオーバー
 「リンクステート トラッキング」を参照
 トランク ポート
 設定する [16-19](#)
 定義済み [14-3, 16-3](#)
 トランスペアレント モード、VTP [17-3](#)
 トンネリング
 IEEE 802.1Q [20-1](#)
 定義 [20-1](#)
 レイヤ 2 プロトコル [20-8](#)
 トンネル ポート
 IEEE 802.1Q、設定 [20-6](#)

説明 [14-4, 20-1](#)
 定義済み [16-4](#)
 他の機能との非互換性 [20-6](#)

な

内部ネイバー、BGP [41-48](#)
 夏時間 [7-6](#)
 等コスト ルーティング [1-13, 41-92](#)
 名前付き IPv4 ACL [38-15](#)
 並べ替え、ACL エントリ [38-15](#)

に

二重タグ パケット
 IEEE 802.1Q トンネリング [20-2](#)
 レイヤ 2 プロトコル トンネリング [20-11](#)
 認可
 RADIUS での [11-35](#)
 TACACS+ での [11-12, 11-17](#)
 認証
 AAA でのローカル モード [11-46](#)
 EIGRP [41-40](#)
 HSRP [46-11](#)
 OpenIxx [12-29](#)
 RADIUS
 キー [11-29](#)
 ログイン [11-31](#)
 TACACS+
 キー [11-14](#)
 定義済み [11-12](#)
 ログイン [11-15](#)
 「ポートベース認証」を参照
 認証キー、ルーティング プロトコル [41-105](#)
 認証失敗 VLAN
 「制限付き VLAN」を参照
 認証の互換性、Catalyst 6000 スイッチとの [12-8](#)
 認証マネージャ
 CLI コマンド [12-9](#)

以前の 802.1x CLI コマンドとの互換性 [12-9 ~ ??](#)

概要 [12-7](#)

ね

ネイティブ VLAN

IEEE 802.1Q トンネリング [20-4](#)

設定する [16-22](#)

デフォルト [16-22](#)

ネイバー、BGP [41-59](#)

ネイバー オフセット番号、REP [24-4](#)

ネイバー探索、IPv6 [42-4](#)

ネイバー探索および回復、EIGRP [41-36](#)

ネットワーク エッジ アクセス トポロジ

「NEAT」を参照

ネットワーク管理

CDP [32-1](#)

RMON [34-1](#)

SNMP [36-1](#)

ネットワーク タイム プロトコル

「NTP」を参照

ネットワークの設計

サービス [1-19](#)

パフォーマンス [1-19](#)

ネットワークの設定例

ネットワーク サービスを提供する [1-19](#)

ネットワーク パフォーマンスを改善する [1-19](#)

ネットワーク パフォーマンス、IP SLA で測定する [47-3](#)

ネットワーク ポリシー TLV [31-2, 31-7](#)

IP ソース ガード [26-17](#)

アドレス、Cisco IOS DHCP サーバ [26-7](#)

バインディング データベース

DHCP スヌーピング

「DHCP スヌーピング バインディング データベース」を参照

アドレス、DHCP サーバ

「DHCP、Cisco IOS サーバ データベース」を参照

バインディング テーブル、DHCP スヌーピング

「DHCP スヌーピング バインディング データベース」を参照

パケットの変更、QoS での [39-20](#)

パス MTU 検出 [42-4](#)

パス コスト

MSTP [22-21](#)

STP [21-19](#)

パスワード

VTP ドメイン [17-9](#)

暗号化 [11-4](#)

回復 [53-3](#)

回復をディセーブルにする [11-5](#)

概要 [11-1](#)

クラスタでの [6-15](#)

セキュリティ [1-9](#)

設定する

Telnet [11-6](#)

イネーブル [11-3](#)

シークレットをイネーブルにする [11-4](#)

ユーザ名での [11-7](#)

デフォルト設定 [11-3](#)

バックアップ インターフェイス

「Flex Link」を参照

バックアップ スタティック ルーティング、設定 [48-12](#)

バックアップ リンク [25-2](#)

バナー

設定する

Message-of-the-Day ログイン [7-11](#)

ログイン [7-12](#)

デフォルト設定 [7-11](#)

