



Catalyst 3750 スイッチ ソフトウェア コンフィギュレーション ガイド

Catalyst 3750 Switch Software Configuration Guide

Cisco IOS Release 12.2(52)SE

2009 年 9 月

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

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

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

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

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

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

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

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

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

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

Catalyst 3750 スイッチ ソフトウェア コンフィギュレーション ガイド

Copyright © 2004–2009 Cisco Systems, Inc.

All rights reserved.

Copyright © 2004–2010, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

はじめに	xlix
対象読者	xlix
目的	xlix
表記法	I
関連資料	I
マニュアルの入手方法およびテクニカル サポート	lii

CHAPTER 1

概要	1-1
機能	1-1
使用および導入を簡素化する機能	1-2
パフォーマンス向上機能	1-4
管理オプション	1-6
管理の簡易性に関する機能	1-6
アベイラビリティおよび冗長性に関する機能	1-8
VLAN 機能	1-9
セキュリティ機能	1-10
QoS および CoS 機能	1-13
レイヤ 3 機能	1-14
PoE 機能	1-16
モニタ機能	1-16
スイッチ初期設定後のデフォルト値	1-17
ネットワークの構成例	1-20
スイッチを使用する場合の設計概念	1-20
Catalyst 3750 スイッチを使用した中小規模のネットワーク	1-26
Catalyst 3750 スイッチによる大規模ネットワーク	1-27
Catalyst 3750 スイッチによる集合住宅ネットワーク	1-28
長距離広帯域トランスポートの構成	1-30
次の作業	1-30

CHAPTER 2

CLI の使用方法	2-1
コマンド モードの概要	2-1
ヘルプ システムの概要	2-3
コマンドの省略形	2-4
コマンドの no 形式および default 形式の概要	2-4

CLI のエラー メッセージ	2-5
コンフィギュレーション ロギングの使用法	2-5
コマンド履歴の使用法	2-6
コマンド履歴バッファ サイズの変更	2-6
コマンドの呼び出し	2-6
コマンド履歴機能のディセーブル化	2-7
編集機能の使用法	2-7
編集機能のイネーブル化およびディセーブル化	2-7
キーストロークによるコマンドの編集	2-7
画面幅よりも長いコマンドラインの編集	2-9
show および more コマンド出力の検索およびフィルタリング	2-10
CLI のアクセス	2-10
コンソール接続または Telnet による CLI アクセス	2-11

CHAPTER 3

スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て	3-1
起動プロセスの概要	3-2
スイッチ情報の割り当て	3-3
デフォルトのスイッチ情報	3-3
DHCP ベースの自動設定の概要	3-4
DHCP クライアントの要求プロセス	3-4
DHCP ベースの自動設定およびイメージ アップデートの概要	3-5
DHCP 自動設定	3-6
DHCP 自動イメージ アップデート	3-6
制限事項	3-6
DHCP ベースの自動設定の設定	3-7
DHCP サーバ設定時の注意事項	3-7
TFTP サーバの設定	3-8
DNS の設定	3-9
リレー デバイスの設定	3-9
コンフィギュレーション ファイルの入手方法	3-10
構成例	3-11
DHCP の自動設定およびイメージ アップデート機能の設定	3-12
DHCP 自動設定の設定 (コンフィギュレーション ファイルのみ)	3-12
DHCP の自動イメージ アップデートの設定 (コンフィギュレーション ファイルとイメージ)	3-13
クライアントの設定	3-15
手動でのスイッチ情報の割り当て	3-16
実行コンフィギュレーションの確認および保存	3-17
スタートアップ コンフィギュレーションの変更	3-18

起動のデフォルト設定	3-18
コンフィギュレーション ファイルの自動ダウンロード	3-18
システム コンフィギュレーションを読み書きするためのファイル名の指定	3-19
手動で起動する場合	3-19
特定のソフトウェア イメージを起動する場合	3-20
環境変数の制御	3-21
ソフトウェア イメージ リロードのスケジュール設定	3-22
リロードのスケジュール設定	3-23
リロード スケジュール情報の表示	3-24

CHAPTER 4

Cisco IOS Configuration Engine の設定	4-1
Cisco Configuration Engine ソフトウェアの概要	4-1
コンフィギュレーション サービス	4-2
イベント サービス	4-3
NSM	4-3
CNS ID およびデバイスのホスト名に関する重要事項	4-3
ConfigID	4-4
DeviceID	4-4
ホスト名および DeviceID	4-4
ホスト名、DeviceID、ConfigID の使用方法	4-5
Cisco IOS エージェントの概要	4-5
初期設定	4-5
差分（部分）設定	4-6
同期設定	4-6
Cisco IOS エージェントの設定	4-6
自動 CNS 設定のイネーブル化	4-7
CNS イベント エージェントのイネーブル化	4-8
Cisco IOS CNS エージェントのイネーブル化	4-9
初期設定のイネーブル化	4-9
部分設定のイネーブル化	4-13
CNS 設定の表示	4-14

CHAPTER 5

スイッチ スタックの管理	5-1
スタックの概要	5-1
スタック メンバシップ	5-3
マスターの選択	5-4
スタック MAC アドレスとルータ MAC アドレス	5-5
メンバー番号	5-6
メンバーのプライオリティ値	5-6

スタックのオフライン設定	5-7	
割り当てられたスイッチのスタックへの追加による影響	5-7	
スタックの割り当てられたスイッチの交換による影響	5-9	
割り当てられたスイッチのスタックからの削除による影響	5-9	
スイッチ スタックのハードウェア互換性と SDM 不一致モード	5-9	
スタックのソフトウェア互換性に関する推奨事項	5-9	
スタック プロトコル バージョンの互換性	5-10	
スイッチ間のメジャー バージョン番号の非互換性	5-10	
スイッチ間のマイナー バージョン番号の非互換性	5-10	
自動アップグレードおよび自動アドバイスの概要	5-11	
自動アップグレードおよび自動アドバイスのメッセージ例	5-12	
互換性のないソフトウェアおよびメンバー イメージのアップグレード	5-14	
スタックのコンフィギュレーション ファイル	5-14	
スイッチ スタックのシステム全体の設定に関する補足考慮事項	5-15	
スタックの管理接続	5-16	
IP アドレスによるスタックへの接続	5-16	
SSH セッションによるスタックへの接続	5-16	
コンソール ポートによるスタックへの接続	5-16	
特定のメンバーへの接続	5-16	
スタックの設定のシナリオ	5-17	
スイッチ スタックの設定	5-18	
デフォルトのスイッチ スタック コンフィギュレーション	5-19	
固定 MAC アドレスのイネーブル化	5-19	
スタック メンバー情報の割り当て	5-21	
メンバー番号の割り当て	5-21	
スタック メンバー プライオリティ 値の設定	5-21	
スタックへの新しいメンバーの割り当て	5-22	
スタック メンバシップの変更	5-23	
特定のスタック メンバーへの CLI アクセス	5-23	
スタック情報の表示	5-23	
スタックのトラブルシューティング	5-24	
手動での StackWise ポートのディセーブル化	5-24	
他のメンバーの起動中に StackWise ポートを再度イネーブルにする方法	5-25	
show switch stack-ports summary コマンド出力の概要	5-25	
ループバック問題の特定	5-26	
ソフトウェア ループバック	5-27	
ソフトウェア ループバックの例 : StackWise ケーブルが接続されていない場合	5-28	
ソフトウェア ループバックの例 : StackWise ケーブルが接続されている場合	5-28	
ハードウェア ループバック	5-29	

ハードウェア ループバックの例 : LINK OK イベント	5-29
ハードウェア ループバックの例 : LINK NOT OK イベント	5-30
切断されている StackWise ケーブルの検出	5-31
StackWise ポート間の接続障害の解決	5-32

CHAPTER 6**スイッチのクラスタ化** 6-1

スイッチ クラスタの概要	6-2
クラスタ コマンド スイッチの特性	6-3
スタンバイ クラスタ コマンド スイッチの特性	6-3
候補スイッチおよびクラスタ メンバー スイッチの特性	6-4
スイッチ クラスタのプランニング	6-5
クラスタ候補およびクラスタ メンバーの自動検出	6-5
CDP ホップを使用しての検出	6-6
CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出	6-6
異なる VLAN からの検出	6-7
異なる管理 VLAN からの検出	6-8
RP による検出	6-9
新しくインストールしたスイッチの検出	6-10
HSRP およびスタンバイ クラスタ コマンド スイッチ	6-11
仮想 IP アドレス	6-12
クラスタ スタンバイ グループに関する他の考慮事項	6-12
クラスタ設定の自動復旧	6-13
IP アドレス	6-14
ホスト名	6-14
パスワード	6-15
SNMP コミュニティ スtring	6-15
スイッチ クラスタとスイッチ スタック	6-15
Terminal Access Controller Access Control System Plus (TACACS+) および Remote Authentication Dial In User Service (RADIUS)	6-17
LRE プロファイル	6-17
CLI によるスイッチ クラスタの管理	6-17
Catalyst1900 および Catalyst2820 の CLI に関する考慮事項	6-18
SNMP によるスイッチ クラスタの管理	6-18

CHAPTER 7**スイッチの管理** 7-1

システム日時の管理	7-1
システム クロックの概要	7-2
NTP の概要	7-2
NTP の設定	7-4

NTP のデフォルト設定	7-4
NTP 認証の設定	7-5
NTP アソシエーションの設定	7-6
NTP ブロードキャスト サービスの設定	7-7
NTP アクセス制限の設定	7-8
NTP パケット用の送信元 IP アドレスの設定	7-10
NTP 設定の表示	7-11
手動での日時の設定	7-11
システム クロックの設定	7-12
日時設定の表示	7-12
タイム ゾーンの設定	7-13
夏時間の設定	7-14
システム名とプロンプトの設定	7-15
デフォルトのシステム名およびプロンプトの設定	7-16
システム名の設定	7-16
DNS の概要	7-16
DNS のデフォルト設定	7-17
DNS の設定	7-17
DNS の設定の表示	7-18
バナーの作成	7-18
バナーのデフォルト設定	7-19
MoTD ログイン バナーの設定	7-19
ログイン バナーの設定	7-20
MAC アドレス テーブルの管理	7-20
アドレス テーブルの作成	7-21
MAC アドレスおよび VLAN	7-21
MAC アドレスおよびスイッチ スタック	7-22
MAC アドレス テーブルのデフォルト設定	7-22
アドレス エージング タイムの変更	7-22
ダイナミック アドレス エントリの削除	7-23
MAC アドレス変更通知トラップの設定	7-23
MAC アドレス移行通知トラップの設定	7-25
MAC しきい値通知トラップの設定	7-27
スタティック アドレス エントリの追加および削除	7-28
ユニキャスト MAC アドレス フィルタリングの設定	7-29
VLAN での MAC アドレス ラーニングのディセーブル化	7-30
アドレス テーブル エントリの表示	7-32
ARP テーブルの管理	7-32

CHAPTER 8

SDM テンプレートの設定	8-1
SDM テンプレートの概要	8-1
デュアル IPv4/IPv6 SDM テンプレート	8-2
SDM テンプレートとスイッチ スタック	8-4
スイッチ SDM テンプレートの設定	8-5
デフォルトの SDM テンプレート	8-5
SDM テンプレートの設定時の注意事項	8-5
SDM テンプレートの設定	8-6
SDM テンプレートの表示	8-7

CHAPTER 9

スイッチ ベース認証の設定	9-1
スイッチへの不正アクセスの防止	9-1
特権 EXEC コマンドへのアクセスの保護	9-2
デフォルトのパスワードおよび権限レベル設定	9-3
スタティック イネーブル パスワードの設定または変更	9-3
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護	9-4
パスワード回復のディセーブル化	9-5
端末回線に対する Telnet パスワードの設定	9-6
ユーザ名とパスワードのペアの設定	9-7
複数の権限レベルの設定	9-8
コマンドの権限レベルの設定	9-8
回線に対するデフォルトの権限レベルの変更	9-9
権限レベルへのログインおよび終了	9-10
TACACS+ によるスイッチ アクセスの制御	9-10
TACACS+ の概要	9-10
TACACS+ の動作	9-12
TACACS+ の設定	9-13
TACACS+ のデフォルト設定	9-13
TACACS+ サーバ ホストの特定および認証鍵の設定	9-13
TACACS+ ログイン認証の設定	9-14
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定	9-16
TACACS+ アカウンティングの起動	9-17
TACACS+ 設定の表示	9-18
RADIUS によるスイッチ アクセスの制御	9-18
RADIUS の概要	9-18
RADIUS の動作	9-20
RADIUS Change of Authorization (CoA)	9-20
概要	9-21

要求に関する Change-of-Authorization	9-21
CoA 要求応答コード	9-23
CoA 要求コマンド	9-24
セッション終了のスタッキングの注意事項	9-26
RADIUS の設定	9-27
RADIUS のデフォルト設定	9-28
RADIUS サーバ ホストの識別	9-28
RADIUS ログイン認証の設定	9-30
AAA サーバ グループの定義	9-32
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定	9-34
RADIUS アカウンティングの起動	9-35
すべての RADIUS サーバの設定	9-36
ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定	9-36
ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定	9-38
スイッチ上での CoA 設定	9-39
CoA 機能のモニタリングとトラブルシューティング	9-40
RADIUS サーバ ロード バランシングの設定	9-40
RADIUS の設定の表示	9-40
Kerberos によるスイッチ アクセスの制御	9-40
Kerberos の概要	9-41
Kerberos の動作	9-43
境界スイッチに対する認証の取得	9-43
KDC からの TGT の取得	9-43
ネットワーク サービスに対する認証の取得	9-44
Kerberos の設定	9-44
スイッチのローカル認証および許可の設定	9-45
SSH のためのスイッチの設定	9-46
SSH の概要	9-46
SSH サーバ、統合クライアント、およびサポートされているバージョン	9-47
制限事項	9-47
SSH の設定	9-48
設定時の注意事項	9-48
スイッチで SSH を実行するためのセットアップ	9-48
SSH サーバの設定	9-49
SSH の設定およびステータスの表示	9-50
SSL HTTP のためのスイッチの設定	9-51
セキュア HTTP サーバおよびクライアントの概要	9-51
CA の信頼点	9-51
CipherSuite	9-53

セキュア HTTP サーバおよびクライアントの設定	9-53
SSL のデフォルト設定	9-53
SSL の設定時の注意事項	9-54
CA の信頼点の設定	9-54
セキュア HTTP サーバの設定	9-55
セキュア HTTP クライアントの設定	9-56
セキュア HTTP サーバおよびクライアントのステータスの表示	9-57
SCP のためのスイッチの設定	9-57
Secure Copy に関する情報	9-58

CHAPTER 10

IEEE 802.1X ポートベース認証の設定	10-1
IEEE 802.1X ポートベース認証の概要	10-1
デバイスの役割	10-2
認証プロセス	10-3
認証の開始およびメッセージ交換	10-5
認証マネージャ	10-7
ポートベース認証	10-7
ユーザ単位 ACL と Filter-Id	10-8
認証マネージャの CLI コマンド	10-9
許可ステートおよび無許可ステートのポート	10-10
802.1X 認証とスイッチ スタック	10-11
802.1X のホスト モード	10-12
マルチドメイン認証	10-12
802.1X マルチ認証モード	10-14
MAC 移動	10-14
802.1X アカウンティング	10-15
802.1X アカウンティング アトリビュート値 (AV) ペア	10-15
802.1X 準備チェック	10-16
VLAN 割り当てを使用した 802.1X 認証	10-16
ユーザ単位 ACL を使用した 802.1X 認証の利用	10-18
ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証	10-19
リダイレクト URL に対する Cisco Secure ACS とアトリビュート値 (AV) ペア	10-19
ダウンロード可能な ACL に対する Cisco Secure ACS と AV ペア	10-20
VLAN ID ベースの MAC 認証	10-20
ゲスト VLAN を使用した 802.1X 認証	10-21
制限付き VLAN による 802.1X 認証	10-22
アクセス不能認証バイパスによる 802.1X 認証	10-23
マルチ認証ポートに関するサポート	10-23
認証結果	10-23

相互作用機能	10-23	
音声 VLAN ポートを使用した 802.1X 認証	10-24	
ポート セキュリティを使用した 802.1X 認証	10-25	
Wake-on-LAN (WoL) 機能を使用した 802.1X 認証	10-26	
MAC 認証バイパスを使用した 802.1X 認証	10-26	
802.1X ユーザ分散	10-28	
802.1X ユーザ分散設定時の注意事項	10-28	
NAC レイヤ 2 802.1X 検証	10-28	
柔軟な認証の順序	10-29	
Open1x 認証	10-29	
音声認識 802.1X セキュリティの使用	10-30	
Network Edge Access Topology (NEAT) を使用した 802.1X サプリカント スイッチ およびオーセンティケータ スイッチ	10-30	
注意事項	10-31	
ACL および RADIUS Filter-Id アトリビュートによる IEEE 802.1X 認証の使用	10-31	
共通セッション ID	10-32	
802.1X 認証の設定	10-33	
802.1X 認証のデフォルト設定	10-34	
802.1X 認証設定時の注意事項	10-35	
802.1X 認証	10-35	
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス	10-36	
MAC 認証バイパス	10-36	
ポートごとに許可できるデバイスの最大数	10-37	
802.1X 準備チェックの設定	10-37	
音声認識 802.1X セキュリティの設定	10-38	
802.1X 違反モードの設定	10-39	
802.1X 認証の設定	10-40	
スイッチおよび RADIUS サーバ間の通信の設定	10-42	
ホスト モードの設定	10-43	
定期的な再認証の設定	10-44	
ポートに接続するクライアントの手動での再認証	10-45	
待機時間の変更	10-46	
スイッチからクライアントへの再送信時間の変更	10-46	
スイッチからクライアントへのフレーム再送信回数の設定	10-47	
再認証回数設定	10-48	
MAC 移動のイネーブル化	10-49	
802.1X アカウンティングの設定	10-49	
ゲスト VLAN の設定	10-50	
制限付き VLAN の設定	10-51	

アクセス不能認証バイパス機能の設定	10-53
WoL を使用した 802.1X 認証の設定	10-55
MAC 認証バイパスの設定	10-56
802.1X ユーザ分散の設定	10-57
NAC レイヤ 2 802.1X 検証の設定	10-58
NEAT を使用したオーセンティケータおよびサブリカント スイッチの設定	10-59
Auto Smartport (ASP) による NEAT の設定	10-61
ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定	10-61
ダウンロード可能な ACL の設定	10-61
ダウンロード ポリシーの設定	10-62
VLAN ID ベースの MAC 認証の設定	10-63
認証の順序を柔軟に設定	10-64
Open1x の設定	10-64
ポート上での 802.1X 認証のディセーブル化	10-65
802.1X 認証設定のデフォルト値へのリセット	10-66
802.1X の統計情報およびステータスの表示	10-66

CHAPTER 11

Web ベース認証の設定	11-1
Web ベース認証の概要	11-1
デバイスの役割	11-2
ホスト検出	11-2
セッションの作成	11-3
認証プロセス	11-3
ローカル Web 認証バナー	11-4
Web 認証のカスタマイズ可能な Web ページ	11-6
注意事項	11-6
Web ベース認証とその他の機能の相互作用	11-7
ポート セキュリティ	11-7
LAN ポート IP (LPIP)	11-8
ゲートウェイ IP (GWIP)	11-8
ACL	11-8
コンテキスト ベース アクセス コントロール (CBAC)	11-8
802.1X 認証	11-8
EtherChannel	11-8
Web ベース認証の設定	11-9
Web ベース認証のデフォルト設定	11-9
Web ベース認証の設定時の注意事項および制限事項	11-9
Web ベース認証設定のタスク リスト	11-10
認証ルールとインターフェイスの設定	11-10

AAA 認証の設定	11-11
スイッチと RADIUS サーバ間の通信設定	11-12
HTTP サーバの設定	11-13
認証プロキシ Web ページのカスタマイズ	11-14
ログインに成功した場合のリダイレクション URL の指定	11-15
AAA 失敗ポリシーの設定	11-16
Web ベース認証パラメータの設定	11-16
Web 認証ローカル バナーの設定	11-17
Web ベース認証のキャッシュ エントリの削除	11-17
Web ベース認証ステータスの表示	11-18

CHAPTER 12

インターフェイス特性の設定	12-1
インターフェイス タイプの概要	12-1
ポートベースの VLAN	12-2
スイッチ ポート	12-3
アクセス ポート	12-3
トランク ポート	12-4
トンネル ポート	12-4
ルーテッド ポート	12-5
スイッチ仮想インターフェイス	12-5
SVI Autostate Exclude	12-6
EtherChannel ポート グループ	12-7
10 ギガビット イーサネット インターフェイス	12-7
Power over Ethernet (PoE) ポート	12-8
サポート対象の protocol および標準	12-8
受電装置検出および初期電力割り当て	12-9
電力管理モード	12-10
インターフェイスの接続	12-11
インターフェイス コンフィギュレーション モードの使用法	12-12
インターフェイスの設定手順	12-13
インターフェイス範囲の設定	12-14
インターフェイス レンジ マクロの設定および使用法	12-15
イーサネット インターフェイスの設定	12-17
イーサネット インターフェイスのデフォルト設定	12-18
10 ギガビット イーサネット インターフェイスの設定時の注意事項	12-19
インターフェイス速度およびデュプレックス モードの設定	12-19
速度とデュプレックス モードの設定時の注意事項	12-20
インターフェイス速度およびデュプレックス パラメータの設定	12-21
IEEE 802.3X フロー制御の設定	12-22

インターフェイスでの Auto-MDIX の設定	12-23
PoE ポートの電力管理モードの設定	12-24
PoE ポートに接続された受電装置のパワー バジェット	12-25
インターフェイスに関する記述の追加	12-27
レイヤ 3 インターフェイスの設定	12-28
SVI Autostate Exclude の設定	12-29
システム MTU の設定	12-30
Cisco 冗長電源システム (RPM) 2300 の設定	12-32
インターフェイスのモニタリングおよびメンテナンス	12-34
インターフェイス ステータスのモニタ	12-34
インターフェイスおよびカウンタのクリアとリセット	12-35
インターフェイスのシャットダウンおよび再起動	12-36