は

バージョン依存のトランスペアレント モード [17-4](#)

バーチャル プライベート ネットワーク

「VPN」を参照

ハードウェアの制限とレイヤ 3 インターフェイス [14-22](#)

バインディング

DHCP スヌーピング データベース [26-7](#)

表示時 [7-10](#)
 パフォーマンス機能 [1-2](#)
 パフォーマンス、ネットワークの設計 [1-19](#)
 パラレルパス、ルーティングテーブル内 [41-92](#)
 範囲
 インターフェイスの [14-10](#)
 マクロ [14-12](#)

ひ

非 IPv6 トラフィック、フィルタリング [45-3](#)
 非 IP トラフィック フィルタリング [38-28](#)
 ピア、BGP [41-59](#)
 非階層型ポリシー マップ
 設定時の注意事項 [39-34](#)
 説明 [39-10](#)
 光ファイバ、単一方向リンクの検出 [33-1](#)
 非対称リンク、IEEE 802.1Q トンネリング [20-4](#)
 非トランッキングモード [16-16](#)
 非認識 Type-Length-Value (TLV) サポート [17-4](#)
 表示、スイッチアラームの [3-13](#)
 標準範囲 VLAN [16-5](#)
 設定時の注意事項 [16-6](#)
 設定する [16-5](#)
 定義済み [16-1](#)

ふ

ファイル

crashinfo、説明 [53-20](#)

tar

イメージファイルの形式 [A-24](#)

作成する [A-6](#)

抽出する [A-7](#)

内容を表示する [A-7](#)

拡張 crashinfo

説明 [53-20](#)

場所 [53-20](#)

基本 crashinfo

説明 [53-20](#)

場所 [53-20](#)

コピーする [A-5](#)

削除 [A-5](#)

内容を表示する [A-8](#)

ファイル システム

使用可能なファイル システムを表示する [A-2](#)

デフォルトを設定する [A-2](#)

ネットワーク ファイル システム名 [A-5](#)

ファイル情報を表示する [A-3](#)

ローカル ファイル システム名 [A-1](#)

不一致、自動ネゴシエーション [53-8](#)

フィルタ、IP

「ACL、IP」を参照

フィルタリング

IPv6 トラフィック [45-3, 45-7](#)

show コマンドと more コマンドの出力 [2-10](#)

VLAN での [38-31](#)

非 IP トラフィック [38-28](#)

フィルタリング、show コマンドと more コマンドの出力の [2-10](#)

ブーティング

特定のイメージ [4-20](#)

ブート プロセス [4-2](#)

ブートローダ、機能 [4-2](#)

ブートストラップ ルータ (BSR)、説明 [50-7](#)

ブートローダ

アクセス [4-20](#)

環境変数 [4-20](#)

説明 [4-2](#)

トラップ ドア メカニズム [4-2](#)

プロンプト [4-20](#)

フォールバック ブリッジング

STP

hello BPDU インターバル [52-9](#)

VLAN ブリッジ STP [52-2](#)

VLAN ブリッジ スパニングツリー プライオリティ [52-6](#)

インターフェイスでディセーブル [52-10](#)