CHAPTER 13

Auto Smartport マクロの設定	13-1
Auto Smartport マクロおよびスタティック Smartports マクロの概要	13-1
Auto Smartport および Cisco Medianet	13-2
Auto Smartport の設定	13-3
デフォルトの Auto Smartport 設定	13-3
Auto Smartport の設定に関する注意事項	13-4
Auto Smartport のイネーブル化	13-5
Auto Smartport デフォルト パラメータ値の設定	13-5
Auto Smartport MAC アドレス グループの設定	13-7
Auto Smartport マクロ固定の設定	13-8
Auto Smartport 組み込みマクロ オプションの設定	13-9
ユーザ定義イベント トリガーの作成	13-11
Auto Smartport ユーザ定義マクロの設定	13-15
スタティック Smartport マクロの設定	13-17
デフォルトのスタティック Smartport 設定	13-17
スタティック Smartport コンフィギュレーションに関する注意事項	13-17
スタティック Smartport マクロの適用	13-18
Auto Smartport マクロおよびスタティック Smartport マクロの表示	13-20

CHAPTER 14

VLAN の設定	14-1
VLAN の概要	14-1
サポートされる VLAN	14-3
VLAN ポート メンバシップ モード	14-3
標準範囲 VLAN の設定	14-5
トークン リング VLAN	14-6

標準範囲 VLAN 設定時の注意事項	14-6
標準範囲 VLAN の設定	14-7
イーサネット VLAN のデフォルト設定	14-8
イーサネット VLAN の作成または変更	14-8
VLAN の削除	14-9
VLAN へのスタティック アクセス ポートの割り当て	14-10
拡張範囲 VLAN の設定	14-11
VLAN のデフォルト設定	14-11
拡張範囲 VLAN 設定時の注意事項	14-11
拡張範囲 VLAN の作成	14-12
内部 VLAN ID を指定した拡張範囲 VLAN の作成	14-14
VLAN の表示	14-15
VLAN トランクの設定	14-15
トランキングの概要	14-15
カプセル化タイプ	14-17
IEEE 802.1Q の設定に関する考慮事項	14-18
レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定	14-18
トランク ポートとしてのイーサネット インターフェイスの設定	14-19
他の機能との相互作用	14-19
トランク ポートの設定	14-20
トランクでの許可 VLAN の定義	14-21
プルーニング適格リストの変更	14-22
タグなしトラフィック用ネイティブ VLAN の設定	14-23
トランク ポートの負荷分散の設定	14-23
STP ポート プライオリティによる負荷分散	14-24
STP パス コストによる負荷分散	14-26
VMPS の設定	14-27
VMPS の概要	14-27
ダイナミック アクセス ポート VLAN メンバシップ	14-28
VMPS クライアントのデフォルト設定	14-29
VMPS 設定時の注意事項	14-29
VMPS クライアントの設定	14-30
VMPS の IP アドレスの入力	14-30
VMPS クライアント上のダイナミック アクセス ポートの設定	14-30
VLAN メンバシップの再確認	14-31
再確認インターバルの変更	14-31
再試行回数の変更	14-32
VMPS のモニタリング	14-32
ダイナミック アクセス ポート VLAN メンバシップのトラブルシューティング	14-33

VMPS の設定例	14-33
-----------	-------

CHAPTER 15
VTP の設定 15-1

VTP の概要	15-1
VTP ドメイン	15-2
VTP モード	15-3
VTP アドバタイズ	15-4
VTP バージョン 2	15-5
VTP バージョン 3	15-5
VTP プルーニング	15-6
VTP とスイッチ スタック	15-8
VTP の設定	15-8
VTP のデフォルト設定	15-9
VTP 設定時の注意事項	15-9
ドメイン名	15-10
パスワード	15-10
VTP バージョン	15-10
設定要件	15-11
VTP モードの設定	15-12
VTP バージョン 3 パスワードの設定	15-14
VTP バージョン 3 プライマリ サーバの設定	15-15
VTP バージョンのイネーブル化	15-15
VTP プルーニングのイネーブル化	15-16
ポート単位での VTP の設定	15-17
VTP ドメインへの VTP クライアント スwitch の追加	15-17
VTP のモニタ	15-19

CHAPTER 16
音声 VLAN の設定 16-1

音声 VLAN の概要	16-1
Cisco IP Phone の音声トラフィック	16-2
Cisco IP Phone のデータトラフィック	16-2
音声 VLAN の設定	16-3
音声 VLAN のデフォルト設定	16-3
音声 VLAN 設定時の注意事項	16-3
Cisco7960 IP Phone に接続するポートの設定	16-5
Cisco IP Phone の音声トラフィックの設定	16-5
着信データ フレームのプライオリティ設定	16-7
音声 VLAN の表示	16-8

CHAPTER 17

プライベート VLAN の設定	17-1
プライベート VLAN の概要	17-1
プライベート VLAN での IP アドレッシング方式	17-3
複数のスイッチにまたがるプライベート VLAN	17-4
プライベート VLAN の他機能との相互作用	17-5
プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャストトラフィック	17-5
プライベート VLAN と SVI	17-5
プライベート VLAN およびスイッチ スタック	17-6
プライベート VLAN の設定	17-6
プライベート VLAN の設定手順	17-6
デフォルトのプライベート VLAN 設定	17-7
プライベート VLAN 設定時の注意事項	17-7
セカンダリおよびプライマリ VLAN の設定	17-7
プライベート VLAN ポート設定	17-9
他の機能との間の制限	17-9
プライベート VLAN 内の VLAN の設定および対応付け	17-10
プライベート VLAN ホストポートとしてのレイヤ 2 インターフェイスの設定	17-12
プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定	17-13
セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング	17-14
プライベート VLAN のモニタリング	17-15

CHAPTER 18

IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定	18-1
IEEE 802.1Q トンネリングの概要	18-1
IEEE 802.1Q トンネリングの設定	18-4
IEEE 802.1Q トンネリングのデフォルト設定	18-4
IEEE 802.1Q トンネリング設定時の注意事項	18-4
ネイティブ VLAN	18-4
システム MTU	18-6
IEEE 802.1Q トンネリングおよびその他の機能	18-6
IEEE 802.1Q トンネリング ポートの設定	18-7
レイヤ 2 プロトコル トンネリングの概要	18-8
レイヤ 2 プロトコル トンネリングの設定	18-10
レイヤ 2 プロトコル トンネリングのデフォルト設定	18-11
レイヤ 2 プロトコル トンネリング設定時の注意事項	18-12
レイヤ 2 プロトコル トンネリングの設定	18-13
EtherChannel のレイヤ 2 トンネリングの設定	18-15
サービス プロバイダー エッジ スイッチの設定	18-15

カスタマー スイッチの設定	18-16
トンネリング ステータスのモニタリングおよびメンテナンス	18-18

CHAPTER 19

STP の設定 19-1

スパニング ツリー機能の概要	19-1
STP の概要	19-2
スパニング ツリー トポロジと BPDU	19-3
ブリッジ ID、スイッチ プライオリティ、および拡張システム ID	19-5
スパニング ツリー インターフェイス ステート	19-5
ブロッキング ステート	19-7
リスニング ステート	19-7
ラーニング ステート	19-7
フォワーディング ステート	19-8
ディセーブル ステート	19-8
スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み	19-8
スパニング ツリーおよび冗長接続	19-9
スパニング ツリー アドレスの管理	19-9
接続を維持するためのエージング タイムの短縮	19-10
スパニング ツリー モードおよびプロトコル	19-10
サポートされるスパニング ツリー インスタンス	19-11
スパニング ツリーの相互運用性と下位互換性	19-11
STP および IEEE 802.1Q トランク	19-12
VLAN ブリッジ スパニング ツリー	19-12
スパニング ツリーとスイッチ スタック	19-12
スパニング ツリー機能の設定	19-13
スパニング ツリー機能のデフォルト設定	19-13
スパニング ツリー設定時の注意事項	19-14
スパニング ツリー モードの変更	19-15
スパニング ツリーのディセーブル化	19-16
ルート スイッチの設定	19-17
セカンダリ ルート スイッチの設定	19-18
ポート プライオリティの設定	19-19
パス コストの設定	19-21
VLAN のスイッチ プライオリティの設定	19-22
スパニング ツリー タイマーの設定	19-23
Hello タイムの設定	19-23
VLAN の転送遅延時間の設定	19-24
VLAN の最大エージング タイムの設定	19-24
転送保留カウンタの設定	19-25

スパンニング ツリー ステータスの表示 19-25

CHAPTER 20

MSTP の設定 20-1

MSTP の概要 20-2

MST リージョン 20-2

IST、CIST、および CST 20-3

MST リージョン内の動作 20-3

MST リージョン間の動作 20-4

IEEE 802.1s の用語 20-5

ホップ カウント 20-6

境界ポート 20-6

IEEE 802.1s の実装 20-7

ポートの役割名の変更 20-7

レガシー スイッチと標準スイッチの相互運用 20-7

単一方向リンクの失敗の検出 20-8

MSTP とスイッチ スタック 20-9

IEEE 802.1D STP との相互運用性 20-9

RSTP の概要 20-10

ポートの役割およびアクティブ トポロジ 20-10

高速コンバージェンス 20-11

ポートの役割の同期化 20-12

BPDU のフォーマットおよびプロセス 20-13

優位 BPDU 情報の処理 20-14

下位 BPDU 情報の処理 20-14

トポロジの変更 20-14

MSTP 機能の設定 20-15

MSTP のデフォルト設定 20-16

MSTP 設定時の注意事項 20-16

MST リージョンの設定および MSTP のイネーブル化 20-17

ルート スイッチの設定 20-19

セカンダリ ルート スイッチの設定 20-20

ポート プライオリティの設定 20-21

パス コストの設定 20-22

スイッチ プライオリティの設定 20-23

Hello タイムの設定 20-24

転送遅延時間の設定 20-25

最大エージング タイムの設定 20-25

最大ホップ カウントの設定 20-26

リンク タイプの指定による高速移行の保証 20-26

ネイバー タイプの指定	20-27
プロトコル移行プロセスの再起動	20-27
MST コンフィギュレーションおよびステータスの表示	20-28

CHAPTER 21

オプションのスパニング ツリー機能の設定	21-1
オプションのスパニング ツリー機能の概要	21-1
PortFast の概要	21-2
BPDU ガードの概要	21-2
BPDU フィルタリングの概要	21-3
UplinkFast の概要	21-3
CSUF の概要	21-5
CSUF の機能	21-6
高速コンバージェンスを実行させるイベント	21-7
BackboneFast の概要	21-7
EtherChannel ガードの概要	21-10
ルート ガードの概要	21-10
ループ ガードの概要	21-11
オプションのスパニング ツリー機能の設定	21-11
オプションのスパニング ツリー機能のデフォルト設定	21-12
オプションのスパニング ツリー設定時の注意事項	21-12
PortFast のイネーブル化	21-12
BPDU ガードのイネーブル化	21-13
BPDU フィルタリングのイネーブル化	21-15
冗長リンク用 UplinkFast のイネーブル化	21-16
CSUF のイネーブル化	21-17
BackboneFast のイネーブル化	21-17
EtherChannel ガードのイネーブル化	21-17
ルート ガードのイネーブル化	21-18
ループ ガードのイネーブル化	21-19
スパニング ツリー ステータスの表示	21-20

CHAPTER 22

Flex Link および MAC アドレス テーブル移動更新機能の設定	22-1
Flex Link および MAC アドレス テーブル移動更新機能の概要	22-1
Flex Link	22-2
VLAN Flex Link ロード バランシングおよびサポート	22-3
Flex Link マルチキャスト高速コンバージェンス	22-3
他の Flex Link ポートのマルチキャスト ルータ ポートとしての学習	22-3
IGMP レポートの生成	22-4
IGMP レポートの送信	22-4

設定例	22-4
MAC アドレス テーブル移動更新	22-6
Flex Link および MAC アドレス テーブル移動更新機能の設定	22-8
デフォルト設定	22-8
設定時の注意事項	22-8
Flex Link の設定	22-9
Flex Link の VLAN ロード バランシングの設定	22-11
MAC アドレス テーブル移動更新機能の設定	22-12
Flex Link および MAC アドレス テーブル移動更新機能のモニタ	22-14

CHAPTER 23

Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定 23-1

DHCP スヌーピングの概要	23-1
DHCP サーバ	23-2
DHCP リレー エージェント	23-2
DHCP スヌーピング	23-2
Option 82 データ挿入	23-4
Cisco IOS DHCP サーバ データベース	23-7
DHCP スヌーピング バインディング データベース	23-7
DHCP スヌーピングおよびスイッチ スタック	23-9
DHCP スヌーピングの設定	23-9
DHCP スヌーピングのデフォルト設定	23-9
DHCP スヌーピング設定時の注意事項	23-10
DHCP リレー エージェントの設定	23-12
パケット転送アドレスの指定	23-12
DHCP スヌーピングおよび Option 82 のイネーブル化	23-13
プライベート VLAN での DHCP スヌーピングのイネーブル化	23-15
Cisco IOS DHCP サーバ データベースのイネーブル化	23-15
DHCP スヌーピング バインディング データベース エージェントのイネーブル化	23-16
DHCP スヌーピング情報の表示	23-17
IP ソース ガードの概要	23-17
送信元 IP アドレス フィルタリング	23-18
送信元 IP および MAC アドレス フィルタリング	23-18
スタティック ホストの IP ソース ガード	23-18
IP ソース ガードの設定	23-19
デフォルトの IP ソース ガードの設定	23-20
IP ソース ガード設定時の注意事項	23-20
IP ソース ガードのイネーブル化	23-21
スタティック ホストの IP ソース ガードの設定	23-22

	レイヤ2アクセスポートでのスタティックホストのIPソースガードの設定	23-22
	プライベートVLANホストポートでのスタティックホストのIPソースガードの設定	23-25
	IPソースガード情報の表示	23-27
	DHCPサーバのポートベースのアドレス割り当ての概要	23-28
	DHCPサーバのポートベースのアドレス割り当ての設定	23-28
	ポートベースのアドレス割り当てのデフォルト設定	23-28
	ポートベースのアドレス割り当ての設定時の注意事項	23-28
	DHCPサーバのポートベースのアドレス割り当てのイネーブル化	23-29
	DHCPサーバのポートベースのアドレス割り当ての表示	23-31
CHAPTER 24	ダイナミックARPインスペクションの設定	24-1
	ダイナミックARPインスペクションの概要	24-1
	インターフェイス信頼状態およびネットワークセキュリティ	24-3
	ARPパケットのレート制限	24-4
	ARP ACLとDHCPスヌーピングエントリの相対的なプライオリティ	24-5
	廃棄されたパケットのロギング	24-5
	ダイナミックARPインスペクションの設定	24-5
	デフォルトのダイナミックARPインスペクションの設定	24-6
	ダイナミックARPインスペクションの設定時の注意事項	24-6
	DHCP環境でのダイナミックARPインスペクションの設定	24-7
	非DHCP環境のARP ACLの設定	24-9
	着信ARPパケットのレート制限	24-11
	妥当性チェックの実行	24-12
	ログバッファの設定	24-13
	ダイナミックARPインスペクション情報の表示	24-15
CHAPTER 25	IGMPスヌーピングおよびMVRの設定	25-1
	IGMPスヌーピングの概要	25-2
	IGMPバージョン	25-3
	マルチキャストグループへの加入	25-3
	マルチキャストグループからの脱退	25-5
	即時脱退	25-6
	IGMP脱退タイマーの設定	25-6
	IGMPレポート抑制	25-6
	IGMPスヌーピングおよびスイッチスタック	25-7
	IGMPスヌーピングの設定	25-7
	IGMPスヌーピングのデフォルト設定	25-7
	IGMPスヌーピングのイネーブル化およびディセーブル化	25-8

スヌーピング方法の設定	25-9
マルチキャスト ルータ ポートの設定	25-10
グループに加入するホストの静的な設定	25-10
IGMP 即時脱退のイネーブル化	25-11
IGMP 脱退タイマーの設定	25-12
TCN 関連のコマンドの設定	25-12
TCN イベント後のマルチキャスト フラッディング時間の制御	25-13
フラッディング モードからの回復	25-13
TCN イベント中のマルチキャスト フラッディングのディセーブル化	25-14
IGMP スヌーピング クエリアの設定	25-14
IGMP レポート抑制のディセーブル化	25-16
IGMP スヌーピング情報の表示	25-16
MVR の概要	25-18
マルチキャスト TV アプリケーションで MVR を使用する場合	25-19
MVR の設定	25-20
MVR のデフォルト設定	25-20
MVR 設定時の注意事項および制限事項	25-21
MVR グローバル パラメータの設定	25-21
MVR インターフェイスの設定	25-23
MVR 情報の表示	25-24
IGMP フィルタリングおよびスロットリングの設定	25-25
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定	25-26
IGMP プロファイルの設定	25-26
IGMP プロファイルの適用	25-27
IGMP グループの最大数の設定	25-28
IGMP スロットリング アクションの設定	25-29
IGMP フィルタリングおよび IGMP スロットリング設定の表示	25-30

CHAPTER 26

ポート単位のトラフィック制御の設定	26-1
ストーム制御の設定	26-1
ストーム制御の概要	26-1
ストーム制御のデフォルト設定	26-3
ストーム制御およびしきい値レベルの設定	26-3
小さいフレームの着信レートの設定	26-5
保護ポートの設定	26-6
保護ポートのデフォルト設定	26-6
保護ポート設定時の注意事項	26-7
保護ポートの設定	26-7
ポート ブロックिंगの設定	26-7

ポート ブロッキングのデフォルト設定	26-8	
インターフェイスでのフラッディング トラフィックのブロッキング		26-8
ポート セキュリティの設定	26-9	
ポート セキュリティの概要	26-9	
セキュア MAC アドレス	26-9	
セキュリティ違反	26-10	
ポート セキュリティのデフォルト設定	26-11	
ポート セキュリティの設定時の注意事項	26-12	
ポート セキュリティのイネーブル化および設定	26-13	
ポート セキュリティ エージングのイネーブル化および設定		26-18
ポート セキュリティおよびスイッチ スタック	26-20	
ポート セキュリティおよびプライベート VLAN	26-20	
ポート単位のトラフィック制御設定の表示	26-21	

CHAPTER 27

CDP の設定	27-1	
CDP の概要	27-1	
CDP およびスイッチ スタック	27-2	
CDP の設定	27-2	
CDP のデフォルト設定	27-2	
CDP の特性の設定	27-2	
CDP のディセーブル化およびイネーブル化	27-3	
インターフェイス上での CDP のディセーブル化およびイネーブル化		27-4
CDP のモニタおよびメンテナンス	27-5	

CHAPTER 28

LLDP、LLDP-MED、および接続された場所のサービスの設定	28-1	
LLDP、LLDP-MED、および接続された場所のサービスの概要	28-1	
LLDP	28-1	
LLDP-MED	28-2	
接続された場所のサービス	28-3	
LLDP、LLDP-MED、および接続された場所のサービスの設定	28-5	
デフォルト LLDP 設定	28-5	
設定時の注意事項	28-5	
LLDP のイネーブル化	28-6	
LLDP 特性の設定	28-6	
LLDP-MED TLV の設定	28-7	
ネットワーク ポリシー TLV の設定	28-8	
ロケーション TLV と接続された場所の サービスの設定	28-9	
LLDP、LLDP-MED、および接続された場所のサービスのモニタリングおよびメンテナンス	28-11	

CHAPTER 29

UDLD の設定	29-1
UDLD の概要	29-1
動作モード	29-1
単一方向の検出方法	29-2
UDLD の設定	29-3
UDLD のデフォルト設定	29-4
設定時の注意事項	29-4
UDLD のグローバルなイネーブル化	29-5
インターフェイス上での UDLD のイネーブル化	29-6
UDLD によってディセーブル化されたインターフェイスのリセット	29-6
UDLD ステータスの表示	29-7

CHAPTER 30

SPAN および RSPAN の設定	30-1
SPAN および RSPAN の概要	30-1
ローカル SPAN	30-2
リモート SPAN	30-3
SPAN と RSPAN の概念および用語	30-4
SPAN セッション	30-4
モニタ対象トラフィック	30-5
送信元ポート	30-6
送信元 VLAN	30-7
VLAN フィルタリング	30-7
宛先ポート	30-8
RSPAN VLAN	30-9
SPAN および RSPAN と他の機能の相互作用	30-9
SPAN/RSPAN およびスイッチ スタック	30-10
SPAN および RSPAN の設定	30-10
SPAN および RSPAN のデフォルト設定	30-11
ローカル SPAN の設定	30-11
SPAN 設定時の注意事項	30-11
ローカル SPAN セッションの作成	30-12
ローカル SPAN セッションの作成および着信トラフィックの設定	30-15
フィルタリングする VLAN の指定	30-17
RSPAN の設定	30-18
RSPAN 設定時の注意事項	30-18
RSPAN VLAN としての VLAN の設定	30-19
RSPAN 送信元セッションの作成	30-20
RSPAN 宛先セッションの作成	30-22
RSPAN 宛先セッションの作成および着信トラフィックの設定	30-23

フィルタリングする VLAN の指定	30-25
SPAN および RSPAN のステータス表示	30-26

CHAPTER 31

RMON の設定	31-1
RMON の概要	31-1
RMON の設定	31-3
RMON のデフォルト設定	31-3
RMON アラームおよびイベントの設定	31-3
インターフェイス上でのグループ履歴統計情報の収集	31-5
インターフェイス上でのイーサネット グループ統計情報の収集	31-6
RMON ステータスの表示	31-6