- インターフェイス プライオリティ **52-7**
- 最大アイドル時間 **52-10**
- 転送遅延時間 **52-9**
- パス コスト **52-7**
- SVI およびルーテッド ポート **52-1**
- VLAN ブリッジ STP **21-11**
- インターフェイスを接続する **14-8**
- 概要 **52-1**
- サポート **1-13**
- サポートされていないプロトコル **52-4**
- 設定時の注意事項 **52-4**
- 説明 **52-1**
- デフォルト設定 **52-3**
- ブリッジ グループ
 - 機能 **52-2**
 - 削除 **52-5**
 - 作成 **52-4**
 - サポートされる数 **52-5**
 - 説明 **52-2**
 - 表示 **52-11**
- ブリッジ テーブル
 - クリア **52-11**
 - 表示 **52-11**
- フレーム転送
 - パケット転送 **52-2**
 - パケットのフラッドイング **52-2**
- プロトコル、未サポート **52-4**
- 保護ポート **52-4**
- 複数認証 **12-13**
- 複数認証モード
 - 設定する **12-42**
- 物理ポート **14-2**
- プライオリティ
 - CoS の上書き **18-6**
 - CoS を信頼する **18-6**
 - HSRP **46-8**
- プライベート VLAN
 - IP アドレス指定 **19-3**
 - SDM テンプレート **19-4**
- SVI **19-5**
- エンド ステーション アクセス **19-3**
- コミュニティ VLAN **19-2, 19-3**
- コミュニティ ポート **19-2**
- サブドメイン **19-1**
- セカンダリ VLAN **19-2**
- 設定 **19-10**
- 設定作業 **19-6**
- 設定時の注意事項 **19-6, 19-7, 19-8**
- デフォルト設定 **19-6**
- 独立 VLAN **19-2, 19-3**
- 独立ポート **19-2**
- トラフィック **19-5**
- 複数のスイッチ間 **19-4**
- プライマリ VLAN **19-1, 19-3**
- ポート
 - コミュニティ **19-2**
 - 設定時の注意事項 **19-8**
 - 説明 **16-4**
 - 独立 **19-2**
 - ホスト ポートの設定 **19-11**
 - 無差別 **19-2**
 - 無差別ポートの設定 **19-12**
- マッピング **19-13**
- 無差別ポート **19-2**
- モニタリング **19-15**
- 利点 **19-1**
- プライベート VLAN エッジ ポート
 - 「保護ポート」を参照
- プライマリ VLAN **19-1, 19-3**
- プライマリ エッジ ポート、REP **24-4**
- プライマリ リンク **25-2**
- フラッシュ デバイス、番号 **A-1**
- フラッド トラフィック、ブロッキング **29-8**
- プリエンブション遅延時間、REP **24-5**
- ブリッジ グループ
 - 「フォールバック ブリッジング」を参照
- ブリッジド パケット、ACL **38-40**
- ブリッジ プロトコル データ ユニット

「BPDU」を参照

プルーニング、VTP

イネーブルにする

VTP ドメインで **17-15**

ポート上での **16-21**

概要 **17-5**

ディセーブルにする

VTP ドメインで **17-15**

ポート上での **16-21**

例 **17-6**

プルーニング適格リスト

VLAN **17-16**

VTP プルーニングの **17-6**

変更する **16-21**

プレフィックス リスト、BGP **41-56**

フロー制御

設定する **14-20**

説明 **14-19**

フローチャート

QoS 出力キューイングとスケジューリング **39-18**

QoS 入力キューイングとスケジューリング **39-16**

QoS 分類 **39-7**

QoS ポリシングとマーキング **39-11**

ブロードキャスト ストーム **29-1, 41-14**

ブロードキャストのフラッディング **41-17**

ブロードキャスト パケット

ダイレクト **41-14**

フラッディング **41-14**

フローベース パケット分類 **1-12**

プロキシ ARP

IP ルーティングがディセーブル **41-11**

設定 **41-11**

定義 **41-9**

プロキシ レポート **25-4**

ブロッキング パケット **29-7**

プロトコル依存モジュール、EIGRP **41-36**

プロトコル ストーム プロテクション **29-21**

プロバイダー エッジ デバイス **41-77**

プロファイル外マークダウン **1-12**

へ

ヘルプ、コマンドライン **2-3**

編集機能

イネーブルとディセーブル **2-7**

使用されたキーストローク **2-8**

ラップされた行 **2-9**

ほ

防止する、不正アクセスを **11-1**

ボーダー ゲートウェイ プロトコル

「BGP」を参照

ポート

IEEE 802.1Q トンネル **16-4**

REP **24-6**

VLAN の割り当て **16-10**

アクセス **14-3**

スイッチ **14-2**

スタティック アクセス **16-3, 16-10**

セキュア **29-9**

ダイナミック アクセス **16-4**

デュアルパーパス アップリンク **14-7**

トランク **16-3, 16-15**

ブロッキング **29-7**

保護される **29-6**

ルーテッド **14-4**

ポート ACL

タイプ **38-3**

定義 **38-2**

ポート VLAN ID TLV **31-2**

ポート記述 TLV **31-1**

ポート シャットダウン応答、VMPS **16-26**

ポート ステータス モニタリング アラーム

FCS Bit Error Rate アラーム **3-3**

Link Fault アラーム **3-3**

Port not Forwarding アラーム **3-3**

Port not Operating アラーム **3-3**

ポート セキュリティ

- QoS 信頼境界と [39-39](#)
- イネーブル化 [29-20](#)
- 違反 [29-10](#)
- エージング [29-18](#)
- スティッキ ラーニング [29-10](#)
- 設定 [29-14](#)
- 説明 [29-9](#)
- デフォルト設定 [29-12](#)
- トランク ポートでの [29-15](#)
- 表示 [29-23](#)
- プライベート VLAN の [29-20](#)
- 他の機能との [29-12](#)
- ポートチャネル
 - 「EtherChannel」を参照
- ポートの信頼状態
 - サポート [1-12](#)
- ポート プライオリティ
 - MSTP [22-20](#)
 - STP [21-17](#)
- ポート ブロックング [1-3, 29-7](#)
- ポートベース認証
 - ACL と RADIUS Filter-Id 属性での [12-31](#)
 - EAPOL-Start フレーム [12-5](#)
 - EAP-Request/Identity フレーム [12-5](#)
 - EAP-Response/Identity フレーム [12-5](#)
 - VLAN 割り当て
 - AAA 認証 [12-39](#)
 - 設定タスク [12-17](#)
 - 説明 [12-16](#)
 - 特性 [12-16](#)
 - Wake-on-LAN、説明 [12-25](#)
 - アカウンティング [12-14](#)
 - アクセス不能認証バイパス
 - 設定する [12-52](#)
 - 説明 [12-23](#)
 - 注意事項 [12-35](#)
 - イネーブル化
 - 802.1x 認証 [13-12](#)
 - 音声 VLAN
 - PVID [12-25](#)
 - VVID [12-25](#)
 - 説明 [12-25](#)
 - 音声認識 802.1x セキュリティ
 - 設定する [12-37](#)
 - 説明 [12-29, 12-37](#)
 - 開始およびメッセージ交換 [12-5](#)
 - カプセル化 [12-3](#)
 - クライアント、定義 [12-3, 13-2](#)
 - ゲスト VLAN
 - 設定時の注意事項 [12-22, 12-23](#)
 - 説明 [12-21](#)
 - 柔軟な認証の順序設定
 - 概要 [12-28](#)
 - 設定する [12-63](#)
 - 準備状態チェック
 - 設定する [12-36](#)
 - 説明 [12-16, 12-36](#)
 - スイッチ
 - RADIUS クライアント [12-3](#)
 - プロキシとして [12-3, 13-2](#)
 - スイッチ サブリカント
 - 概要 [12-29](#)
 - 設定する [12-58](#)
 - 設定
 - RADIUS サーバ [12-42, 13-13](#)
 - 違反モード [12-38 ~ 12-39](#)
 - スイッチからクライアントへの再送信時間 [12-45](#)
 - スイッチ上の RADIUS サーバ パラメータ [12-41, 13-12](#)
 - スイッチとクライアント間のフレーム再送信回数 [12-46](#)
 - 待機時間 [12-44](#)
 - 設定時の注意事項 [12-34, 13-9](#)
 - 設定する
 - 802.1x 認証 [12-39](#)
 - アクセス不能認証バイパス [12-52](#)
 - クライアントの手動での再認証 [12-44](#)
 - ゲスト VLAN [12-49](#)