CHAPTER 32

システム メッセージ ログिंगの設定	32-1
システム メッセージ ログिंगの概要	32-1
システム メッセージ ログिंगの設定	32-2
システム ログ メッセージのフォーマット	32-2
システム メッセージ ログिंगのデフォルト設定	32-4
メッセージ ログिंगのディセーブル化	32-4
メッセージ表示宛先デバイスの設定	32-5
ログ メッセージの同期化	32-6
ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化	32-8
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化	32-8
メッセージ重大度の定義	32-9
履歴テーブルおよび SNMP に送信される Syslog メッセージの制限	32-10
設定変更ロガーのイネーブル化	32-11
UNIX Syslog サーバの設定	32-12
UNIX Syslog デーモンへのログ メッセージ	32-13
UNIX システム ログング ファシリティの設定	32-13
ログング設定の表示	32-14

CHAPTER 33

SNMP の設定	33-1
SNMP の概要	33-1
SNMP バージョン	33-2
SNMP マネージャ機能	33-3
SNMP エージェント機能	33-4
SNMP コミュニティ スtring	33-4
SNMP を使用して MIB 変数にアクセスする方法	33-4
SNMP 通知	33-5
SNMP ifIndex MIB オブジェクト値	33-6

SNMP の設定	33-6
SNMP のデフォルト設定	33-7
SNMP 設定時の注意事項	33-7
SNMP エージェントのディセーブル化	33-8
コミュニティ スtring の設定	33-8
SNMP グループおよびユーザの設定	33-10
SNMP 通知の設定	33-13
CPU しきい値通知のタイプと値の設定	33-17
エージェント コンタクトおよびロケーションの設定	33-17
SNMP を通して使用する TFTP サーバの制限	33-18
SNMP の例	33-19
SNMP ステータスの表示	33-20

CHAPTER 34

組み込みイベント マネージャの設定	34-1
組み込みイベント マネージャの概要	34-2
イベント ディテクタ	34-3
組み込みイベント マネージャの操作	34-4
組み込みイベント マネージャ ポリシー	34-5
組み込みイベント マネージャの環境変数	34-5
EEM 3.2	34-6
組み込みイベント マネージャの設定	34-6
組み込みイベント マネージャのアプレットの登録および定義	34-6
組み込みイベント マネージャの TCL スクリプトの登録および定義	34-7
組み込みイベント マネージャ情報の表示	34-8

CHAPTER 35

ACL によるネットワーク セキュリティの設定	35-1
ACL の概要	35-1
サポートされる ACL	35-2
ポート ACL	35-3
ルータ ACL	35-4
VLAN マップ	35-5
分割トラフィックおよび非分割トラフィックの処理	35-6
ACL およびスイッチ スタック	35-7
IPv4 ACL の設定	35-7
標準および拡張 IPv4 ACL の作成	35-8
アクセス リスト番号	35-9
ACL のロギング	35-9
番号制標準 ACL の作成	35-10
番号制拡張 ACL の作成	35-11

ACL 内の ACE シーケンスの再編集	35-15	
名前付き標準および拡張 ACL の作成	35-15	
ACL での時間範囲の使用法	35-17	
ACL へのコメントの挿入	35-19	
端末回線への IPv4 ACL の適用	35-19	
インターフェイスへの IPv4 ACL の適用	35-20	
IP ACL のハードウェアおよびソフトウェアの処理	35-22	
ACL のトラブルシューティング	35-22	
IPv4 ACL の設定例	35-23	
番号制 ACL	35-25	
拡張 ACL	35-25	
名前付き ACL	35-26	
IP ACL に適用される時間範囲	35-26	
コメント付き IP ACL エントリ	35-27	
ACL のロギング	35-27	
名前付き MAC 拡張 ACL の作成	35-28	
レイヤ 2 インターフェイスへの MAC ACL の適用	35-30	
VLAN マップの設定	35-31	
VLAN マップの設定時の注意事項	35-32	
VLAN マップの作成	35-33	
ACL および VLAN マップの例	35-33	
VLAN への VLAN マップの適用	35-35	
ネットワークでの VLAN マップの使用法	35-36	
ワイヤリング クローゼットの設定	35-36	
別の VLAN にあるサーバへのアクセスの拒否	35-37	
ルータ ACL を VLAN マップと組み合わせて使用する方法	35-38	
VLAN マップとルータ ACL の設定時の注意事項	35-38	
VLAN に適用されるルータ ACL と VLAN マップの例	35-39	
ACL およびスイッチド パケット	35-39	
ACL およびブリッジド パケット	35-40	
ACL およびルーテッド パケット	35-41	
ACL およびマルチキャスト パケット	35-41	
IPv4 ACL の設定の表示	35-42	

CHAPTER 36

QoS の設定	36-1
QoS の概要	36-2
QoS の基本モデル	36-3
分類	36-5
QoS ACL に基づく分類	36-7

クラス マップおよびポリシー マップに基づく分類	36-7
ポリシングおよびマーキング	36-8
物理ポートのポリシング	36-9
SVI のポリシング	36-10
マッピング テーブル	36-12
キューイングおよびスケジューリングの概要	36-13
WTD	36-13
SRR のシェーピングおよび共有	36-14
入力キューでのキューイングおよびスケジューリング	36-15
出力キューでのキューイングおよびスケジューリング	36-17
パケットの変更	36-20
自動 QoS の設定	36-20
生成される自動 QoS 設定	36-21
コンフィギュレーションにおける自動 QoS の影響	36-26
自動 QoS 設定時の注意事項	36-26
Cisco IOS Release 12.2(20)SE 以前のリリースからのアップグレード	36-27
VoIP 用自動 QoS のイネーブル化	36-27
自動 QoS 設定例	36-29
自動 QoS 情報の表示	36-30
標準 QoS の設定	36-31
標準 QoS のデフォルト設定	36-31
入力キューのデフォルト設定	36-32
出力キューのデフォルト設定	36-32
マッピング テーブルのデフォルト設定	36-33
標準 QoS 設定時の注意事項	36-34
QoS ACL の注意事項	36-34
インターフェイスへの QoS の適用	36-34
ポリシングの注意事項	36-35
一般的な QoS の注意事項	36-35
QoS のグローバルなイネーブル化	36-36
物理ポートで VLAN ベースの QoS をイネーブル化	36-36
ポートの信頼状態による分類の設定	36-37
QoS ドメイン内のポートの信頼状態の設定	36-37
インターフェイスの CoS 値の設定	36-39
ポート セキュリティを確保するための信頼境界機能の設定	36-39
DSCP 透過モードのイネーブル化	36-41
別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定	36-41
QoS ポリシーの設定	36-43
ACL によるトラフィックの分類	36-44

クラス マップによるトラフィックの分類	36-47
ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング	36-49
階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング	36-53
集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング	36-60
DSCP マップの設定	36-62
CoS/DSCP マップの設定	36-62
IP precedence/DSCP マップの設定	36-63
ポリシング済み DSCP マップの設定	36-64
DSCP/CoS マップの設定	36-65
DSCP/DSCP 変換マップの設定	36-66
入力キューの特性の設定	36-68
入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定	36-68
入力キュー間のバッファ スペースの割り当て	36-70
入力キュー間の帯域幅の割り当て	36-70
入力プライオリティ キューの設定	36-71
出力キューの特性の設定	36-72
設定時の注意事項	36-73
出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定	36-73
出力キューおよび ID への DSCP または CoS 値のマッピング	36-75
出力キューでの SRR シェーピング重みの設定	36-76
出力キューでの SRR 共有重みの設定	36-78
出力緊急キューの設定	36-79
出力インターフェイスの帯域幅の制限	36-79
標準 QoS 情報の表示	36-80

CHAPTER 37

EtherChannel およびリンクステート トラッキングの設定 37-1

EtherChannel の概要	37-1
EtherChannel の概要	37-2
ポートチャンネル インターフェイス	37-4
PAgP	37-5
PAgP モード	37-6
仮想スイッチおよびデュアル アクティブ検出との PAgP 相互作用	37-6
PAgP と他の機能との相互作用	37-7
LACP	37-7
LACP モード	37-8
LACP と他の機能との相互作用	37-8

EtherChannel の On モード	37-8
ロード バランシングおよび転送方式	37-9
EtherChannel およびスイッチ スタック	37-10
EtherChannel の設定	37-11
EtherChannel のデフォルト設定	37-12
EtherChannel 設定時の注意事項	37-12
レイヤ 2 EtherChannel の設定	37-14
レイヤ 3 EtherChannel の設定	37-16
ポートチャネル論理インターフェイスの作成	37-16
物理インターフェイスの設定	37-17
EtherChannel ロード バランシングの設定	37-20
PAgP 学習方式およびプライオリティの設定	37-21
LACP ホットスタンバイ ポートの設定	37-23
LACP システム プライオリティの設定	37-23
LACP ポート プライオリティの設定	37-24
EtherChannel、PAgP、および LACP ステータスの表示	37-25
リンクステート トラッキングの概要	37-25
リンクステート トラッキングの設定	37-28
デフォルトのリンクステート トラッキングの設定	37-28
リンクステート トラッキングの設定時の注意事項	37-29
リンクステート トラッキングの設定	37-29
リンクステート トラッキング ステータスの表示	37-30

CHAPTER 38

IP ユニキャスト ルーティングの設定	38-1
IP ルーティングの概要	38-2
ルーティング タイプ	38-3
IP ルーティングおよびスイッチ スタック	38-3
ルーティングを設定する手順	38-5
IP アドレス指定の設定	38-6
アドレス指定のデフォルト設定	38-6
ネットワーク インターフェイスへの IP アドレスの割り当て	38-7
サブネット ゼロの使用	38-8
クラスレス ルーティング	38-8
アドレス解決方法の設定	38-10
スタティック ARP キャッシュの定義	38-11
ARP カプセル化の設定	38-12
プロキシ ARP のイネーブル化	38-12
IP ルーティングがディセーブルの場合のルーティング支援機能	38-13
プロキシ ARP	38-13

デフォルト ゲートウェイ	38-13	
ICMP Router Discovery Protocol (IRDP)	38-14	
ブロードキャスト パケットの処理方法の設定	38-15	
指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化		38-16
UDP ブロードキャスト パケットおよびプロトコルの転送	38-17	
IP ブロードキャスト アドレスの確立	38-18	
IP ブロードキャストのフラッディング	38-18	
IP アドレスのモニタおよびメンテナンス	38-20	
IP ユニキャスト ルーティングのイネーブル化	38-20	
RIP の設定	38-21	
RIP のデフォルト設定	38-22	
基本的な RIP パラメータの設定	38-23	
RIP 認証の設定	38-25	
サマリー アドレスおよびスプリット ホライズンの設定		38-25
スプリット ホライズンの設定	38-27	
OSPF の設定	38-27	
OSPF のデフォルト設定	38-28	
OSPF Nonstop Forwarding	38-30	
基本的な OSPF パラメータの設定	38-31	
OSPF インターフェイスの設定	38-32	
OSPF エリア パラメータの設定	38-33	
その他の OSPF パラメータの設定	38-34	
LSA グループ同期設定の変更	38-36	
ループバック インターフェイスの設定	38-37	
OSPF のモニタ	38-37	
EIGRP の設定	38-38	
EIGRP のデフォルト設定	38-40	
EIGRP Nonstop Forwarding	38-41	
基本的な EIGRP パラメータの設定	38-42	
EIGRP インターフェイスの設定	38-43	
EIGRP ルート認証の設定	38-44	
EIGRP スタブ ルーティングの設定	38-45	
EIGRP のモニタおよびメンテナンス	38-46	
BGP の設定	38-47	
BGP のデフォルト設定	38-49	
NSF 認識	38-52	
BGP ルーティングのイネーブル化	38-52	
ルーティング ポリシー変更の管理	38-55	
BGP 判断アトリビュートの設定	38-56	

ルート マップによる BGP フィルタリングの設定	38-58
ネイバーによる BGP フィルタリングの設定	38-59
BGP フィルタリング用のプレフィクス リストの設定	38-60
BGP コミュニティ フィルタリングの設定	38-61
BGP ネイバーおよびピア グループの設定	38-63
集約アドレスの設定	38-65
ルーティング ドメイン連合の設定	38-66
BGP ルート リフレクタの設定	38-66
ルート ダンプ化の設定	38-67
BGP のモニタおよびメンテナンス	38-68
ISO CLNS ルーティングの設定	38-69
IS-IS ダイナミック ルーティングの設定	38-70
IS-IS のデフォルト設定	38-71
NSF 認識	38-72
IS-IS ルーティングのイネーブル化	38-72
IS-IS グローバル パラメータの設定	38-74
IS-IS インターフェイス パラメータの設定	38-77
ISO IGRP と IS-IS のモニタおよびメンテナンス	38-79
マルチ VRF CE の設定	38-80
マルチ VRF CE の概要	38-80
マルチ VRF CE のデフォルト設定	38-82
マルチ VRF CE の設定時の注意事項	38-83
VRF の設定	38-84
マルチキャスト VRF の設定	38-85
VRF 認識サービスの設定	38-85
ARP のユーザ インターフェイス	38-86
ping のユーザ インターフェイス	38-86
SNMP のユーザ インターフェイス	38-86
HSRP のユーザ インターフェイス	38-87
Syslog のユーザ インターフェイス	38-87
traceroute のユーザ インターフェイス	38-88
FTP および TFTP のユーザ インターフェイス	38-88
VPN ルーティング セッションの設定	38-89
BGP PE/CE ルーティング セッションの設定	38-89
マルチ VRF CE の設定例	38-90
マルチ VRF CE ステータスの表示	38-94
プロトコル独立機能の設定	38-95
dCEF の設定	38-95
等価コスト ルーティング パスの個数の設定	38-97

スタティックユニキャストルートの設定	38-97	
デフォルトのルートおよびネットワークの指定	38-98	
ルートマップによるルーティング情報の再配信	38-99	
PBRの設定	38-103	
PBR設定時の注意事項	38-104	
PBRのイネーブル化	38-105	
ルーティング情報のフィルタリング	38-107	
パッシブインターフェイスの設定	38-107	
ルーティングアップデートのアドバタイズメントおよび処理の制御	38-108	
ルーティング情報の送信元のフィルタリング	38-109	
認証鍵の管理	38-110	
IPネットワークのモニタおよびメンテナンス	38-111	

CHAPTER 39

IPv6ユニキャストルーティングの設定	39-1	
IPv6の概要	39-1	
IPv6アドレス	39-2	
サポート対象のIPv6ユニキャストルーティング機能	39-3	
128ビット幅のユニキャストアドレス	39-3	
IPv6DNS	39-4	
IPv6ユニキャストのパスMTUディスカバリ	39-4	
ICMPv6	39-4	
近接ディスカバリ	39-4	
デフォルトルータプリファレンス	39-5	
IPv6のステートレス自動設定および重複アドレス検出	39-5	
IPv6アプリケーション	39-5	
デュアルIPv4/IPv6プロトコルスタック	39-6	
IPv6DHCPアドレス割り当て	39-6	
IPv6のスタティックルート	39-7	
IPv6RIP	39-7	
IPv6OSPF	39-7	
EIGRPIPv6	39-7	
HSRPIPv6	39-7	
IPv6によるSNMPおよびSyslog	39-8	
IPv6によるHTTP(S)	39-8	
サポートされていないIPv6ユニキャストルーティング機能	39-9	
制限事項	39-9	
IPv6とスイッチスタック	39-10	
IPv6の設定	39-11	
IPv6のデフォルト設定	39-11	

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化	39-12
デフォルト ルータ プリファレンスの設定	39-14
IPv4 および IPv6 プロトコル スタックの設定	39-15
DHCP 設定による IPv6 アドレス割り当て	39-16
DHCPv6 アドレス割り当てのデフォルト設定	39-16
DHCPv6 アドレス割り当て設定の注意事項	39-16
DHCPv6 サーバ機能のイネーブル化	39-17
DHCPv6 クライアント機能のイネーブル化	39-19
IPv6 ICMP レート制限の設定	39-20
IPv6 の CEF および dCEF の設定	39-20
IPv6 のスタティック ルートの設定	39-21
IPv6 RIP の設定	39-22
IPv6 OSPF の設定	39-23
EIGRP IPv6 の設定	39-25
IPv6 HSRP の設定	39-25
HSRP バージョン 2 のイネーブル化	39-26
HSRP IPv6 グループのイネーブル化	39-26
IPv6 の表示	39-28

CHAPTER 40

IPv6 MLD スヌーピングの設定	40-1
MLD スヌーピングの概要	40-1
MLD メッセージ	40-2
MLD クエリー	40-3
マルチキャスト クライアント エージングの堅牢性	40-3
マルチキャスト ルータ 検出	40-3
MLD レポート	40-4
MLD Done メッセージおよび即時脱退	40-4
TCN 処理	40-5
スイッチ スタック内の MLD スヌーピング	40-5
IPv6 MLD スヌーピングの設定	40-5
MLD スヌーピングのデフォルト設定	40-6
MLD スヌーピング設定時の注意事項	40-6
MLD スヌーピングのイネーブル化またはディセーブル化	40-7
スタティックなマルチキャスト グループの設定	40-8
マルチキャスト ルータ ポートの設定	40-8
MLD 即時脱退のイネーブル化	40-9
MLD スヌーピング クエリーの設定	40-10
MLD リスナー メッセージ抑制のディセーブル化	40-11
MLD スヌーピング情報の表示	40-12

CHAPTER 41

IPv6 ACL の設定	41-1
IPv6 ACL の概要	41-2
サポートされる ACL 機能	41-3
IPv6 ACL の制限事項	41-3
IPv6 ACL とスイッチ スタック	41-4
IPv6 ACL の設定	41-4
IPv6 ACL のデフォルト設定	41-4
他の機能との相互作用	41-5
IPv6 ACL の作成	41-5
インターフェイスへの IPv6 ACL の適用	41-8
IPv6 ACL の表示	41-9

CHAPTER 42

HSRP の設定	42-1
HSRP の概要	42-2
HSRP バージョン	42-4
Multiple HSRP	42-4
HSRP およびスイッチ スタック	42-5
HSRP の設定	42-5
HSRP のデフォルト設定	42-6
HSRP 設定時の注意事項	42-6
HSRP のイネーブル化	42-7
HSRP のプライオリティの設定	42-8
MHSRP の設定	42-11
HSRP 認証およびタイマーの設定	42-11
ICMP リダイレクトメッセージの HSRP サポートのイネーブル化	42-13
HSRP グループおよびクラスタリングの設定	42-13
HSRP のトラブルシューティング	42-13
HSRP 設定の表示	42-14

CHAPTER 43

Cisco IOS IP SLA 動作の設定	43-1
Cisco IOS IP SLA の概要	43-1
Cisco IOS IP SLA によるネットワーク パフォーマンスの測定	43-3
IP SLA 応答側と IP SLA コントロール プロトコル	43-4
IP SLA の応答時間の計算	43-4
IP SLA 動作のスケジューリング	43-5
IP SLA 動作しきい値モニタリング	43-5
IP SLA 動作の設定	43-6
デフォルト設定	43-6
設定時の注意事項	43-6

IP SLA 応答側の設定	43-8
UDP ジッタ動作を使用した IP サービス レベルの分析	43-8
ICMP エコー動作を使用した IP サービス レベルの分析	43-11
IP SLA 動作のモニタリング	43-13

CHAPTER 44

拡張オブジェクト トラッキングの設定	44-1
拡張オブジェクト トラッキングの概要	44-1
拡張オブジェクト トラッキング機能の設定	44-2
デフォルト設定	44-2
インターフェイスのラインプロトコルまたは IP ルーティング ステートのトラッキング	44-2
トラッキング リストの設定	44-4
ブール論理式を使用したトラッキング リストの設定	44-4
ウェイトしきい値を使用したトラッキング リストの設定	44-5
パーセンテージしきい値を使用したトラッキング リストの設定	44-6
HSRP オブジェクト トラッキングの設定	44-7
他のトラッキング特性の設定	44-8
IP SLA オブジェクト トラッキングの設定	44-9
スタティック ルーティング サポートの設定	44-10
プライマリ インターフェイスの設定	44-11
Cisco IP SLA のモニタリング エージェントおよびトラッキング オブジェクトの設定	44-11
ルーティング ポリシーおよびデフォルト ルートの設定	44-12
拡張オブジェクト トラッキングのモニタリング	44-13

CHAPTER 45

WCCP による Web キャッシュ サービスの設定	45-1
WCCP の概要	45-1
WCCP メッセージ交換	45-2
WCCP ネゴシエーション	45-3
MD5 セキュリティ	45-3
パケット リダイレクションおよびサービス グループ	45-4
WCCP とスイッチ スタック	45-5
サポートされない WCCP 機能	45-5
WCCP の設定	45-5
WCCP のデフォルト設定	45-6
WCCP 設定時の注意事項	45-6
Web キャッシュ サービスのイネーブル化	45-7
WCCP のモニタおよびメンテナンス	45-10

CHAPTER 46

IP マルチキャスト ルーティングの設定	46-1
IP マルチキャスト ルーティングの実装の概要	46-2
IGMP の概要	46-3
IGMP バージョン 1	46-3
IGMPv2	46-4
PIM の概要	46-4
PIM のバージョン	46-4
PIM のモード	46-5
PIM スタブルーティング	46-5
IGMP ヘルパー	46-7
自動 RP	46-7
BSR	46-7
マルチキャスト転送およびリバースパスチェック	46-8
DVMRP の概要	46-10
CGMP の概要	46-10
マルチキャスト ルーティングおよびスイッチ スタック	46-11
IP マルチキャスト ルーティングの設定	46-11
マルチキャスト ルーティングのデフォルト設定	46-12
マルチキャスト ルーティング設定時の注意事項	46-12
PIMv1 および PIMv2 の相互運用性	46-12
自動 RP および BSR 設定時の注意事項	46-13
基本的なマルチキャスト ルーティングの設定	46-14
SSM の設定	46-15
SSM コンポーネントの概要	46-16
SSM とインターネット標準マルチキャストとの違い	46-16
SSM の IP アドレスの範囲	46-16
SSM の動作	46-17
IGMPv3 ホスト シグナリング	46-17
設定時の注意事項	46-17
SSM の設定	46-18
SSM のモニタリング	46-19
SSM マッピングの設定	46-19
設定時の注意事項	46-19
SSM マッピングの概要	46-20
SSM マッピングの設定	46-22
SSM マッピングのモニタリング	46-24
PIM スタブルーティングの設定	46-25
PIM スタブルーティングの設定時の注意事項	46-25
PIM スタブルーティングのイネーブル化	46-25