- 制限付き VLAN [12-50](#)
- 定期的な再認証 [12-43](#)
- ホスト モード [12-42](#)
- 説明 [12-1](#)
- ダウンロード可能 ACL とリダイレクト URL
 - 概要 [12-19 ~ 12-21](#)
 - 設定 [12-60 ~ 12-62, ?? ~ 12-62](#)
- デバイスの役割 [12-2, 13-2](#)
- デフォルト値へのリセット [12-65](#)
- デフォルト設定 [12-33, 13-9](#)
- 統計情報の表示 [12-65, 13-17](#)
- 統計情報、表示する [12-65](#)
- 認証サーバ
 - RADIUS サーバ [12-3](#)
 - 定義 [12-3, 13-2](#)
- 複数認証 [12-13](#)
- 方式リスト [12-39](#)
- ポート
 - 音声 VLAN [12-25](#)
 - 許可および無許可 [12-10](#)
 - 許可ステートおよび dot1x port-control コマンド [12-10](#)
- ポートあたりのデバイスの最大数 [12-36](#)
- ポート セキュリティ
 - 説明 [12-25](#)
- ホスト モード [12-11](#)
- マジック パケット [12-25](#)
- ユーザ単位 ACL
 - AAA 許可 [12-39](#)
 - 設定タスク [12-18](#)
 - 説明 [12-17](#)
- ユーザ単位の ACL
 - RADIUS サーバ属性 [12-18](#)
- ユーザ ディストリビューション
 - 概要 [12-27](#)
 - 注意事項 [12-27](#)
- ポートベース認証方式、サポートされる [12-7](#)
- ポート メンバーシップ モード、VLAN [16-3](#)
- 保護ポート [1-9, 29-6](#)
- 補助 VLAN
 - 「音声 VLAN」を参照
- ホスト、ダイナミック ポートでの制限 [16-31](#)
- ホスト ポート
 - 種類 [19-2](#)
 - 設定 [19-11](#)
- ホスト名、クラスタでの [6-14](#)
- ポリシーベース ルーティング
 - 「PBR」を参照
- ポリシー マップ、QoS の
 - SVI での階層
 - 設定時の注意事項 [39-34](#)
 - 設定する [39-53](#)
 - 説明 [39-12](#)
 - 階層 [39-9](#)
 - 説明 [39-8](#)
 - 特性 [39-49](#)
 - 表示する [39-80](#)
 - 物理ポートでの非階層
 - 設定時の注意事項 [39-34](#)
 - 説明 [39-10](#)
- ポリシング
 - 階層
 - 「階層型ポリシー マップ」を参照
 - 説明 [39-4](#)
 - トークン バケット アルゴリズム [39-10](#)
 - ポリシング機能
 - 数 [39-35](#)
 - 設定する
 - 各一致トラフィック クラスでの [39-49](#)
 - 複数トラフィック クラスでの [39-60](#)
 - 説明 [39-4](#)
 - タイプ [39-10](#)
 - 表示する [39-80](#)
 - ポリシング済み DSCP マップ、QoS での [39-65](#)

ま

マーキング

集約ポリシング機能でのアクション **39-60**

説明 **39-4, 39-9**

マジック パケット **12-25**

マッピング テーブル、QoS の
設定する

- CoS/DSCP **39-63**
- DSCP **39-62**
- DSCP/CoS **39-66**
- DSCP/DSCP 変換 **39-67**
- IP precedence/DSCP **39-64**
- ポリシング済み DSCP **39-65**