RP の設定	46-26	
マルチキャスト グループへの RP の手動割り当て		46-27
自動 RP の設定	46-28	
PIMv2 BSR の設定	46-33	
自動 RP および BSR の使用	46-37	
RP マッピング情報のモニタ	46-38	
PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング		46-38
高度な PIM 機能の設定	46-38	
PIM 共有ツリーおよび送信元ツリーの概要		46-38
PIM SPT 使用の延期	46-40	
PIM ルータクエリー メッセージ インターバルの変更		46-41
オプションの IGMP 機能の設定	46-41	
IGMP のデフォルト設定	46-42	
グループのメンバーとしてのスイッチの設定		46-42
IP マルチキャスト グループへのアクセスの制御		46-43
IGMP バージョンの変更	46-44	
IGMP ホストクエリー メッセージ インターバルの変更		46-45
IGMPv2 の IGMP クエリー タイムアウトの変更	46-46	
IGMPv2 の最大クエリー応答時間の変更	46-46	
スタティックに接続されたメンバーとしてのスイッチの設定		46-47
オプションのマルチキャスト ルーティング機能の設定	46-47	
CGMP サーバ サポート機能のイネーブル化	46-48	
sdr リスナー サポート機能の設定	46-49	
sdr リスナー サポート機能のイネーブル化		46-49
sdr キャッシュ エントリの存在期間の制限		46-50
IP マルチキャスト境界の設定	46-50	
基本的な DVMRP 相互運用性機能の設定	46-52	
DVMRP 相互運用性設定	46-52	
DVMRP トンネルの設定	46-54	
DVMRP ネイバーへのネットワーク 0.0.0.0 のアダバタイズ		46-56
mrinfo 要求への応答	46-57	
高度な DVMRP 相互運用性機能の設定	46-57	
DVMRP ユニキャスト ルーティングのイネーブル化		46-58
DVMRP の非プルニング ネイバーの拒否	46-59	
ルート交換の制御	46-61	
アダバタイズされる DVMRP ルート数の制限		46-61
DVMRP ルートしきい値の変更	46-61	
DVMRP サマリー アドレスの設定	46-62	
DVMRP 自動サマライズのディセーブル化	46-64	

DVMRP ルートへのメトリック オフセットの追加	46-64
IP マルチキャスト ルーティングのモニタおよびメンテナンス	46-65
キャッシュ、テーブル、およびデータベースのクリア	46-65
システムおよびネットワーク統計情報の表示	46-66
IP マルチキャスト ルーティングのモニタ	46-67

CHAPTER 47**MSDP の設定**

47-1

MSDP の概要	47-1
MSDP の動作	47-2
MSDP の利点	47-3
MSDP の設定	47-3
MSDP のデフォルト設定	47-4
デフォルトの MSDP ピアの設定	47-4
SA ステートのキャッシング	47-6
MSDP ピアからの送信元情報の要求	47-8
スイッチから発信される送信元情報の制御	47-8
送信元の再配信	47-9
SA 要求メッセージのフィルタリング	47-10
スイッチで転送される送信元情報の制御	47-11
フィルタの使用法	47-12
SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限	47-13
スイッチで受信される送信元情報の制御	47-13
MSDP メッシュ グループの設定	47-15
MSDP ピアのシャットダウン	47-16
MSDP への境界 PIM DM 領域の追加	47-16
RP アドレス以外の発信元アドレスの設定	47-17
MSDP のモニタおよびメンテナンス	47-18

CHAPTER 48**フォールバック ブリッジングの設定**

48-1

フォールバック ブリッジングの概要	48-1
フォールバック ブリッジングの概要	48-1
フォールバック ブリッジングおよびスイッチ スタック	48-3
フォールバック ブリッジングの設定	48-3
フォールバック ブリッジングのデフォルト設定	48-4
フォールバック ブリッジング設定時の注意事項	48-4
ブリッジ グループの作成	48-4
スパンニング ツリー パラメータの調整	48-6
VLAN ブリッジ スパンニング ツリー プライオリティの変更	48-6

インターフェイス プライオリティの変更	48-7
パス コストの割り当て	48-7
BPDU インターバルの調整	48-8
インターフェイスでのスパニング ツリーのディセーブル化	48-10
フォールバック ブリッジングのモニタリングおよびメンテナンス	48-11

CHAPTER 49

トラブルシューティング	49-1
ソフトウェアで障害が発生した場合の回復	49-2
パスワードを忘れた場合の回復	49-3
パスワード回復がイネーブルになっている場合の手順	49-5
パスワード回復がディセーブルになっている場合の手順	49-6
スイッチ スタック問題の回避	49-8
コマンド スイッチで障害が発生した場合の回復	49-9
故障したコマンド スイッチをクラスタ メンバーと交換する場合	49-10
故障したコマンド スイッチを他のスイッチと交換する場合	49-11
クラスタ メンバー スイッチとの接続の回復	49-13
自動ネゴシエーションの不一致の防止	49-13
PoE スイッチ ポートのトラブルシューティング	49-13
電力喪失によるポートの障害	49-14
不正リンクアップによるポート障害	49-14
SFP モジュールのセキュリティと識別	49-14
SFP モジュール ステータスのモニタリング	49-15
温度のモニタリング	49-15
ping の使用	49-15
ping の概要	49-15
ping の実行	49-16
レイヤ 2 traceroute の使用	49-17
レイヤ 2 traceroute の概要	49-17
使用時の注意事項	49-17
物理パスの表示	49-18
IP traceroute の使用	49-18
IP traceroute の概要	49-18
IP traceroute の実行	49-19
TDR の使用	49-20
TDR の概要	49-20
TDR の実行および結果の表示	49-21
debug コマンドの使用	49-21
特定機能に関するデバッグのイネーブル化	49-21

	システム全体診断のイネーブル化	49-22	
	デバッグおよびエラー メッセージ出力のリダイレクト		49-22
	show platform forward コマンドの使用	49-23	
	crashinfo ファイルの使用	49-25	
	基本 crashinfo ファイル	49-25	
	拡張 crashinfo ファイル	49-26	
	トラブルシューティングの表	49-26	
	CPU 使用率のトラブルシューティング	49-26	
	CPU 使用率が高い場合に発生する可能性のある症状		49-26
	問題と原因の確認	49-27	
	Power over Ethernet (PoE) のトラブルシューティング		49-28
	StackWise のトラブルシューティング	49-31	
CHAPTER 50	オンライン診断の設定	50-1	
	オンライン診断の概要	50-1	
	オンライン診断のスケジューリング	50-2	
	ヘルス モニタリング診断の設定	50-2	
	オンライン診断テストの実行	50-3	
	オンライン診断テストの開始	50-3	
	オンライン診断テストおよびテスト結果の表示	50-4	
APPENDIX A	Catalyst 3750G Integrated Wireless LAN Controller スイッチの設定		A-1
	ワイヤレス LAN コントローラ スイッチの概要	A-2	
	ワイヤレス LAN コントローラ スイッチおよびスイッチ スタック		A-2
	コントローラとスイッチの相互作用	A-3	
	内部ポート	A-3	
	ワイヤレス LAN コントローラ スイッチの設定	A-4	
	内部ポート設定	A-4	
	内部ポートの再設定	A-6	
	コントローラへのアクセス	A-7	
	内部ワイヤレス コントローラ情報の表示	A-7	
APPENDIX B	サポート対象 MIB	B-1	
	MIB の一覧	B-1	
	FTP による MIB ファイルへのアクセス	B-4	

APPENDIX C

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

フラッシュ ファイル システムの操作	C-1
使用可能なファイル システムの表示	C-2
デフォルト ファイル システムの設定	C-3
ファイル システムのファイルに関する情報の表示	C-3
ディレクトリの変更および作業ディレクトリの表示	C-4
ディレクトリの作成および削除	C-4
ファイルのコピー	C-5
ファイルの削除	C-6
tar ファイルの作成、表示、および抽出	C-6
tar ファイルの作成	C-6
tar ファイルの内容の表示	C-7
tar ファイルの抽出	C-8
ファイルの内容の表示	C-8
コンフィギュレーション ファイルの操作	C-9
コンフィギュレーション ファイルの作成および使用上の注意事項	C-10
コンフィギュレーション ファイルのタイプおよび場所	C-10
テキスト エディタによるコンフィギュレーション ファイルの作成	C-11
TFTP によるコンフィギュレーション ファイルのコピー	C-11
TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	C-11
TFTP によるコンフィギュレーション ファイルのダウンロード	C-12
TFTP によるコンフィギュレーション ファイルのアップロード	C-13
FTP によるコンフィギュレーション ファイルのコピー	C-13
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	C-14
FTP によるコンフィギュレーション ファイルのダウンロード	C-14
FTP によるコンフィギュレーション ファイルのアップロード	C-16
RCP によるコンフィギュレーション ファイルのコピー	C-17
RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	C-17
RCP によるコンフィギュレーション ファイルのダウンロード	C-18
RCP によるコンフィギュレーション ファイルのアップロード	C-19
設定情報の消去	C-20
スタートアップ コンフィギュレーション ファイルの消去	C-20
格納されたコンフィギュレーション ファイルの削除	C-20
コンフィギュレーションの交換またはロールバック	C-21
コンフィギュレーション交換およびロールバックの概要	C-21
設定時の注意事項	C-22

コンフィギュレーションアーカイブの設定	C-23	
コンフィギュレーション交換またはロールバック動作の実行		C-24
ソフトウェア イメージの操作	C-25	
スイッチ上のイメージの場所	C-26	
サーバまたは Cisco.com 上のイメージの tar ファイル形式		C-26
TFTP によるイメージ ファイルのコピー	C-27	
TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備		C-28
TFTP によるイメージ ファイルのダウンロード	C-28	
TFTP によるイメージ ファイルのアップロード	C-30	
FTP によるイメージ ファイルのコピー	C-31	
FTP によるイメージ ファイルのダウンロードまたはアップロードの準備		C-31
FTP によるイメージ ファイルのダウンロード	C-32	
FTP によるイメージ ファイルのアップロード	C-35	
RCP によるイメージ ファイルのコピー	C-36	
RCP によるイメージ ファイルのダウンロードまたはアップロードの準備		C-36
RCP によるイメージ ファイルのダウンロード	C-38	
RCP によるイメージ ファイルのアップロード	C-40	
スタック メンバー間のイメージ ファイルのコピー	C-41	

APPENDIX D

Cisco IOS Release 12.2(52)SE でサポートされていないコマンド	D-1
ACL	D-2
サポートされていない特権 EXEC コマンド	D-2
サポートされていないグローバル コンフィギュレーション コマンド	D-2
サポートされていないルートマップ コンフィギュレーション コマンド	D-2
アーカイブ コマンド	D-2
サポートされていない特権 EXEC コマンド	D-2
ARP コマンド	D-3
サポートされていないグローバル コンフィギュレーション コマンド	D-3
サポートされていないインターフェイス コンフィギュレーション コマンド	D-3
ブート ローダ コマンド	D-3
サポートされていないグローバル コンフィギュレーション コマンド	D-3
組み込みイベント マネージャ	D-3
サポートされていない特権 EXEC コマンド	D-3
サポートされていないグローバル コンフィギュレーション コマンド	D-3
アプレット コンフィギュレーション モードでサポートされていないコマンド	D-4
フォールバック ブリッジング	D-4
サポートされていない特権 EXEC コマンド	D-4
サポートされていないグローバル コンフィギュレーション コマンド	D-4
サポートされていないインターフェイス コンフィギュレーション コマンド	D-5

ハイ アベイラビリティ	D-5	
サポートされていない SSO 認識 HSRP コマンド	D-5	
HSRP	D-6	
サポートされていないグローバル コンフィギュレーション コマンド	D-6	
サポートされていないインターフェイス コンフィギュレーション コマンド	D-6	D-6
IGMP スヌーピング コマンド	D-6	
サポートされていないグローバル コンフィギュレーション コマンド	D-6	
インターフェイス コマンド	D-6	
サポートされていない特権 EXEC コマンド	D-6	
サポートされていないグローバル コンフィギュレーション コマンド	D-6	
サポートされていないインターフェイス コンフィギュレーション コマンド	D-7	D-7
IP マルチキャスト ルーティング	D-7	
サポートされていない特権 EXEC コマンド	D-7	
サポートされていないグローバル コンフィギュレーション コマンド	D-7	
サポートされていないインターフェイス コンフィギュレーション コマンド	D-7	D-7
IP SLA	D-8	
サポートされていない MPLS ヘルス モニタ コマンド	D-8	
サポートされていないイーサネット ゲートキーパー登録コマンド	D-8	D-8
サポートされていない VoIP コール セットアップ プロブ コマンド	D-8	D-8
IP ユニキャスト ルーティング	D-8	
サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド	D-8	D-8
サポートされていないグローバル コンフィギュレーション コマンド	D-9	
サポートされていないインターフェイス コンフィギュレーション コマンド	D-9	D-9
サポートされていない BGP ルータ コンフィギュレーション コマンド	D-10	D-10
サポートされていない VPN コンフィギュレーション コマンド	D-10	D-10
サポートされていないルート マップ コマンド	D-10	D-10
IPv6	D-10	
IPv4/v6 トンネリング コマンド	D-10	D-10
レイヤ 3	D-11	
BGP	D-11	
その他のサポートされていない BGP コマンド	D-11	D-11
OSPF	D-12	
VRF 認識 AAA	D-12	
MAC アドレス コマンド	D-13	
サポートされていない特権 EXEC コマンド	D-13	
サポートされていないグローバル コンフィギュレーション コマンド	D-13	D-13
その他	D-13	
サポートされていないユーザ EXEC コマンド	D-13	D-13
サポートされていない特権 EXEC コマンド	D-13	D-13

サポートされていないグローバル コンフィギュレーション コマンド	D-14
MSDP	D-14
サポートされていない特権 EXEC コマンド	D-14
サポートされていないグローバル コンフィギュレーション コマンド	D-14
マルチキャスト	D-14
サポートされていない BiDirectional PIM (bidir-PIM; 双方向 PIM) コマンド	D-14
サポートされていないマルチキャスト ルーティング マネージャ コマンド	D-14
サポートされていない IP マルチキャスト レート制限コマンド	D-15
サポートされていない UDLR コマンド	D-15
サポートされていない GRE でのマルチキャスト コマンド	D-15
NetFlow コマンド	D-15
サポートされていないグローバル コンフィギュレーション コマンド	D-15
NAT コマンド	D-15
サポートされていない特権 EXEC コマンド	D-15
QoS	D-15
サポートされていないグローバル コンフィギュレーション コマンド	D-15
サポートされていないインターフェイス コンフィギュレーション コマンド	D-15
サポートされていないポリシーマップ コンフィギュレーション コマンド	D-16
RADIUS	D-16
サポートされていないグローバル コンフィギュレーション コマンド	D-16
SNMP	D-16
サポートされていないグローバル コンフィギュレーション コマンド	D-16
SNMPv3	D-16
サポートされていない 3DES 暗号化コマンド	D-16
スパンニング ツリー	D-16
サポートされていないグローバル コンフィギュレーション コマンド	D-16
サポートされていないインターフェイス コンフィギュレーション コマンド	D-17
VLAN	D-17
サポートされていないグローバル コンフィギュレーション コマンド	D-17
サポートされていないユーザ EXEC コマンド	D-17
サポートされていない VLAN データベース コマンド	D-17
VTP	D-17
サポートされていない特権 EXEC コマンド	D-17



はじめに

対象読者

このマニュアルでは、Catalyst 3750 スイッチ（以降、スイッチと記載）を管理するネットワークングの専門家を対象としています。Cisco IOS ソフトウェアの使用経験があり、イーサネットおよび LAN の概念や専門用語を十分理解していることが前提です。

目的

Catalyst 3750 スイッチは、IP ベース イメージまたは IP サービス イメージによってサポートされます。IP ベース イメージは、Access Control List (ACL; アクセス コントロール リスト)、QoS (Quality of Service)、スタティック ルーティング、EIGRP スタブルルーティング、Routing Information Protocol (RIP) を含むレイヤ 2+ 機能を提供します。IP サービス イメージは、より豊富なエンタープライズ クラスの機能セットを提供します。それには、レイヤ 2+ 機能と完全なレイヤ 3 ルーティング (IP ユニキャストルーティング、IP マルチキャスト ルーティング、およびフォールバックブリッジング) が含まれます。IP サービス イメージには、レイヤ 2+ スタティック ルーティングや RIP と区別される特長として、Enhanced Interior Gateway Routing Protocol (EIGRP) や Open Shortest Path First (OSPF) などのプロトコルが含まれています。

このマニュアルでは、スイッチで使用するために作成または変更されたコマンドの使用手順を説明しません。これらのコマンドの詳細は扱いません。これらのコマンドの詳細については、このリリースに対応する『*Catalyst Switch Command Reference*』を参照してください。3750 Cisco IOS Release 12.2 の標準コマンドについては、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software]) にアクセスし、Cisco IOS のマニュアルセットを参照してください。

このマニュアルには、スイッチの管理に使用する組み込みのデバイス マネージャ、または Cisco Network Assistant (以降、*Network Assistant*) の GUI (グラフィカル ユーザ インターフェイス) に関する詳細は記載されていません。ただし、記述されている概念は、GUI ユーザにも有益なものです。デバイス マネージャについては、スイッチのオンライン ヘルプを参照してください。Network Assistant の詳細については、Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。

このマニュアルでは、表示されるシステム メッセージまたはスイッチの設置方法については説明しません。詳細については、このリリースの『*Catalyst 3750 Switch System Message Guide*』および『*Catalyst 3750 Switch Hardware Installation Guide*』を参照してください。

最新のマニュアル更新状況については、このリリースのリリース ノートを参照してください。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

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

対話形式の例では、次の表記法を使用しています。

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

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



(注)

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



注意

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

関連資料

スイッチの詳細については以下のマニュアルも参照してください。これらの資料は次の Cisco.com のサイトでご利用になれます。

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html



(注)

インストール、設定、またはアップグレードを実行する前に、次のマニュアルを参照してください。

- 初期設定の情報については、『Getting Started Guide』の「Using Express Setup」の章、または『Hardware Installation Guide』にある付録の「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイスマネージャの要件については、リリースノート（発注はできませんが、Cisco.com から入手できます）の「System Requirements」を参照してください。
- Network Assistant の要件については、『Getting Started with Cisco Network Assistant』を参照してください（発注はできませんが、Cisco.com から入手できます）。

- クラスタの要件については、『*Release Notes for Cisco Network Assistant*』を参照してください（発注はできませんが、Cisco.com から入手できます）。
- アップグレード情報を入手するには、リリースノートの「**Downloading Software**」を参照してください。

スイッチに関する他の情報については、次のマニュアルを参照してください。

- 『*Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2975, 2970, and 2960 Switch System Message Guide*』
- 『*Catalyst 3750 Switch Software Configuration Guide*』
- 『*Catalyst 3750 Switch Command Reference*』
- デバイス マネージャ オンライン ヘルプ（スイッチで利用可能）
- 『*Catalyst 3750 Switch Hardware Installation Guide*』
- 『*Catalyst 3750 Switch Getting Started Guide*』
- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Release Notes for Cisco Network Assistant*』
- 『*Cisco Small Form-Factor Pluggable Modules Installation Notes*』
- 『*Cisco CWDM GBIC and CWDM SFP Installation Note*』
- 『*Cisco RPS 300 Redundant Power System Hardware Installation Guide*』
- 『*Cisco RPS 675 Redundant Power System Hardware Installation Guide*』
- 『*Cisco Redundant Power System 2300 Hardware Installation Guide*』
- Network Admission Control (NAC) の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- これらの互換性マトリクスに関するマニュアルは、次の Cisco.com サイトにあります。

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

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

これらのマニュアルは、Catalyst 3750G Integrated Wireless LAN Controller スイッチおよび統合ワイヤレス LAN コントローラに関する詳細情報を提供するもので、Cisco.com で入手可能です。

- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』
- 『*Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point*』 Release 4.0.x.0
- 『*Cisco Wireless LAN Controller Configuration Guide*』 Release 4.0
- 『*Cisco Wireless LAN Controller Command Reference*』 Release 4.0

マニュアルの入手方法およびテクニカル サポート

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

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

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



CHAPTER 1

概要

この章では、Catalyst 3750 スイッチ ソフトウェアについて説明します。内容は次のとおりです。

- 「機能」(P.1-1)
- 「スイッチ初期設定後のデフォルト値」(P.1-17)
- 「ネットワークの構成例」(P.1-20)
- 「次の作業」(P.1-30)

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

このマニュアル内の IP という用語は、特に IP Version 6 (IPv6) を参照している場合を除き、IP Version 4 (IPv4) を意味します。

機能

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

- IP ベース イメージ：レイヤ 2+ 機能を提供します（エンタープライズ クラスのインテリジェント サービス）。これらの機能としては、Access Control List (ACL; アクセス コントロール リスト)、QoS (Quality of Service)、スタティック ルーティング、EIGRP スタブルルーティング、PIM スタブルルーティング、Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)、Routing Information Protocol (RIP) などがあります。IP ベース イメージがインストールされたスイッチは、IP サービス イメージにアップグレードできます。
- IP サービス イメージ：より豊富なエンタープライズクラスのインテリジェント サービス セットを提供します。それには、すべての IP ベース イメージ機能と完全なレイヤ 3 ルーティング (IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、およびフォールバック ブリッジング) が含まれます。IP サービス イメージには、レイヤ 2+ スタティック ルーティングや RIP と区別される特長として、Enhanced Interior Gateway Routing Protocol (EIGRP) や Open Shortest Path First (OSPF) などのプロトコルが含まれています。

IP サービス イメージだけに対応するレイヤ 3 機能については、「レイヤ 3 機能」(P.1-14) に記載されています。



(注) 特に注記がないかぎり、このマニュアルで取り上げる機能はすべて、IP ベース イメージと IP サービス イメージでサポートされています。

IPv6 Multicast Listener Discovery (MLD) スヌーピングは、すべての Catalyst 3560 および 3750 イメージでサポートされます。詳細については、第 40 章「IPv6 MLD スヌーピングの設定」を参照してください。

IPv6 のフル サポートでは、IP サービス イメージが必要です。IPv6 ルーティングの詳細については、第 39 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

IPv6 ACL の詳細については、第 41 章「IPv6 ACL の設定」を参照してください。

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

- 「使用および導入を簡素化する機能」(P.1-2)
- 「パフォーマンス向上機能」(P.1-4)
- 「管理オプション」(P.1-6)
- 「管理の簡易性に関する機能」(P.1-6)
- 「アベイラビリティおよび冗長性に関する機能」(P.1-8)
- 「VLAN 機能」(P.1-9)
- 「セキュリティ機能」(P.1-10)
- 「QoS および CoS 機能」(P.1-13)
- 「レイヤ 3 機能」(P.1-14) (IP サービス イメージが必要な機能を含む)
- 「PoE 機能」(P.1-16)
- 「モニタ機能」(P.1-16)

使用および導入を簡素化する機能

- Express Setup は、基本的な IP 情報、コンタクト情報、スイッチおよび Telnet のパスワード、および SNMP（簡易ネットワーク管理プロトコル）に関する情報を使用し、ブラウザ ベースのプログラムを通じて、スイッチの初回設定を迅速に行うことができます。Express Setup の詳細については、『Getting Started Guide』を参照してください。
- ユーザ定義およびデフォルト設定の SmartPort マクロは、ネットワークへの配置を簡単にするためにカスタム スイッチ設定を作成します。
- 組み込みのデバイス マネージャ GUI（グラフィカル ユーザ インターフェイス）は、単体のスイッチを Web ブラウザから設定および管理します。デバイス マネージャの起動については、『Getting Started Guide』を参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Cisco Network Assistant（以降、*Network Assistant* と記載）の機能概要
 - 管理コミュニティは、ルータやアクセス ポイントを組み込むことができる点や、セキュリティを強化できる点以外は、クラスタと同じようなデバイス グループです。
 - イン트라ネットの任意の場所からスイッチ、スイッチ スタック、およびスイッチ クラスタを簡単に最小限の手間で管理できます。
 - 1 つの GUI を使用して、複数の設定作業を行うことができます。特定の処理を実行するための CLI（コマンドライン インターフェイス）コマンドを覚える必要はありません。
 - 対話式のガイド モードで、VLAN（仮想 LAN）、Access Control List（ACL; アクセス制御リスト）、QoS（Quality of Service）などの複雑な機能をガイドに従って設定できます。

- 設定ウィザードを使用すると、トラフィックの QoS プライオリティ、データ アプリケーションのプライオリティ レベル、セキュリティといった複雑な機能を設定するために必要な最小限の情報を、プロンプトの指示に従って入力するだけですみます。
- スイッチにイメージをダウンロードできます。
- VLAN および QoS の設定、目録および統計レポート、リンクおよびスイッチ レベルでのモニタとトラブルシューティング、複数のスイッチのソフトウェア アップグレードといったアクションを、複数のポート、複数のスイッチに対して同時に実行できます。
- 相互接続されたデバイスのトポロジを表示して、既存のスイッチ クラスタ、クラスタに参加できる適格なスイッチ、およびスイッチ間のリンク情報を確認できます。
- 前面パネル イメージで表示される LED によって、単独または複数のスイッチの状態をリアルタイムでモニタできます。このイメージに表示されるシステム LED、Redundant Power System (RPS; 冗長電源システム) LED、およびポート LED の色は、実際の LED の色と同じです。



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

- Cisco StackWise テクノロジーの機能概要
 - StackWise ポートを使用して最大 9 台のスイッチを接続し、ネットワーク内で単一のスイッチまたはスイッチルータとして動作します。
 - スイッチ スタック全体で、双方向 32 Gbps スイッチング ファブリックを作成できます。スイッチ スタックでは、すべてのスタックメンバーがシステム帯域にフルにアクセスできます。
 - 単一の IP アドレスとコンフィギュレーション ファイルを使用して、スイッチ スタック全体を管理できます。
 - 新規スタックメンバーの自動 Cisco IOS バージョン検査。スタック マスターまたは TFTP サーバから自動的にイメージをロードするオプションがあります。
 - スタックの動作を中断せずに、スタック内のスイッチを追加、削除、交換します。
 - オフラインの設定機能を使用して、スイッチ スタックに新しいメンバーを割り当てます。特定のスタック メンバー番号、およびスタックに属していない新しいスイッチの特定のスイッチ タイプを、インターフェイス コンフィギュレーションに事前設定します。割り当てられたスイッチがスタックの一部であるかどうかには関係なく、スイッチ スタックはスタック リロードでこの情報を保持します。
 - スタックリング アクティビティ統計情報（各スタック メンバーからリングに送信されたフレーム数）を表示します。
- スイッチのクラスタ化テクノロジーの機能概要
 - イーサネット、ファスト イーサネット、Fast EtherChannel、Small Form-Factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュール、ギガビット イーサネット、Gigabit EtherChannel 接続を含めて、地理的な近接にも相互接続メディアにも関係なく、複数のクラスタ対応スイッチの設定、モニタ、認証、およびソフトウェア アップグレードをまとめて実行できます。クラスタ対応スイッチのリストについては、リリース ノートを参照してください。
 - 候補スイッチの自動検出と、最大 16 台のスイッチからなるクラスタの作成機能。1 つの IP アドレスを使用してクラスタを管理できます。
 - 拡張検出機能により、コマンド スイッチに直接接続されていないクラスタ候補を検出できます。

- スタックのトラブルシューティング拡張機能
- デフォルト設定およびユーザ定義の **Auto Smartport** マクロは、ポートで検出されたデバイス タイプに基づいたダイナミックポート設定を行います。
- スマート インストールを使用すると、ネットワークに管理のためのシングル ポイント（ディレクタ）を実現できます。スマート インストールを使用することで、新しく導入されたスイッチのイメージおよび設定をゼロ タッチで更新でき、任意のクライアント スwitchのイメージと設定をダウンロードできます。詳細については、『*Cisco Smart Install Configuration Guide*』を参照してください。
- **Auto SmartPort** 拡張機能は、マクロ持続性、Link Layer Discovery Protocol (LLDP) ベースのトリガー、Media Access Control (MAC; メディア アクセス制御) アドレスおよび Organizational Unique Identifier (OUI; 組織固有識別子) ベースのトリガー、リモート マクロ、および新しいデバイス タイプである Cisco Digital Media Player (Cisco DMP) と Cisco IP Video Surveillance Camera (Cisco IPVSC) に基づく自動設定へのサポートを追加します。

パフォーマンス向上機能

- Cisco EnergyWise は Power over Ethernet (PoE) エンティティのエネルギーの使用を管理
詳細については、Cisco.com から入手できる『*Cisco EnergyWise Version 2 Configuration Guide*』を参照してください。
- すべてのスイッチ ポートでの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。帯域幅の利用を最適化します。
- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の **Auto MDIX** 機能により、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定
- ルーテッド フレームの場合は最大 1546 バイト、ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート
- すべてのポートにおける IEEE 802.3x フロー制御（スイッチは休止フレームを送信しません）
- スイッチ スタック内で最大 32Gbps の転送レート
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（Fast EtherChannel）全二重の帯域幅を確保
- Port Aggregation Protocol (PAgP) および Link Aggregation Control Protocol (LACP) により、EtherChannel リンクを自動的に作成
- スタック内の複数のスイッチ間で、レイヤ 2 およびレイヤ 3 パケットをギガビット回線レートで転送
- マルチキャスト Virtual Routing and Forwarding (VRF; VPN ルーティングおよび転送) Lite。ネットワーク バーチャライゼーションおよびバーチャル プライベート マルチキャスト ネットワーク用に複数のプライベート ルーティング ドメインを設定します。
- ポート単位でのストーム制御。ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止できます。
- レイヤ 2 の不明なユニキャスト、マルチキャスト、およびブリッジドブロードキャスト トラフィック転送に対するポートブロッキング

- Cisco Group Management Protocol (CGMP) サーバのサポートおよび Internet Group Management Protocol (IGMP) バージョン 1、バージョン 2、およびバージョン 3 対応の IGMP スヌーピング。
 - (CGMP デバイスの場合) CGMP が特定のエンドステーションへのマルチキャストトラフィックを制限し、ネットワーク全般のトラフィックを軽減
 - (IGMP デバイスの場合) IGMP スヌーピングによってマルチメディアトラフィックとマルチキャストトラフィックを転送
- 1つのマルチキャストルータクエリーにつき1つのIGMPレポートだけをマルチキャストデバイスへ送信するIGMPレポート抑制 (IGMPv1 または IGMPv2 クエリーだけをサポート)。
- IGMP スヌーピングクエリーサポート。IGMP 一般クエリーメッセージを定期的に生成するようにスイッチを設定します。
- IGMP ヘルパーにより、スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャストストリームを加入させることができます。
- Multicast VLAN Registration (MVR)。マルチキャスト VLAN 上でマルチキャストストリームを継続的に送信し、なおかつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。
- IGMP フィルタリング。スイッチポート上のホストが所属できるマルチキャストグループセットを管理します。
- IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定する IGMP スロットリング。
- ネットワーク終了の待ち時間を設定できる IGMP の脱退タイマー。
- Switch Database Management (SDM) テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステムリソースを割り当てられます。
- Web Cache Communication Protocol (WCCP)。トラフィックのローカル広域アプリケーションエンジンへのリダイレクト、コンテンツ要求のローカルでの対処、およびネットワーク内の Web トラフィックパターンのローカライズ (IP サービスイメージが必要) を行います。
- Cisco IOS IP Service Level Agreements (SLA)。Cisco IOS ソフトウェアの一部で、ネットワークパフォーマンスを測定するためにアクティブトラフィックモニタリングを使用します。
- 設定可能なスモールフレーム着信しきい値。スモールフレーム (64 バイト以下) が指定のレート (しきい値) でインターフェイスに着信すると、ストーム制御を防止します。
- Flex Link マルチキャスト高速コンバージェンス。Flex Link が失敗したあとのマルチキャストトラフィックコンバージェンスの時間を短縮します。
- RADIUS サーバロードバランシング。アクセス要求および認証要求がサーバグループの中で均等に分散されるようにします。
- Cisco Medianet。ネットワークインフラストラクチャでの幅広いビデオアプリケーションのインテリジェントサービスを実現します。Medianet のサービスの 1 つは、Auto Smartport による Cisco Digital Media Player および Cisco IP Video Surveillance Camera の自動プロビジョニングです。
- CPU 生成トラフィックの QoS マーキングおよび出力ネットワークポート上での CPU 生成トラフィックのキューのサポート。

管理オプション

- 組み込みデバイス マネージャ : GUI のデバイス マネージャがソフトウェア イメージに組み込まれています。このデバイス マネージャは、単体のスイッチの設定、管理に使用します。デバイス マネージャの起動については、『[Getting Started Guide](#)』を参照してください。デバイス マネージャの詳細については、スイッチのオンラインヘルプを参照してください。
- Network Assistant : Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に使用します。Network Assistant の詳細については、Cisco.com から入手できる『[Getting Started with Cisco Network Assistant](#)』を参照してください。
- CLI : Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、スイッチのコンソール ポートに管理ステーションを直接接続するか、リモート管理ステーションから Telnet を使用します。任意のスタック メンバーのコンソール ポートに接続することにより、スイッチ スタックを管理できます。CLI の詳細については、[第 2 章「CLI の使用方法」](#)を参照してください。
- SNMP : CiscoWorks 2000 LAN Management Suite (LMS) および HP OpenView などの SNMP 管理アプリケーション。HP OpenView、SunNet Manager などのプラットフォームが稼働している SNMP 対応管理ステーションから管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring (RMON; リモート モニタリング) グループをサポートします。SNMP の詳しい使用方法については、[第 33 章「SNMP の設定」](#)を参照してください。
- Cisco IOS Configuration Engine (以前は Cisco IOS CNS エージェントと呼ばれていたもの) : コンフィギュレーション サービスがネットワーク デバイスおよびサービスの配置と管理を自動化します。スイッチごとに設定変更の内容を生成してスイッチに送信し、その設定変更を適用したあと、その結果を記録することで初期設定および設定の更新を自動化できます。
CNS の詳細については、[第 4 章「Cisco IOS Configuration Engine の設定」](#)を参照してください。

管理の簡易性に関する機能

- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。
- Dynamic Host Configuration Protocol (DHCP) によるスイッチ情報 (IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System (DNS; ドメイン ネーム システム)、TFTP サーバ名) の自動設定。
- DHCP リレーによる DHCP クライアントからの UDP ブロードキャストの転送 (IP アドレス要求を含む)。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 特定の設定や新しいイメージを多数のスイッチにダウンロードできる DHCP ベースの自動設定およびイメージアップデート。
- 事前に IP アドレスをスイッチ ポートへ割り当てることができる DHCP サーバ ポート ベースのアドレス割り当て。
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送。
- Address Resolution Protocol (ARP; アドレス解決プロトコル)。IP アドレスおよび対応する Media Access Control (MAC; メディア アクセス制御) アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットを廃棄するユニキャスト MAC アドレス フィルタリング。

- 設定可能な MAC アドレス スケーリングにより、VLAN での MAC アドレス ラーニングをディセーブルにして、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol (CDP; シスコ検出プロトコル) バージョン 1 および 2。ネットワーク トポロジを検出し、ネットワーク上のスイッチと他のシスコ製デバイスとのマッピングを行います。
- Link Layer Discovery Protocol (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED) によるサードパーティ製 IP 電話との相互運用性の確保。
- スイッチからエンドポイント デバイスへロケーション情報を提供する LLDP メディア拡張 (LLDP-MED) ロケーション TLV。
- Network Time Protocol (NTP)。すべてのスイッチに外部ソースから同じタイムスタンプを提供します。
- Cisco IOS File System (IFS; Cisco IOS ファイル システム)。スイッチが使用するすべてのファイル システムに対して単一インターフェイスを提供します。
- SSM PIM プロトコル。マルチキャスト アプリケーション (ビデオなど) を最適化します。
- マルチキャスト アプリケーションに対する Source Specific Multicast (SSM) マッピング。グループへ送信元をマッピングしてリスナーをマルチキャスト ソースへ動的に接続させ、アプリケーションの依存性を軽減します。
- IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズするための Enhanced Interior Gateway Routing Protocol (EIGRP) v6 のサポート。
- IP サービス (HSRP、ARP、SNMP、IP SLA、TFTP、File Transfer Protocol (FTP; ファイル転送プロトコル)、Syslog、traceroute、ping) をサポート。これらのサービスを VRF 認識にすることで、複数のルーティング インスタンスで動作させます。
- スイッチの設定変更を記録して表示させるコンフィギュレーション ロギング。
- 一意のデバイス ID。show inventory ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Communicator または Microsoft Internet Explorer ブラウザセッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- 最大 5 の暗号化 Secure Shell (SSH; セキュア シェル) 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- SNMP のバージョン 1、バージョン 2c、およびバージョン 3 の get および set 要求による帯域内管理アクセス。
- 帯域外管理アクセス。スイッチのコンソール ポートに端末を直接接続するか、またはシリアル接続とモデム経由でリモート端末に接続します。
- Secure Copy Protocol (SCP) 機能。スイッチ設定またはスイッチ イメージ ファイルをセキュアな認証方法でコピーします (ソフトウェアの暗号化バージョンが必要)。
- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼働している設定を交換します。
- Catalyst 3750 Integrated Wireless LAN Controller スイッチのみ、Catalyst 3750 スイッチと最大 25 または 50 の Lightweight アクセスポイントをサポートする Cisco 4400 シリーズ ワイヤレス LAN コントローラが統合されています。
- Cisco IOS の HTTP クライアント サポート。HTTP クライアントが IPv4 HTTP サーバおよび IPv6 HTTP サーバの両方へ要求を送信でき、Cisco IOS の HTTP サーバは同様に両方からの HTTP 要求をサービスできます。

- SNMP。IPv6 トランスポートで設定できるため、IPv6 ホストは SNMP クエリーの送信と IPv6 を実行しているデバイスからの SNMP 通知の受信を行うことができます。
- IPv6 のステートレス自動設定。ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。
- VLAN での MAC アドレス ラーニングのディセーブル化。
- 事前に IP アドレスをスイッチ ポートへ割り当てることができる DHCP サーバ ポート ベースのアドレス割り当て。
- 接続された場所のサービスは、Cisco Mobility Services Engine (MSE) に接続されたデバイスの場所と接続のトラッキング情報を送信します。
- CPU 使用率のしきい値トラップは CPU 使用率をモニタします。
- VLAN、Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP; DiffServ コード ポイント)、およびタグ付けモードを指定して音声と音声シグナリングのプロファイルを作成する LLDP-MED ネットワーク ポリシー Time、Length、Value (TLV; 時間、長さ、時間)。
- DHCPDISCOVER パケットのオプション 12 フィールドへのホスト名挿入のサポート。これによって、DHCP プロトコルを使用して送信される同一のコンフィギュレーション ファイルが提供されます。
- オプション 82 DHCP フィールドのサーキット ID サブオプションに対する固定文字列ベースのフォーマットの選択をサポートする DHCP スヌーピング拡張機能。
- 電力ポリシー TLV 要求に基づいてスイッチが Powered Device (PD; 受電装置) に電力を付与することを認めることにより、LLDP-MED のサポートを拡大します。
- Power over Ethernet (PoE) デバイスおよびデーモンが稼動しているエンド ポイントなどの、EnergyWise エンティティの電力利用を管理する Cisco EnergyWise。

アベイラビリティおよび冗長性に関する機能

- HSRP により、コマンド スイッチとレイヤ 3 ルータの冗長性を確立します。
- 拡張オブジェクト トラッキングは HSRP とトラッキング メカニズムを分離し、HSRP 以外のプロセスで使用可能な個別のスタンダロン型トラッキング プロセスを作成します。
- 自動スタック マスター再選択により、使用不能になったスタック マスターを交換します (フェールオーバーのサポート)。
新たに選択されたスタック マスターは、1 秒以内にレイヤ 2 トラフィックの受信を開始し、3 ~ 5 秒以内にレイヤ 3 トラフィックの受信を開始します。
- クロススタック EtherChannel により、スイッチ スタック全体で冗長リンクが提供されます。
- Unidirectional Link Detection (UDLD; 単一方向リンク検出) およびアグレッシブ UDLD。光ファイバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向リンクを検出し、ディセーブルにします。
- IEEE 802.1D Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) による冗長バックボーン接続およびループフリー ネットワーク。STP には次の機能があります。
 - 最大 128 のスパニング ツリー インスタンスをサポートします。
 - Per-VLAN Spanning-Tree Plus (PVST+) による VLAN 間でのロード バランシングを行います。
 - Rapid PVST+ による、VLAN 間でのロード バランシングおよびスパニング ツリー インスタンスの高速コンバージェンスを実現します。

- UplinkFast、クロススタック UplinkFast、および BackboneFast によって、スパニング ツリー トポロジの変更後に高速コンバージェンスを実行し、ギガビット アップリンクおよびクロススタック ギガビット アップリンクなどの冗長アップリンク間のロード バランシングを達成します。
- IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) により、VLAN をスパニング ツリー インスタンスに分類、またデータ トラフィックおよびロード バランシング用に複数の転送パスを確保します。また、IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP; 高速スパニング ツリー プロトコル) に基づいた Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) により、ルートと指定ポートをただちにフォワーディング ステートに変更することで、スパニング ツリーの高速コンバージェンスが実現されます。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニング ツリーのオプション機能は次のとおりです。
 - PortFast。ポートをブロッキング ステートからフォワーディング ステートへただちに變更させることによって、転送遅延を防ぎます。
 - BPDU ガード。Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) を受信する PortFast 対応ポートをシャットダウンします。
 - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
 - ルート ガード。ネットワーク コア外のスイッチがスパニング ツリー ルートになることを防ぎます。
 - ループ ガード。代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。
- 等価コスト ルーティングにより、リンク レベルとスイッチ レベルの冗長性を確立します。
- Flex Link レイヤ 2 インターフェイス。基本リンク冗長の STP に代わるものとして、互いにバックアップします。
- リンクステート トラッキング。接続されたホストとサーバからのアップストリーム トラフィックを伝送するポートの状態をミラーリングします。また、別のシスコ製イーサネット スイッチで動作するリンクへサーバ トラフィックをフェールオーバーすることができます。
- Cisco Redundant Power System 2300 による RPS サポート。RPS 2300 と呼ばれます。電源の信頼性を向上させ、冗長電源システムの設定と管理ができます。RPS 2300 に関する詳細については、装置に付属され、Cisco.com から入手可能な『Cisco Redundant Power System 2300 Hardware Installation Guide』を参照してください。

VLAN 機能

- 最大 1005 個の VLAN をサポートします。適切なネットワーク リソース、トラフィック パターン、および帯域幅を対応付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 規格で認められている 1 ~ 4094 の範囲で VLAN ID をサポートします。
- ダイナミック VLAN メンバシップに対応する VLAN Query Protocol (VQP)。
- すべてのポート上で稼動する ISL (スイッチ間リンク) および IEEE 802.1Q トランキング カプセル化。ネットワークの移動、追加、変更や、ブロードキャストおよびマルチキャスト トラフィックの管理および制御、さらに、ハイセキュリティ ユーザおよびネットワーク リソース別の VLAN グループの確立によるネットワーク セキュリティを実現します。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)。2 台のデバイス間のリンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタイプ (IEEE 802.1Q または ISL) もネゴシエートします。

- VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) および VTP プルーニング。トラフィックのフラグディングをそのトラフィックを受信するステーションへのリンクだけに制限することによって、ネットワーク トラフィックを削減します。
- 音声 VLAN。Cisco IP Phone から音声トラフィック用のサブネットを作成します。
- VLAN 1 の最小化。VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニング ツリー ループまたはストームのリスクを軽減します。この機能をイネーブルに設定すると、トランク上でユーザ トラフィックは送受信されません。スイッチの CPU は、引き続き制御プロトコル フレームの送受信を行います。
- プライベート VLAN。VLAN スケーラビリティ問題に対応します。より制限された IP アドレスを割り当て、スイッチ上で、レイヤ 2 ポートを他のポートから切り離します。
- プライベート VLAN ホストのポート セキュリティ。ポートで学習される MAC アドレス数を制限します。また、ポートで学習される MAC アドレスを定義します。
- VLAN Flex Link ロード バランシング。Spanning Tree Protocol (STP) を必要としないレイヤ 2 冗長性を提供します。プライマリおよびバックアップ リンクとして設定したインターフェイスのペアを使用して、VLAN ベースによるトラフィックのロード バランシングが可能です。
- 制限付き VLAN (認証失敗 VLAN と呼ばれる) による 802.1X 認証のサポート。
- VTP バージョン 3 のサポート。すべての VTP モードの拡張範囲 VLAN (VLAN 1006 ~ 4094) 設定、拡張認証 (暗号化されたパスワードまたはシークレット パスワード)、他のデータベースの伝播、VTP、VTP プライマリおよびセカンダリ サーバ、および、ポートによる VTP のオン/オフ切り替えオプションのサポートを含みます。

セキュリティ機能

- IP Service Level Agreement (IP SLA; IP サービス レベル契約) のサポート。アクティブ トラフィック モニタリングを使用したネットワーク パフォーマンスを測定します。
- IP SLA EOT。スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッタ、パケット損失などのアクションによってトリガされる IP SLA トラッキング動作からの出力を使用します。
- Web 認証。Web ブラウザを使用して、IEEE 802.1X 機能をサポートしないサブリカント (クライアント) を認証できるようになります。
- ローカル Web 認証バナー。カスタム バナーやイメージ ファイルを Web 認証ログイン画面で表示できます。
- MAC authentication bypass (MAB; MAC 認証バイパス) エージング タイマー。MAB を使用して認証したあとに認証された非アクティブのホストを検出します。
- 管理インターフェイス (デバイス マネージャ、Network Assistant、CLI) へのパスワード保護付きアクセス (読み取り専用および読み書きアクセス)。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポートセキュリティ オプション。
- VLAN 認識ポート セキュリティ オプション。違反の発生時にポート全体をシャットダウンするのではなく、そのポート上の VLAN をシャットダウンします。

- ポートセキュリティ エージング。ポートのセキュアアドレスにエージングタイムを設定します。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP ACL。ルーテッドインターフェイス（ルータ ACL）と VLAN の双方向およびレイヤ 2 インターフェイス（ポート ACL）の受信方向に関するセキュリティ ポリシーを定義します。
- MAC 拡張 ACL。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- VLAN ACL（VLAN マップ）。MAC、IP、および TCP/UDP ヘッダーの情報に基づいてトラフィックをフィルタリングし、VLAN 内のセキュリティを確保します。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- インターフェイスに適用される IPv6 ACL。IPv6 トラフィックをフィルタリングします。
- untrusted（信頼性のない）ホストと DHCP サーバの間の untrusted DHCP メッセージをフィルタリングする DHCP スヌーピング。
- IP ソース ガード。DHCP スヌーピング データベースおよび IP 送信元バインディングに基づきルーティングされないインターフェイスでトラフィックを制限します。
- ダイナミック ARP 検査。同じ VLAN 内の他のポートの無効な ARP 要求や応答を信頼しないことで、スイッチでの悪意のある攻撃を回避します。
- IEEE 802.1Q トンネリングにより、サービスプロバイダーのネットワークをまたがるリモートサイトにユーザがいるカスタマーは、その他のカスタマーから VLAN を分離できます。レイヤ 2 プロトコル トンネリングにより、すべてのユーザに関する完全な STP 情報、CDP 情報、VTP 情報が、カスタマー ネットワークに含まれます。
- レイヤ 2 ポイントツーポイント トンネリング。EtherChannel を自動的に作成します。
- レイヤ 2 プロトコル トンネリングのバイパス機能。サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。次の機能がサポートされています。
 - Multidomain Authentication（MDA; マルチドメイン認証）。データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方が、独立して同一の IEEE 802.1X 対応スイッチ ポートを認証することができます。
 - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
 - VLAN 割り当て。802.1X 認証ユーザを特定の VLAN に制限します。
 - ポートセキュリティ。802.1x ポートへのアクセスを制御します。
 - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
 - IP Phone 検出機能拡張。Cisco IP Phone を検出し識別します。
 - ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
 - 制限付き VLAN。802.1x に準拠はしているが、標準の 802.1x で認証するための証明書を持っていないユーザに制限付きのサービスを提供します。
 - 802.1X アカウンティング。ネットワーク使用をトラッキングします。
 - 802.1X と LAN のウェイクアップ機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。

- 802.1X の準備チェック機能。スイッチに IEEE 802.1X を設定する前に、接続されたエンドホストの準備状態を判断します。
- 音声認識 802.1X セキュリティ。セキュリティ違反が発生した VLAN 上でのみトラフィック違反に反応します。
- MAC 認証バイパス。クライアント MAC アドレスに基づいてクライアントを許可します。
- 802.1X スイッチ サプリカントを使用した Network Edge Access Topology (NEAT)、CISP を使用したホスト許可、および自動イネーブル。別のスイッチのサプリカントとしてワイヤリング クローゼットの外側にあるスイッチを認証します。
- オープン アクセスを使用した IEEE 802.1X。ホストが認証される前にネットワークにアクセスできるようにします。
- ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1X 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを可能にします。
- 柔軟な認証のシーケンス。新しいホストを認証するときポートが試みる認証方式の順序を設定します。
- マルチユーザ認証。複数のホストが 802.1X 対応ポート上で認証可能になります。
- Network Admission Control (NAC; ネットワーク アドミッション コントロール) 機能 :
 - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウィルス対策の状態またはガスチャに関する NAC レイヤ 2 802.1X 検証。
NAC レイヤ 2 802.1X 検証の設定に関する詳細については、「[NAC レイヤ 2 802.1X 検証の設定](#)」(P.10-58) を参照してください。
 - デバイスのネットワーク アクセスを許可する前の、エンドポイント システムまたはクライアントのガスチャに関する NAC レイヤ 2 IP 検証。
NAC レイヤ 2 IP 検証の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
 - IEEE 802.1x アクセス不能認証バイパス。
この機能の設定については、「[アクセス不能認証バイパス機能の設定](#)」(P.10-53) を参照してください。
 - Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) ダウン ポリシー。態勢検証が発生したときに、AAA サーバが利用できない場合のホストの NAC レイヤ 2 IP 検証。
この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- Terminal Access Controller Access Control System Plus (TACACS+)。TACACS サーバを介してネットワーク セキュリティを管理する独自の機能です。
- RADIUS。AAA サービスによってリモート ユーザの身元を確認し、リモート ユーザにアクセス権を与え、リモート ユーザのアクションをトラッキングします。
- Kerberos セキュリティ システム。信頼できるサードパーティを使用して、ネットワーク リソースに対する要求を認証します (ソフトウェアの暗号化バージョンが必要)。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer (SSL) バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります (ソフトウェアの暗号化バージョンが必要)。
- 音声認識 IEEE 802.1X および MAC Authentication Bypass (MAB; MAC 認証バイパス) セキュリティ違反。セキュリティ違反が発生すると、ポートのデータ VLAN だけがシャットダウンされません。

- スタティック ホストでの IP ソース ガードのサポート
- RADIUS Change of Authorization (CoA)。セッションが認可された後でそのアトリビュートを変更します。AAA のユーザまたはユーザ グループのポリシーに変更がある場合、管理者は、認証を再インストールするための Cisco Secure ACS などの RADIUS CoA パケットを AAA サーバから送信し、新しいポリシーに適用できます。
- IEEE 802.1X ユーザ ディストリビューション。複数の VLAN (ユーザのグループ向け) のある展開を可能にし、異なる VLAN 間でユーザをロード バランシングすることでネットワークのスケラビリティを増大します。許可されたユーザは、RADIUS サーバによって割り当てられたグループで最もユーザの少ない VLAN に割り当てられます。
- クリティカルな VLAN での複数ホスト認証のサポート。ポートが multi-auth に設定され、AAA サーバが到達不能になったときにも重要なリソースへのアクセスを許可するために、そのポートはクリティカルな VLAN に配置されます。
- カスタマイズ可能な Web 認証機能拡張。ローカル Web 認証のためのユーザ定義 login、success、failure および expire Web ページを作成します。
- Network Edge Access Topology (NEAT) のサポート。ポート ホスト モードを変更し、オーセンティケータ スイッチ ポートに標準ポート設定を適用します。
- MAC 認証に基づく VLAN-ID。ユーザ認証に VLAN および MAC アドレス情報の組み合わせを使用して、許可されていない VLAN からのネットワーク アクセスを防止します。
- MAC 移動。ホスト (IP Phone の後ろに接続されたホストを含む) は、同じスイッチのポート間でモビリティに対して制約されることなく移動できます。MAC 移動によって、スイッチは別のポート上での同じ MAC アドレスの再現を、完全に新しい MAC アドレスと同じ方法で処理します。
- Simple Network Management Protocol version 3 (SNMPv3; 簡易ネットワーク プロトコルバージョン 3) による Triple Data Encryption Standard (3DES) および Advanced Encryption Standard (AES) のサポート。このリリースでは、168 ビットの Triple Data Encryption Standard (3DES) および 128 ビット、192 ビット、256 ビットの Advanced Encryption Standard (AES) 暗号アルゴリズムのサポートが SNMPv3 に追加されました。

QoS および CoS 機能

- Automatic QoS (auto-QoS; 自動 QoS)。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。
- ポートベースの信頼の自動 QoS VoIP 拡張と DSCP および出トラフィックのプライオリティ キューイング。
- クロススタック QoS により、個々のスイッチ単位ではなく、スイッチ スタック内のすべてのスイッチに QoS 機能を設定します。
- 分類
 - IP Type of Service/Differentiated Services Code Point (IP ToS/DSCP) および IEEE 802.1p CoS のポート単位でのプライオリティ設定。ミッションクリティカルなアプリケーションのパフォーマンスを保護します。
 - IP ToS/DSCP および IEEE 802.1p CoS (サービス クラス) のフローベースの packets 分類 (MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく) によるマーキング。ネットワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化されたサービス レベルを可能にするとともに、ネットワーク上のミッションクリティカルなトラフィックにプライオリティを設定します。
 - QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted (信頼性のある) ポート ステート (CoS、DSCP、および IP precedence)。

- 信頼境界機能。Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポートセキュリティを確保します。
- ポリシング
 - 特定のトラフィック フローに対してどの程度のポート帯域幅を割り当てるかを管理する、スイッチ ポート上のトラフィック ポリシング ポリシー。
 - 階層型のポリシー マップで複数のクラス マップを作成する場合、各クラス マップを自身のポートレベル (第 2 レベル) ポリシー マップと関連付けることができます。第 2 レベルのポリシー マップは、それぞれ異なるポリサーを保有できます。
 - トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーションまたはトラフィック フローをあらかじめ定義された特定のレートに制限します。
- 不適合
 - 帯域幅の使用制限を超過したパケットの不適合マークダウン。
- 入力キューイングおよびスケジューリング
 - ユーザ トラフィック用に設定可能な 2 つの入力キュー (一方のキューをプライオリティ キューにできます)。
 - 輻輳回避メカニズムとしての Weighted Tail Drop (WTD)。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
 - Shaped Round Robin (SRR; シェイプド ラウンド ロビン) : パケットがキューからスタック リングへ送出される際のレートを決定するスケジューリング サービス (入力キューでサポートされる唯一のモードはシェアリング)。
- 出力キューおよびスケジューリング
 - 1 ポートに 4 つの出力キュー。
 - 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
 - スケジューリング サービスとしての SRR。キューからパケットを出して出力インターフェイスに入れる速度を指定します (出力キューではシェーピングおよび共有がサポートされます)。シェーピング型出力キューは、ポート帯域幅の割り当てが保証されますが、割り当てられたポート帯域幅の使用に制限されています。共有型出力キューは、設定された帯域幅の割り当てが保証されるだけでなく、他のキューが空になり、その割り当て分の帯域幅が使用されない場合、保証された割り当てより多く使用できます。
- IPv6 QoS trust 機能のサポート

レイヤ 3 機能

次に、レイヤ 3 機能について説明します。



(注)

ここで取り上げる一部の機能は IP サービス イメージだけに対応しています。

- レイヤ 3 ルータの冗長性に対応した HSRP バージョン 1 (HSRPv1)、HSRP バージョン 2 (HSRPv2)、および HSRP バージョン 3 (HSRPv3)。
- IP ルーティング プロトコルによるロード バランシングとスケーラブルなルーテッド バックボーンの構築 :
 - RIP バージョン 1 および 2。

- OSPF (IP サービス イメージが必要)。
- Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6。IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズします。
- IPv6 対応 HSRP (拡張 IP サービス イメージが必要)。
- Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) バージョン 4 (IP サービス イメージが必要)。
- 2 つ以上の VLAN 間の完全レイヤ 3 ルーティング対応の IP ルーティング (VLAN 間ルーティング) により、各 VLAN による独自の自律データリンク ドメインのメンテナンスが可能になります。
- Policy-Based Routing (PBR; ポリシーベース ルーティング)。トラフィック フローに定義済みポリシーを設定します。
- Customer Edge (CE; カスタマー エッジ) デバイスの複数の VPN ルーティング/転送 (マルチ VRF) インスタンス。サービス プロバイダーが、複数の Virtual Private Network (VPN; バーチャルプライベート ネットワーク) をサポートし、VPN 間で IP アドレスを重複できるようにします (IP サービス イメージが必要)。
- フォールバック ブリッジングによる 2 つ以上の VLAN 間での非 IP トラフィックの転送 (IP サービス イメージが必要)。
- スタティック IP ルーティングによるネットワーク パス情報のルーティング テーブル手動作成。
- 等価コスト ルーティングによるロード バランシングおよび冗長構成。
- Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) および ICMP Router Discovery Protocol (IRDP)。ルータのアドバタイズおよびルータ請求メッセージにより直接接続サブネット上のルータのアドレスを検索します。
- Protocol-Independent Multicast (PIM) によるネットワーク内マルチキャスト ルーティング。これにより、ネットワーク内のデバイスは要求されたマルチキャスト フィードの受信が可能になり、マルチキャストに参加しないスイッチのプルーニングが可能になります。PIM sparse mode (PIM-SM; PIM 希薄モード)、PIM dense mode (PIM-DM; PIM 稠密モード)、および PIM sparse-dense モードのサポートも含まれます (IP サービス イメージが必要)。
- Multicast Source Discovery Protocol (MSDP)。複数の PIM-SM ドメインを接続します (IP サービス イメージが必要)。
- Distance Vector Multicast Routing Protocol (DVMRP; ディスタンスベクトル マルチキャスト ルーティング プロトコル) トンネリング。非マルチキャスト ネットワークでの 2 つのマルチキャスト 対応ネットワークを相互接続します (IP サービス イメージが必要)。
- DHCP リレーにより、IP アドレス要求など DHCP クライアントからの UDP ブロードキャストを転送します。
- IPv6 のリレー、クライアント、サーバアドレス割り当て、プレフィクス委任に対応した DHCP。
- 設定されたインターフェイスを介して IPv6 トラフィックを転送するための IPv6 ユニキャスト ルーティング機能 (IP サービス イメージが必要)。
- IPv6 Default Router Preference (DRP; デフォルト ルータの初期設定)。ホスト性能を改善することで、適切なルータを選択します。
- Nonstop Forwarding (NSF) 認識。プライマリ Route Processor (RP; ルート プロセッサ) が障害を起こして、バックアップ RP が引き継ぐ間、またはプライマリ RP で無停止のソフトウェア アップグレードのリロードが手動で行われている間、レイヤ 3 スイッチが NSF 対応近接ルータからのパケットを継続して転送することが可能になります (IP サービス イメージが必要)。
- OSPF および EIGRP の NSF 対応ルーティング。NSF 認識および NSF 対応ネイバーからの情報に基づいてスイッチがルーティング テーブルを再構築することができます。

- Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) ラインステートのアップまたはダウンの計算から VLAN ポートを除外する機能。
- Intermediate System-to-Intermediate System (IS-IS) ルーティングは、Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) ネットワークに対応するダイナミック ルーティング プロトコルをサポートします。

PoE 機能

- 回路上に電力が供給されていないことをスイッチが検出した場合、Power over Ethernet (PoE) 対応ポートに接続されたシスコ製先行標準および IEEE 802.3af 準拠の受電装置に電力を供給できます。
- 電力消費を含む CDP をサポートします。受電装置は、消費している電力量をスイッチに通知します。
- シスコのインテリジェント電力管理をサポートします。受電装置およびスイッチは、電力ネゴシエーション CDP メッセージによってネゴシエーションを行い、電力消費レベルについて合意します。このネゴシエーションにより、高電力のシスコ受電装置は、最高電力モードで動作できるようになります。
- 自動検出およびパワー バジェット。スイッチはパワー バジェットを維持し、電力要求をモニタおよびトラッキングし、利用できる場合のみ電力を供給します。

モニタ機能

- EOT および IP SLA EOT スタティック ルートのサポート。事前に設定したスタティック ルートまたは DHCP ルートがダウンした場合に特定します。
- デバイスおよびシステム管理用の Embedded Event Manager (EEM; 組み込みイベント マネージャ)。主なシステム イベントをモニタし、ポリシーに従って動作します (IP サービス イメージが必要)。
- EEM 3.2 のサポート。近隣探索、ID、および、MAC アドレス テーブルにイベント ディテクタを導入します。
- スイッチ LED による、ポート レベル、スイッチ レベル、およびスタック レベルのステータス確認。
- MAC アドレス通知トラップおよび RADIUS アカウンティング。スイッチが学習または削除した MAC アドレスを保存することによって、ネットワーク上のユーザをトラッキングします。
- Switched Port Analyzer (SPAN; スイッチドポート アナライザ) および Remote SPAN (RSPAN)。任意のポートまたは VLAN について、トラフィック モニタリングが可能です。
- Intrusion Detection System (IDS; 侵入検知システム) における SPAN および RSPAN のサポート。ネットワーク セキュリティ違反をモニタ、撃退、およびレポートします。
- 組み込み RMON エージェントの 4 つのグループ (履歴、統計、アラーム、およびイベント) を使用して、ネットワークをモニタし、トラフィック解析を行うことができます。
- Syslog 機能。認証または許可エラー、リソースの問題、およびタイムアウト イベントに関するシステム メッセージを記録します。
- レイヤ 2 traceroute。パケットが送信元デバイスから宛先デバイスへ送られる物理パスを識別します。

- Time Domain Reflector (TDR)。10/100/1000 の銅線イーサネット ポートでケーブル接続の問題を診断し、解決します。
- SFP モジュール診断管理インターフェイス。SFP モジュールの物理または動作ステータスをモニタします。
- 汎用オンライン診断。スイッチが稼働中のネットワークに接続している間に、スーパーバイザ エンジン、モジュール、およびスイッチのハードウェア機能をテストします。
- HSRP に対する拡張オブジェクト トラッキング。
- Digital Optical Monitoring (DOM; デジタル オプティカル モニタリング)。X2 SFP モジュールのステータスを確認します。

スイッチ初期設定後のデフォルト値

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



(注)

ブラウザベースの Express Setup プログラムによる IP アドレスの割り当てについては、『Getting Started Guide』を参照してください。CLI ベースの設定プログラムによる IP アドレスの割り当てについては、『Hardware Installation Guide』を参照してください。

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

- デフォルト スイッチ IP アドレス、サブネット マスク、デフォルト ゲートウェイは 0.0.0.0 です。詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」および第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。
- ドメイン名はデフォルトで設定されていません。詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブルに設定されています (DHCP サーバとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。DHCP リレー エージェントはイネーブルに設定されています (DHCP リレー エージェントとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」および第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。
- スイッチ スタックはイネーブルに設定されています (設定変更できません)。詳細については、第 5 章「スイッチ スタックの管理」を参照してください。
- スイッチ クラスタはディセーブルに設定されています。スイッチ クラスタの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチの管理」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチの管理」を参照してください。
- NTP はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。