説明 **39-13**

マルチ VRF CE

- 表示 **41-90**
- モニタリング **41-90**

マルチオペレーションのスケジューリング、IP
SLA **47-5**

マルチキャスト TV アプリケーション **28-18**

マルチキャスト VLAN **28-18**

マルチキャスト VLAN レジストレーション
「MVR」を参照

マルチキャスト グループ

- 加入 **28-3**
- スタティックな加入 **28-10, 44-8**
- 即時脱退 **28-6**
- 脱退 **28-5**

マルチキャスト ストーム **29-1**

マルチキャスト パケット

- ACL **38-41**
- ブロッキング **29-8**

マルチキャスト ルータ インターフェイス、モニタリ
ング **28-17, 44-12**

マルチキャスト ルータ ポート、追加する **28-9, 44-8**

マルチドメイン認証
「MDA」を参照

み

ミラーリング トラフィック、分析用の **30-1**

む

無許可ポート、IEEE 802.1x での **12-10**

無差別ポート

設定 **19-12**

定義 **19-2**

矛盾、設定 **53-8**

め

メッセージ、ユーザに対するバナーを使用した **7-10**

メトリック、BGP 内 **41-53**

メトリック変換、ルーティング プロトコル間 **41-98**

メトロ タグ **20-2**

メンバーシップ モード、VLAN ポート **16-3**

メンバ スイッチ

失われた接続性から回復する **53-8**

管理する **6-16**

「候補スイッチ」、「クラスタ スタンバイ グループ」、
「スタンバイ コマンド スイッチ」も参照

自動検出 **6-4**

定義済み **6-1**

パスワード **6-14**

要件 **6-3**

も

モジュール番号 **14-8**

モニタリング

BGP **41-64**

CDP **32-5**

CEF **41-91**

EIGRP **41-43**

Flex Link **25-15**

HSRP **46-13**

IEEE 802.1Q トンネリング **20-18**

IGMP

スヌーピング **28-16, 44-12**

フィルタ **28-30**

- IP
- アドレス テーブル [41-18](#)
 - マルチキャスト ルーティング [50-63](#)
 - ルート [41-106](#)
- IP SLA 動作 [47-13](#)
- IPv4 ACL 設定 [38-43](#)
- IPv6 [42-28](#)
- IPv6 ACL 設定 [45-8](#)
- IS-IS [41-75](#)
- ISO CLNS [41-75](#)
- MAC アドレス テーブル移動更新 [25-15](#)
- MSDP ピア [51-18](#)
- MVR [28-24](#)
- OSPF [41-35](#)
- PROFINET [9-5](#)
- PTP [8-4](#)
- REP [24-15](#)
- RP マッピング情報 [50-36](#)
- SFP ステータス [14-27, 53-10](#)
- Source-Active メッセージ [51-18](#)
- SSM マッピング [50-23](#)
- VLAN [16-15](#)
- フィルタ [38-43](#)
 - マップ [38-43](#)
- VMPS [16-31](#)
- VTP [17-18](#)
- アクセス グループ [38-43](#)
 - アラーム [3-13](#)
 - インターフェイス [14-26](#)
 - オブジェクト トラッキング [48-13](#)
 - 機能 [1-14](#)
 - スイッチ間でのトラフィック フロー [34-1](#)
 - 速度モードとデュプレックス モード [14-19](#)
 - 単方向リンク用のケーブル [33-1](#)
 - トラフィックの抑制 [29-22](#)
 - トンネリング [20-18](#)
 - フォールバックブリッジング [52-11](#)
 - プライベート VLAN [19-15](#)
 - プローブでの分析用のネットワーク トラフィック [30-2](#)
 - ポート
 - ブロッキング [29-23](#)
 - 保護 [29-23](#)
 - マルチ VRF CE [41-90](#)
 - マルチキャスト ルータ インターフェイス [28-17, 44-12](#)
 - レイヤ 2 プロトコル トンネリング [20-18](#)
-
- ゆ
- ユーザ EXEC モード [2-2](#)
 - ユーザ単位 ACL と Filter-Id [12-8](#)
 - ユーザ データグラム プロトコル
 - 「UDP」を参照
 - ユーザ名ベース認証 [11-7](#)
 - 優先処理、トラフィックの
 - 「QoS」を参照
 - 優先遅延、デフォルト設定 [25-8](#)
 - 優先、デフォルト設定 [25-8](#)
 - 誘導ユニキャスト要求 [1-5](#)
 - ユニキャスト MAC アドレス フィルタリング [1-5](#)
 - CPU パケットと [7-21](#)
 - スタティック アドレスを追加する [7-22](#)
 - 設定時の注意事項 [7-21](#)
 - 説明 [7-21](#)
 - ブロードキャスト MAC アドレスと [7-21](#)
 - マルチキャスト アドレスと [7-21](#)
 - ルータ MAC アドレスと [7-21](#)
 - ユニキャスト ストーム [29-1](#)
 - ユニキャスト トラフィック、ブロッキング [29-8](#)
-
- よ
- 予約アドレス、DHCP プールでの [26-30](#)

ら

ライン コンフィギュレーション モード [2-3](#)

り

リークする、IGMP レポートを [25-4](#)

リセット、BGP 内 [41-51](#)

リダイレクト URL [12-19](#), [12-20](#), [12-60](#)

リトライ回数、VMPS、変更する [16-30](#)

リモート SPAN

「RSPAN」を参照

リモート コピー プロトコル

「RCP」を参照

リモート ネットワーク モニタリング

「RMON」を参照

履歴

コマンドを呼び出す [2-6](#)

説明 [2-6](#)

ディセーブルにする [2-7](#)

バッファ サイズを変更する [2-6](#)