- DNS はイネーブルに設定されています。詳細については、第 7 章「スイッチの管理」を参照してください。
- TACACS+ はディセーブルに設定されています。詳細については、第 9 章「スイッチ ベース認証の設定」を参照してください。
- RADIUS はディセーブルに設定されています。詳細については、第 9 章「スイッチ ベース認証の設定」を参照してください。
- 標準の HTTP サーバおよび SSL HTTPS サーバは両方もイネーブルに設定されています。詳細については、第 9 章「スイッチ ベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルに設定されています。詳細については、第 10 章「IEEE 802.1X ポートベース認証の設定」を参照してください。
- ポート パラメータ
 - 動作モードはレイヤ 2 (スイッチポート) です。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
 - インターフェイス速度およびデュプレックス モードが自動ネゴシエーションに設定されています。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
 - Auto-MDIX はイネーブルに設定されています。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
 - フロー制御はディセーブルに設定されています。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
 - PoE は自動ネゴシエーションに設定されています。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。
- VLAN
 - デフォルト VLAN は VLAN 1 です。詳細については、第 14 章「VLAN の設定」を参照してください。
 - VLAN トランキング設定は dynamic auto (DTP) です。詳細については、第 14 章「VLAN の設定」を参照してください。
 - トランク カプセル化はネゴシエーションです。詳細については、第 14 章「VLAN の設定」を参照してください。
 - VTP モードはサーバです。詳細については、第 15 章「VTP の設定」を参照してください。
 - VTP バージョンはバージョン 1 です。詳細については、第 15 章「VTP の設定」を参照してください。
 - プライベート VLAN は設定されていません。詳細については、第 17 章「プライベート VLAN の設定」を参照してください。
 - 音声 VLAN はディセーブルに設定されています。詳細については、第 16 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルに設定されています。詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
- STP、PVST+ は VLAN 1 でイネーブルに設定されています。詳細については、第 19 章「STP の設定」を参照してください。
- MSTP はディセーブルに設定されています。詳細については、第 20 章「MSTP の設定」を参照してください。
- オプションのスパニング ツリー機能はディセーブルに設定されています。詳細については、第 21 章「オプションのスパニング ツリー機能の設定」を参照してください。

- Flex Link は設定されていません。詳細については、第 22 章「Flex Link および MAC アドレステーブル移動更新機能の設定」を参照してください。
- DHCP スヌーピングはディセーブルに設定されています。DHCP スヌーピング情報オプションはイネーブルに設定されています。詳細については、第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。
- IP ソース ガードはディセーブルに設定されています。詳細については、第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。
- DHCP サーバ ポート ベースのアドレス割り当てはディセーブルに設定されています。詳細については、第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。
- ダイナミック ARP インスペクションはすべての VLAN でディセーブルに設定されています。詳細については、第 24 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルに設定されています。IGMP フィルタは適用されていません。詳細については、第 25 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否されます。詳細については、第 25 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルに設定されています。詳細については、第 25 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細については、第 25 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- ポートベース トラフィック
 - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルに設定されています。詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。
 - 保護ポートは定義されていません。詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。
 - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされていません。詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。
 - セキュア ポートは設定されていません。詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。
- CDP はイネーブルに設定されています。詳細については、第 27 章「CDP の設定」を参照してください。
- UDLD はディセーブルに設定されています。詳細については、第 29 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細については、第 31 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細については、第 32 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています (バージョン 1)。詳細については、第 33 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。

- QoS はディセーブルに設定されています。詳細については、[第 36 章「QoS の設定」](#)を参照してください。
- EtherChannel は設定されていません。詳細については、[第 37 章「EtherChannel およびリンクステート トラッキングの設定」](#)を参照してください。
- IP ユニキャスト ルーティングはディセーブルに設定されています。詳細については、[第 38 章「IP ユニキャスト ルーティングの設定」](#)を参照してください。
- IPv6 ユニキャスト ルーティングはディセーブルに設定されています。詳細については、[第 39 章「IPv6 ユニキャスト ルーティングの設定」](#)を参照してください。
- HSRP グループは設定されていません。詳細については、[第 42 章「HSRP の設定」](#)を参照してください。
- IP マルチキャスト ルーティングはすべてのインターフェイスでディセーブルに設定されています。詳細については、[第 46 章「IP マルチキャスト ルーティングの設定」](#)を参照してください。
- MSDP はディセーブルに設定されています。詳細については、[第 47 章「MSDP の設定」](#)を参照してください。
- フォールバック ブリッジングは設定されていません。詳細については、[第 48 章「フォールバックブリッジングの設定」](#)を参照してください。

ネットワークの構成例

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

- 「[スイッチを使用する場合の設計概念](#)」 (P.1-20)
- 「[Catalyst 3750 スイッチを使用した中小規模のネットワーク](#)」 (P.1-26)
- 「[Catalyst 3750 スイッチによる大規模ネットワーク](#)」 (P.1-27)
- 「[Catalyst 3750 スイッチによる集合住宅ネットワーク](#)」 (P.1-28)
- 「[長距離広帯域トランスポートの構成](#)」 (P.1-30)

スイッチを使用する場合の設計概念

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

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

表 1-1 ネットワーク パフォーマンスの向上

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

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

表 1-2 ネットワーク サービスの提供

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

表 1-2 ネットワーク サービスの提供 (続き)

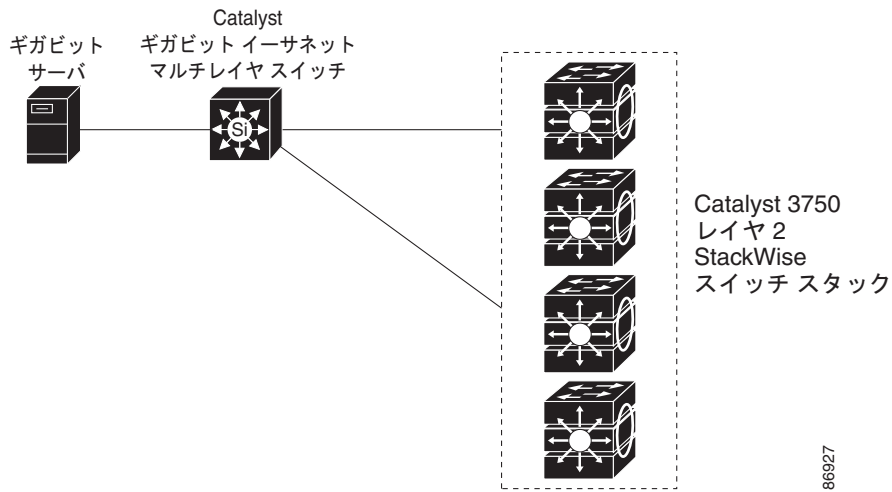
ネットワークに対する需要	推奨する設計方式
常時オンのミッションクリティカルなアプリケーションを実現するための、ネットワークの冗長性およびアベイラビリティに対する大きな需要	<ul style="list-style-type: none"> スタック マスターに障害が生じた場合、すべてのスタック メンバーがスタック マスターの代わりに機能できるスイッチ スタックを使用します。すべてのスタック メンバーが、スイッチ スタックの保存済み実行コンフィギュレーション ファイルの同期化されたコピーを持っています。 クロススタック EtherChannel を使用すると、スイッチ スタック全体で冗長リンクを提供します。 HSRP を使用して、クラスタ コマンド スイッチとルータの冗長構成を確立します。 VLAN トランク、クロススタック UplinkFast、および BackboneFast を使用して、アップリンク ポート上でトラフィックのロード バランシングを実行し、VLAN トラフィックの転送時にポート コストが低いアップリンク ポートが選択されるようにします。
IP テレフォニーに対する新しい需要	<ul style="list-style-type: none"> QoS を使用して、輻輳の発生時に IP テレフォニーなどのアプリケーションを優先順位付けし、ネットワーク内で発生する遅延およびジッタを制御できるようにします。 1 ポートあたり少なくとも 2 つのキューをサポートするスイッチを使用して、音声およびデータ トラフィックのプライオリティを IEEE 802.1p/Q に基づくハイプライオリティまたはロープライオリティのいずれかに設定します。スイッチは、1 ポートあたり少なくとも 4 つのキューをサポートします。 Voice VLAN ID (VVID) を使用して、音声トラフィックに別個の VLAN を用意します。
既存のインフラストラクチャを利用して、自宅または会社からインターネットまたはイントラネットヘッダーおよび音声を高速で伝送する需要の増大	<p>Catalyst Long-Reach Ethernet (LRE) スイッチを使用して、既存のインフラストラクチャ (既存の電話回線など) 上で最大 15MB の IP 接続を提供します。</p> <p>(注) LRE は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチに採用されているテクノロジーです。LRE については、各スイッチ固有のマニュアルセットを参照してください。</p>

スイッチおよびスイッチ スタックを使用して、次のものを作成できます。

- コスト効率の高いワイヤリング クローゼット (図 1-1) : 多数のユーザをワイヤリング クローゼットに接続するコスト効率の高い手法は、最大 9 台の Catalyst 3750 スイッチからなるスイッチ スタックを配備することです。スタック内の 1 台のスイッチに障害が生じた場合にスイッチ接続を維持するには、『Hardware Installation Guide』で推奨されるとおりにスイッチを接続し、クロススタック Etherchannel またはクロススタック UplinkFast のいずれかをイネーブルにします。

スイッチ スタック内の SFP モジュールを使用して、Catalyst4500 や Catalyst 3750-12S ギガビット スイッチなどのギガビット バックボーン スイッチへの冗長アップリンク接続を確立できます。ファストイーサネット、ギガビット、または EtherChannel の各リンクを使用してバックアップ パスを作成することもできます。冗長接続のいずれか一方に障害が発生しても、もう一方がバックアップ パスとして機能します。ギガビット スイッチがクラスタ対応の場合は、そのスイッチとスイッチ スタックを 1 つのスイッチ クラスタとして設定し、単一の IP アドレスを使ってそれらを管理できます。1000BASE-T 接続を使用して、ギガビット スイッチをギガビット サーバへ接続できます。

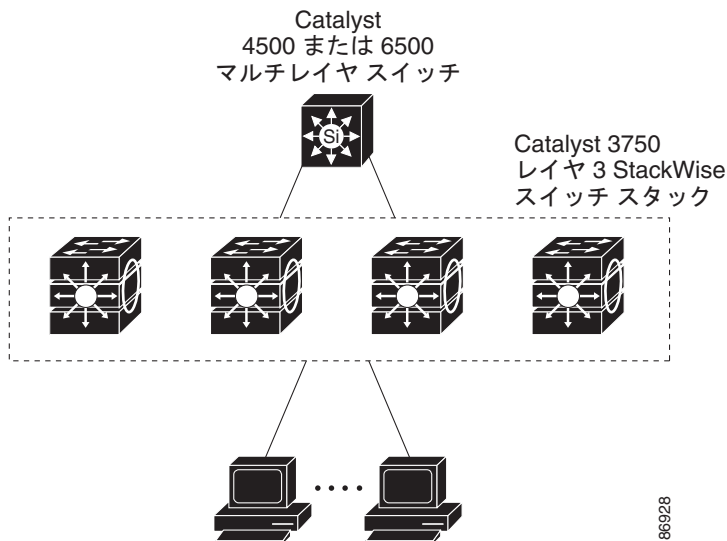
図 1-1 コスト効率の高いワイヤリング クローゼット



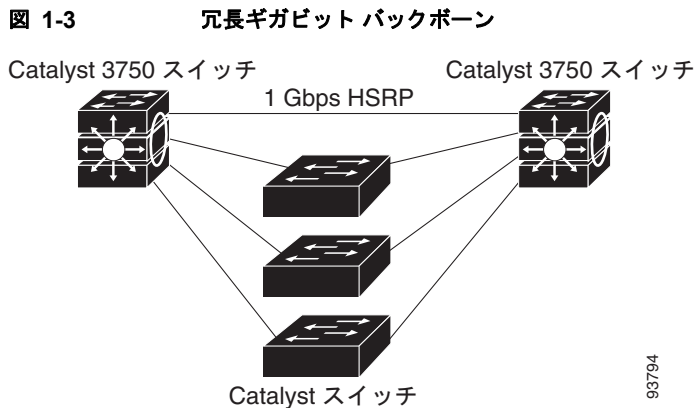
- 高性能ワイヤリング クローゼット (図 1-2) : ネットワーク リソースへ高速アクセスする場合、アクセス レイヤで Catalyst 3750 スイッチとスイッチ スタックを使用すると、デスクトップにギガビットイーサネットを設定できます。輻輳を回避するために、各スイッチ上で QoS DSCP マーキングによるプライオリティ設定を使用します。ディストリビューション層で高速 IP 転送を実現するには、アクセス層のスイッチを、Catalyst 4500 ギガビットスイッチや Catalyst 6500 ギガビットスイッチなどのバックボーン内のギガビットマルチレイヤ スイッチに接続します。

この構成では、各スイッチはネットワーク リソースにアクセスするための、専用の 1 Gbps 接続をユーザに提供します。SFP モジュールを使用すると、光ファイバ接続におけるメディアおよび距離のオプションに柔軟性も提供されます。

図 1-2 高性能ワイヤリング クローゼット



- 冗長ギガビット バックボーン：HSRP によって、2 つの Catalyst 3750G マルチレイヤ ギガビット スイッチ間にバックアップパスを作成して、異なる VLAN およびサブネットのネットワーク信頼性とロード バランシングを強化できます。また、HSRP によって、ネットワーク障害発生時のネットワーク コンバージェンスも高速化されます。Catalyst スイッチは再びスター型構成で、2 つの Catalyst 3750G マルチレイヤ バックボーン スイッチに接続できます。バックボーン スイッチのいずれか一方に障害が生じて、もう一方のバックボーン スイッチが、スイッチとネットワーク リソース間の接続を維持します。



- サーバ集約 (図 1-4) と Linux サーバクラスタ (図 1-5)：スイッチとスイッチ スタックを使用して、サーバグループを相互接続し、ネットワークの物理的なセキュリティと管理を一元化できます。ディストリビューション レイヤで高速 IP 転送を実現するには、アクセス レイヤ スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えることができます。

スイッチ上の QoS およびポリシングによって、特定のデータ ストリームが優先的に処理されます。トラフィック ストリームはいくつかの経路に分けられて処理されます。スイッチのセキュリティ機能によって、パケットの高速処理が保証されます。

サーバラックからコアへの耐障害性は、冗長ギガビット EtherChannel とクロススタック EtherChannel を持つデュアル スイッチ スタックに接続された、デュアル ホーミング サーバによって達成されます。

スイッチのデュアル SFP モジュール アップリンクを使用すると、ネットワーク コアに冗長アップリンクが提供されます。SFP モジュールを使用すると、光ファイバ接続におけるメディアおよび距離のオプションに柔軟性が提供されます。

0.5 ~ 3 m までのさまざまな長さのスタック ケーブルが使用可能なため、複数のサーバラック間のスイッチ スタックの接続を拡張して、複数のスタック集約を実現できます。

図 1-4 サーバ集約

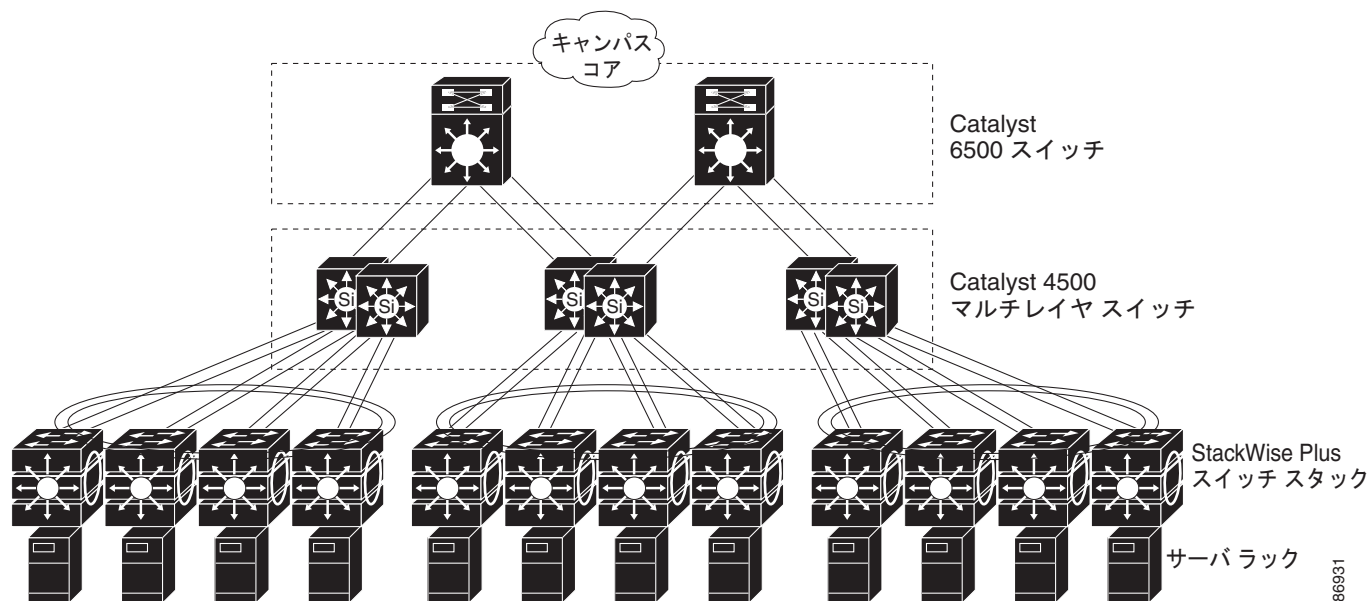
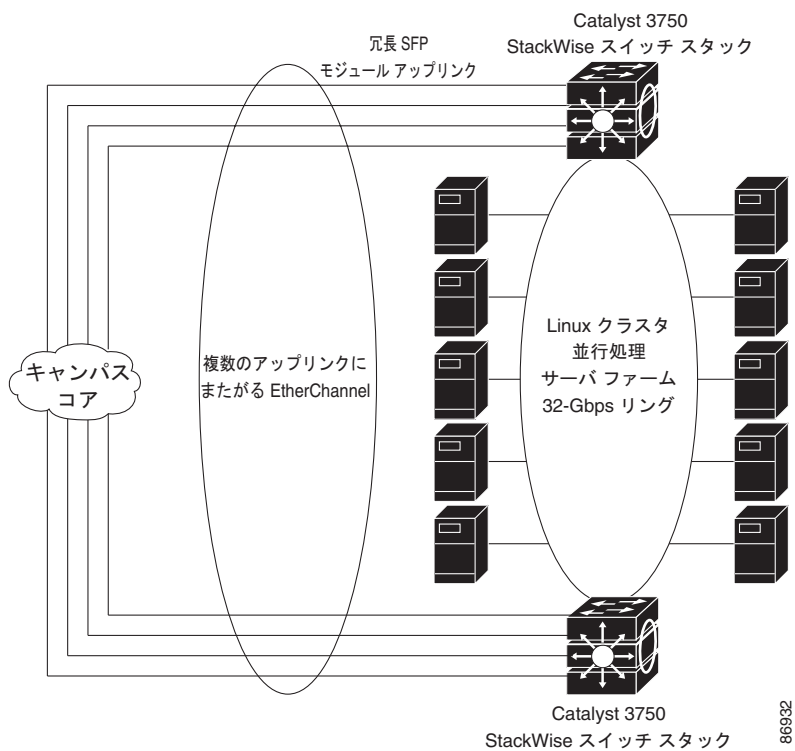


図 1-5 Linux サーバクラスタ



Catalyst 3750 スイッチを使用した中小規模のネットワーク

図 1-6 に、最大 500 人の社員を対象とするネットワークの構成例を示します。このネットワークでは、2 つのルータへの高速接続を実現する Catalyst 3750 レイヤ 3 スイッチ スタックを使用します。ネットワークの信頼性とロード バランシングのために、このネットワークでは HSRP をルータとスイッチでイネーブルにしています。これにより、万ルータやスイッチの 1 つに障害が発生した場合でも、インターネット、WAN、およびミッションクリティカルなネットワーク リソースへの接続が保証されます。スイッチは、より高速にフェールオーバーを実行するためにルーテッドアップリンクを使用しています。また、ロード バランシングと冗長構成用に等価コスト ルーティングが設定されています（レイヤ 2 スイッチ スタックは、ロード バランシングにクロススタック EtherChannel を使用できます）。

スイッチは、ワークステーション、ローカル サーバ、および IEEE 802.3af 準拠（および非準拠）の受電装置（Cisco IP Phone など）に接続されています。サーバファームには、Cisco CallManager (CCM) ソフトウェアを実行するコール処理サーバが含まれます。CCM は、コール処理、ルーティング、および Cisco IP Phone 機能とその設定を制御します。スイッチは、ギガビット インターフェイスによって相互接続されています。

このネットワークでは、VLAN を使用してネットワークを明確なブロードキャスト グループとして論理的に分割し、セキュリティ管理を行っています。データトラフィックおよびマルチメディアトラフィックは同じ VLAN 上で設定されます。Cisco IP Phone からの音声トラフィックは、別個の VVID 上に設定します。データ、マルチメディア、および音声トラフィックを同じ VLAN に割り当てる場合は、ワイヤリング クローゼットごとに 1 つの VLAN しか設定できません。

ある VLAN のエンドステーションが別の VLAN にあるエンドステーションと通信する必要がある場合、ルータまたはレイヤ 3 スイッチが宛先 VLAN にトラフィックをルーティングします。このネットワークでは、スイッチスタックが VLAN 間ルーティングを行います。スタック上の VLAN アクセスコントロールリスト (VLAN マップ) が VLAN 内セキュリティを設定し、不正ユーザがネットワークの重要な領域にアクセスしないようにします。

VLAN 間ルーティング以外に、マルチレイヤ スイッチが DSCP プライオリティなどの QoS メカニズムを使用して各種ネットワークトラフィックに優先順位を付け、ハイプライオリティトラフィックを配信します。輻輳が発生した場合、QoS がロープライオリティトラフィックを廃棄し、ハイプライオリティトラフィックを伝送できるようにします。