履歴テーブル、Syslog メッセージのレベルと番号 [35-10](#)

リロードする、ソフトウェアを [4-22](#)

リンク完全性、REP を使用した確認 [24-3](#)

リンク障害、単一方向の検出 [22-8](#)

リンク冗長性

「Flex Link」を参照

リンクステート トラッキング

設定する [40-24](#)

説明 [40-22](#)

リンクステート プロトコル [41-3](#)

リンク、単方向 [33-1](#)

リンク ローカル ユニキャスト アドレス [42-3](#)

隣接テーブル、CEF [41-91](#)

タイプ [38-4](#)

定義 [38-2](#)

ルータ ID、OSPF [41-34](#)

ルーティング

情報の再配信 [41-95](#)

スタティック [41-3](#)

ダイナミック [41-3](#)

デフォルト [41-3](#)

ルーティングできないプロトコルの転送 [52-1](#)

ルーティング ドメイン連合、BGP [41-62](#)

ルーティング プロトコルのアドミニストレーティブ ディスタンス [41-93](#)

ルーテッド パケット、ACL [38-41](#)

ルーテッド ポート

IP アドレス [14-22](#), [41-4](#)

スイッチ クラスタでの [6-9](#)

設定 [41-3](#)

定義済み [14-4](#)

ルート ガード

イネーブルにする [23-16](#)

サポート [1-7](#)

説明 [23-8](#)

ルート計算タイマー、OSPF [41-32](#)

ルート スイッチ

MSTP [22-18](#)

STP [21-15](#)

ルート選択、BGP [41-52](#)

ルート ターゲット、VPN [41-78](#)

ルート ダンプニング、BGP [41-63](#)

ルート マップ

BGP [41-54](#)

ポリシーベース ルーティング [41-99](#)

ルート リフレクタ、BGP [41-62](#)

ループ ガード

イネーブルにする [23-16](#)

サポート [1-7](#)

説明 [23-9](#)

る

ルータ ACL

れ

例

ネットワーク設定 [1-18](#)

レイヤ 2 traceroute

1 ポートに複数のデバイス [53-13](#)

ARP [53-12](#)

CDP [53-12](#)

IP アドレスおよびサブネット [53-12](#)

MAC アドレスおよび VLAN [53-12](#)

使用上の注意事項 [53-12](#)

説明 [53-12](#)

ブロードキャスト トラフィック [53-12](#)

マルチキャスト トラフィック [53-12](#)

ユニキャスト トラフィック [53-12](#)

レイヤ 2 インターフェイス、デフォルト設定 [14-14](#)レイヤ 2 フレーム、CoS での分類 [39-2](#)

レイヤ 2 プロトコル トンネリング

EtherChannel の設定 [20-15](#)

設定 [20-11](#)

注意事項 [20-12](#)

定義 [20-8](#)

デフォルト設定 [20-12](#)

レイヤ 2 プロトコル パケットのシャットダウンしきい値 [20-12](#)レイヤ 2 プロトコル パケットのドロップしきい値 [20-12](#)

レイヤ 3 インターフェイス

IPv4 アドレスと IPv6 アドレスを割り当てる [42-15](#)

IPv6 アドレスを割り当てる [42-12](#)

IP アドレスの割り当て [41-6](#)

タイプ [41-3](#)

レイヤ 2 モードからの変更 [41-6, 41-83](#)

レイヤ 3 機能 [1-13](#)レイヤ 3 パケット、分類方式 [39-2](#)

レポート抑制、IGMP

説明 [28-6](#)

ディセーブルにする [28-16, 44-11](#)

ろ

ローカル SPAN [30-2](#)

ロード バランシング [46-4](#)

ロギング メッセージ、ACL [38-8](#)

ログイン認証

RADIUS での [11-31](#)

TACACS+ での [11-15](#)

ログイン バナー [7-10](#)

ログ メッセージ

「システム メッセージ ロギング」を参照

ロケーション TLV [31-2, 31-7](#)

わ

ワイヤード ロケーション サービス

概要 [31-3](#)

設定する [31-9](#)

表示する [31-10](#)

ロケーション TLV [31-2](#)

割り当て、アラーム プロファイルのポートへの [3-12](#)

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>