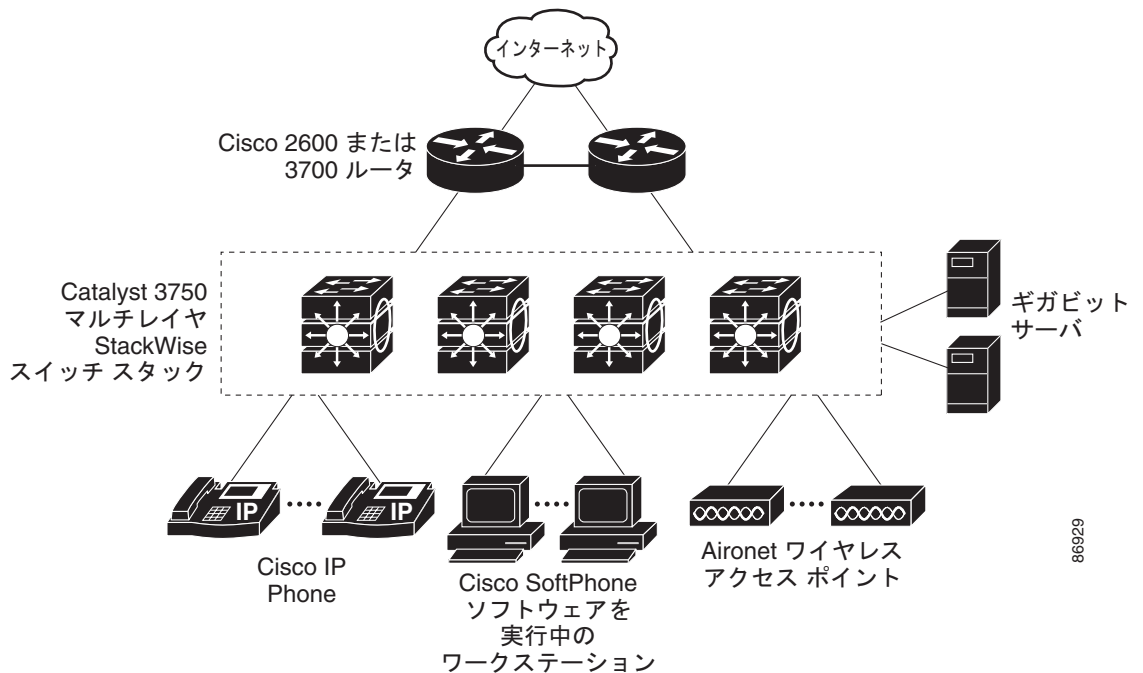
Catalyst PoE スイッチと接続している先行標準の受電装置および IEEE 802.3af 準拠の受電装置では、IEEE 802.1p/Q QoS を使用することにより、音声トラフィックをデータトラフィックよりも優先的に転送できます。

Catalyst PoE スイッチポートは、シスコの先行標準の受電装置および IEEE 802.3af 準拠の受電装置の接続を自動的に検出します。各 PoE スイッチポートは、各ポートに 15.4 W の電力を供給します。受電装置（Cisco IP Phone など）が AC 電源に接続されている場合、冗長化された電力供給を受けることができます。Catalyst PoE スイッチに接続していない受電装置は、電力を得るために AC 電源に接続する必要があります。

CCM は、コール処理、ルーティング、および Cisco IP Phone 機能とその設定を制御します。Cisco SoftPhone ソフトウェアを実行しているワークステーションを持つユーザは、PC からのコールを配置、受信、および制御できます。Cisco IP Phone、CCM ソフトウェア、および Cisco SoftPhone ソフトウェアを使用することで、テレフォニーと IP ネットワークを統合でき、IP ネットワークが音声とデータをサポートします。

VLAN 間ルーティングや他のネットワーク サービスを提供するマルチレイヤ スイッチを使用することで、ルータが重点を置くのは、ファイアウォール サービス、Network Address Translation (NAT; ネットワーク アドレス変換) サービス、Voice over IP (VoIP) ゲートウェイ サービス、WAN およびインターネット アクセスです。

図 1-6 コラプスト バックボーン設定



Catalyst 3750 スイッチによる大規模ネットワーク

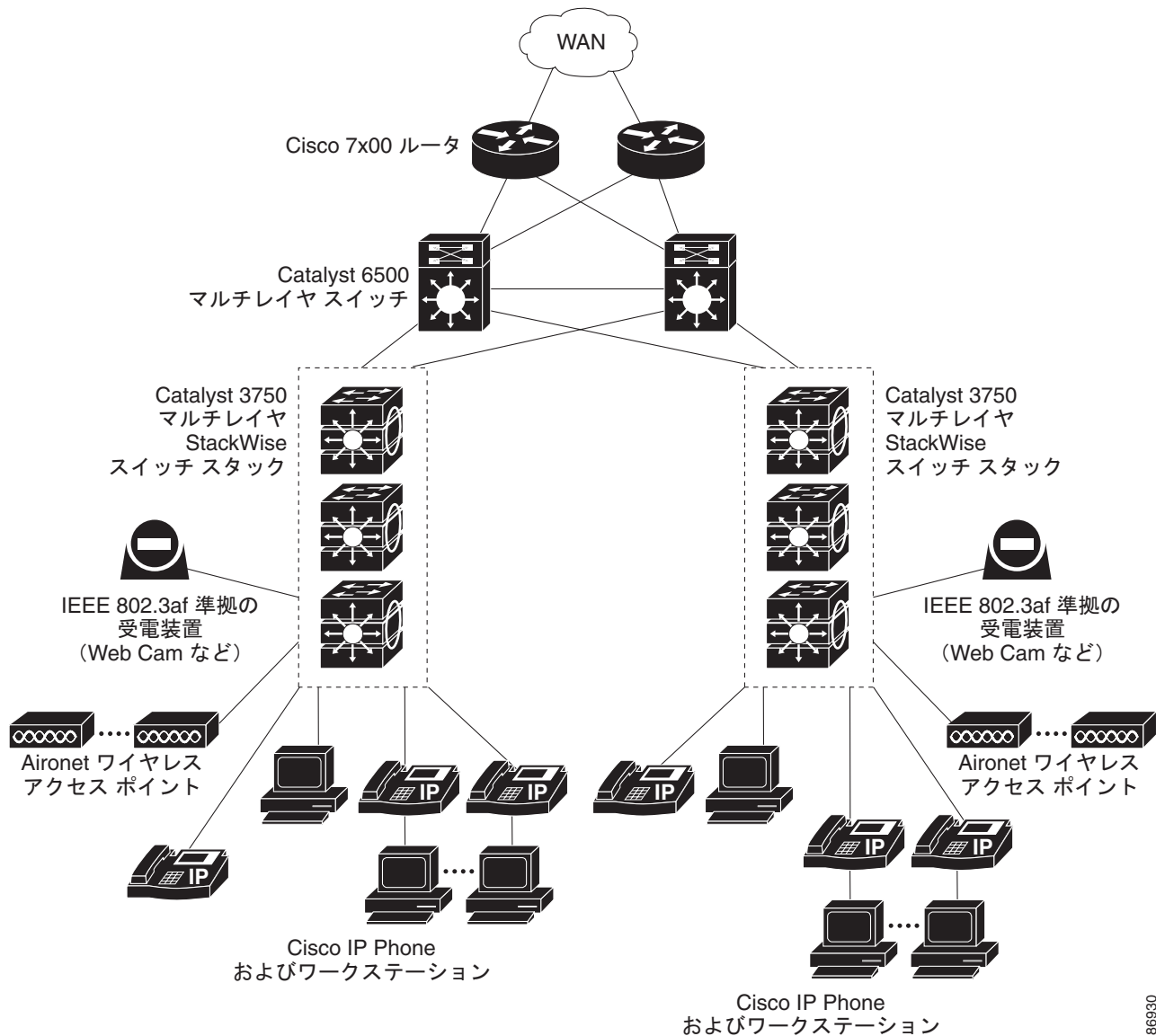
ワイヤリング クローゼット内のスイッチは、これまでレイヤ 2 専用デバイスでしたが、ネットワークトラフィック プロファイルの改善に伴い、マルチキャスト管理やトラフィック分類などのマルチレイヤ サービスを採用するようになってきました。図 1-7 に、ワイヤリング クローゼットに Catalyst 3750 マルチレイヤ スイッチ スタックと、最大 10 のワイヤリング クローゼットを集約する 2 台のバックボーン スイッチ (Catalyst 6500 スイッチなど) だけを使用するネットワークの構成を示します。

ワイヤリング クローゼットの各スタックは、IGMP スヌーピングがイネーブルになっていて、効率的にマルチメディアおよびマルチキャスト トラフィックを伝送します。帯域幅制限に基づいて不適合トラフィックを廃棄またはマークする QoS ACL も、各スタック上で設定されます。VLAN マップは VLAN 内セキュリティを提供し、不正ユーザがネットワークの重要な部分にアクセスしないようにします。QoS 機能は、ポート単位またはユーザ単位で帯域幅を制限します。スイッチ ポートは `trusted` または `untrusted` で設定します。CoS 値、DSCP 値、または IP precedence を信頼するように `trusted` ポートを設定できます。`untrusted` でポートを設定した場合は、ACL を使用し、ネットワーク ポリシーに従ってフレームをマークできます。

各スタックは、VLAN 間ルーティングを提供します。これらは、プロキシ ARP サービスを提供して IP および MAC アドレスのマッピングを取得するので、ルータからこのタスクを取り除き、WAN リンクでのこのタイプのトラフィックを削減します。また、これらのスタックは各アップリンク ポートを `trusted` ルーテッド アップリンクに設定し、アップリンク障害が生じた場合は高速コンバージェンスを行うように設定して、バックボーン スイッチに対して冗長アップリンク接続を行います。

ルータおよびバックボーン スイッチでは、HSRP をイネーブルにして、ロード バランシングおよび冗長接続を実行可能にして、ミッションクリティカルなトラフィックを保証します。

図 1-7 バックボーン設定のワイヤリング クローゼットのスイッチ



86930

Catalyst 3750 スイッチによる集合住宅ネットワーク

住宅地域および商業地域で、イーサネット Metropolitan-Area Networking (MAN; メトロポリタンエリアネットワーク) への高速アクセスを必要とするユーザが増加しています。図 1-8 に、Mini-Point-of-Presence (Mini-POP) においてマルチレイヤ スイッチ スタックを集約スイッチとして使用したギガビットイーサネット MAN リング構成を示します。これらのスイッチは、1000BASE-X SFP モジュールポート経由で接続しています。

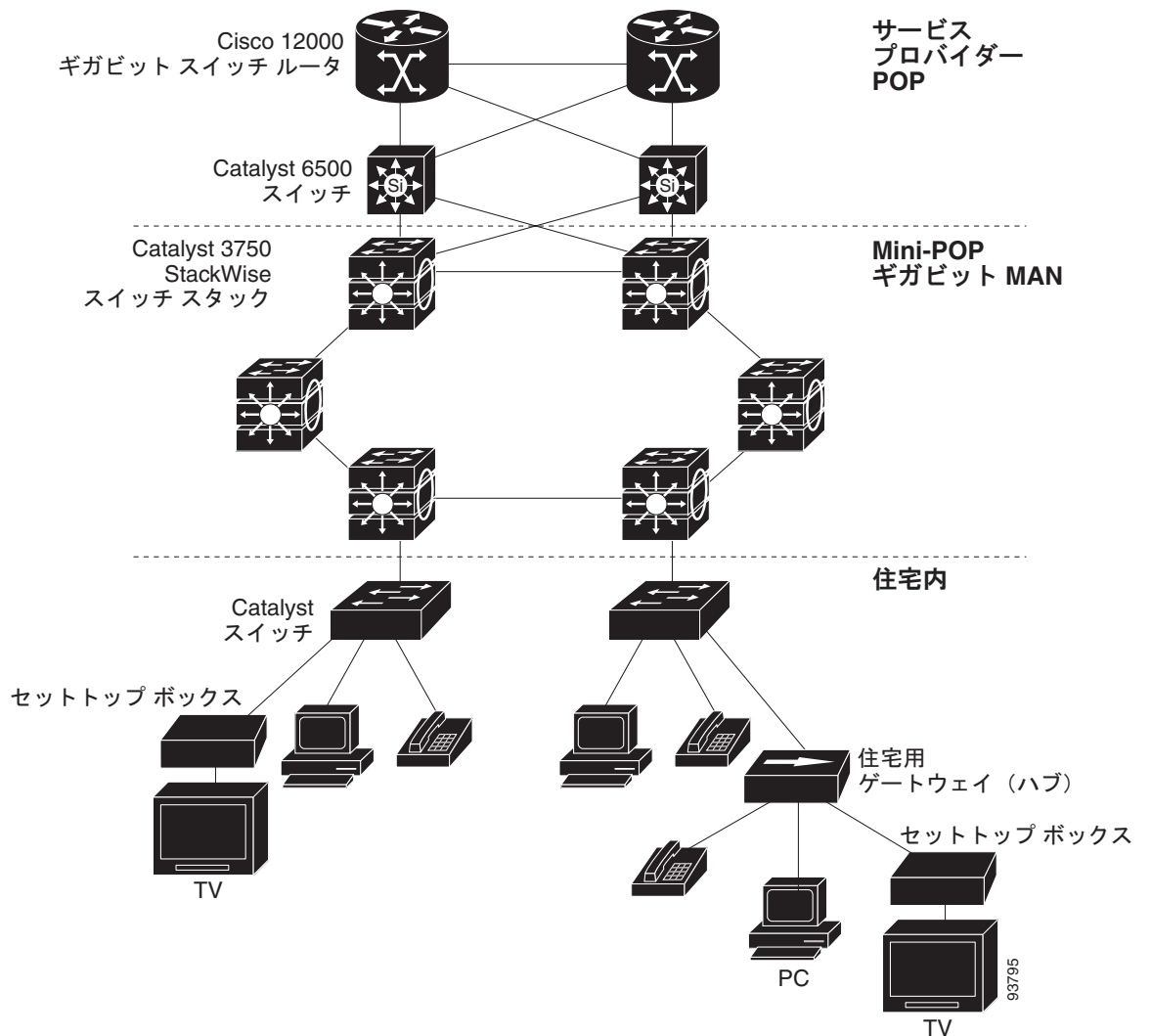
住宅用スイッチとして Catalyst 3750 スイッチを使用し、ユーザが MAN に高速接続できるようにします。既存の電話回線による接続が必要なユーザの場合は、住宅用スイッチとして Catalyst 2900 LRE XL または Catalyst 2950 LRE スイッチを使用できます。Catalyst 2900 LRE XL および Catalyst 2950

LRE スイッチは、別の住宅用スイッチまたは Catalyst 3750 集約スイッチに接続できます。Catalyst Long-Reach Ethernet (LRE) スイッチの詳細については、これらのスイッチのマニュアルを参照してください。

住宅用 Catalyst 3750 スイッチ（および使用されている場合、Catalyst 2950 LRE スイッチ）上のすべてのポートは、保護ポートおよび STP ルートガード機能がイネーブルに設定された IEEE 802.1Q トランクとして設定されています。保護ポート機能はスイッチ上の各ポートを孤立させることで、加入者が他の加入者宛パケットを見ることができないようにして、セキュリティを確保します。STP ルートガードは、許可されていないデバイスが STP ルートスイッチとして使用されるのを防止します。マルチキャストトラフィックを管理するために、すべてのポートで IGMP スヌーピングまたは CGMP がイネーブルに設定されています。Catalyst 3750 マルチレイヤ集約スイッチへのアップリンクポート上の ACL が、セキュリティと帯域幅の管理を行います。

集約スイッチおよびルータは、前出の例「Catalyst 3750 スイッチを使用した中小規模のネットワーク」(P.1-26) および「Catalyst 3750 スイッチによる大規模ネットワーク」(P.1-27) に記載されているようなサービスを提供します。

図 1-8 MAN 構成の Catalyst 3750 スイッチ



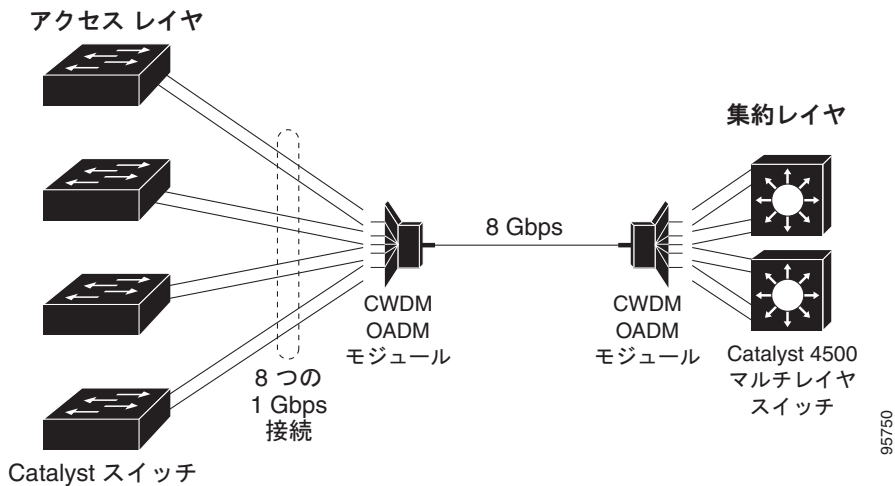
長距離広帯域トランスポートの構成

図 1-9 に、8 Gbps のデータを 1 本の光ファイバ ケーブルで伝送する構成を示します。Catalyst 3750 スイッチには、Coarse Wavelength-Division Multiplexer (CWDM) 光ファイバ SFP モジュールが搭載されています。CWDM SFP モジュールに応じて、データは 1470 ~ 1610 nm の波長で送信されます。波長が高くなるほど、伝送できる距離が長くなります。長距離伝送用に使われる一般的な波長は 1550 nm です。

CWDM SFP モジュールは、最大 393,701 フィート (74.5 マイルまたは 120 km) の距離で、CWDM Optical Add/Drop Multiplexer (OADM; 光分岐挿入) モジュールに接続します。CWDM OADM モジュールは、さまざまな CWDM 波長を結合 (多重化) して、同じ光ファイバ ケーブル上で同時に伝送できるようにします。受信側エンドの CWDM OADM モジュールは、さまざまな波長を分離 (逆多重化) します。

CWDM SFP モジュールおよび CWDM OADM モジュールの詳細については、『Cisco CWDM GBIC and CWDM SFP Installation Note』を参照してください。

図 1-9 長距離広帯域トランスポートの構成



次の作業

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

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



CHAPTER 2

CLI の使用方法

この章では Catalyst 3750 スイッチを設定するための Cisco IOS CLI (コマンドライン インターフェイス) とその使用方法について説明します。内容は次のとおりです。

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

コマンド モードの概要

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

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

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

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

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

表 2-1 コマンドモードの概要

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

表 2-1 コマンドモードの概要 (続き)

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、 interface コマンドを入力し、イ ンターフェイスを指 定します。	Switch(config-if)#	終了してグローバル コンフィギュレー ションモードに戻 るには、 exit を入力 します。 特権 EXEC モード に戻るには、 Ctrl-Z を押すか、 end を入 力します。	このモードを使用して、イー サネット ポートのパラメータ を設定します。 インターフェイスの定義につ いては、「 インターフェイス コ ンフィギュレーション モード の使用法 」(P.12-12) を参 照してください。 同じパラメータを指定して複 数のインターフェイスを設定 する場合は、「 インターフェイ ス範囲の設定 」(P.12-14) を 参照してください。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、 linevty また は line console コマ ンドを使用して回線 を指定します。	Switch(config-line)#	終了してグローバル コンフィギュレー ションモードに戻 るには、 exit を入力 します。 特権 EXEC モード に戻るには、 Ctrl-Z を押すか、 end を入 力します。	このモードを使用して、端末 回線のパラメータを設定しま す。

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

ヘルプシステムの概要

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

表 2-2 ヘルプの概要

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

表 2-2 ヘルプの概要 (続き)

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

コマンドの省略形

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

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

```
Switch# show conf
```

コマンドの no 形式および default 形式の概要

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

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

CLI のエラー メッセージ

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

表 2-3 CLI の代表的なエラー メッセージ

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

コンフィギュレーション ロギングの使用法

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

詳細については、次の URL にアクセスし、『*Configuration Change Notification and Logging*』のモジュール機能を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1e81.html



(注)

CLI または HTTP の変更だけがログとして記録されます。

コマンド履歴の使用方法

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

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

コマンド履歴バッファ サイズの変更

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

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

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

指定できる範囲は 0 ~ 256 です。

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

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

指定できる範囲は 0 ~ 256 です。

コマンドの呼び出し

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

表 2-4 コマンドの呼び出し

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

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

コマンド履歴機能のディセーブル化

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

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

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

編集機能の使用法

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

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

編集機能のイネーブル化およびディセーブル化

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

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

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

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

```
Switch# terminal editing
```

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

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

キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集 (続き)

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

表 2-5 キーストロークによるコマンドの編集 (続き)

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

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

画面幅よりも長いコマンドラインの編集

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

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

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

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

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

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

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

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

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

show および more コマンド出力の検索およびフィルタリング

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

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

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

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

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

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

CLI のアクセス

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

スタック マスターを使用して、スイッチ スタックとスタック メンバー インターフェイスを管理します。個々のスイッチごとにはスタック メンバーを管理できません。1 つまたは複数のスタック メンバーのコンソール ポートを経由してスタック マスターへ接続できます。スタック マスターに対して複数の CLI セッションを使用する場合には十分に注意してください。あるセッションで入力したコマンドは、他のセッションでは表示されません。そのため、入力したコマンド以降のセッションをトラッキングできなくなる場合があります。



(注) スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバー ポートを設定する場合は、CLI コマンドのインターフェイス指定部分にスタック メンバー番号を指定する必要があります。インターフェイスの指定方法の詳細については、「[インターフェイス コンフィギュレーション モードの使用法](#)」(P.12-12) を参照してください。

特定のスタック メンバーをデバッグするために、`session stack-member-number` 特権 EXEC コマンドを使用して、スタック マスターからスタック メンバーへアクセスできます。スタック メンバー番号は、システム プロンプトに付加されます。たとえば、`Switch-2#` はスタック メンバー 2 の特権 EXEC モードのプロンプトです。`Switch` は、スタック マスターのシステム プロンプトです。特定のスタック メンバーへの CLI セッションでは、`show` コマンドと `debug` コマンドだけを使用できます。

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチの『Getting Started Guide』に記載されている手順で、スイッチのコンソールポートに端末または PC を接続し、スイッチの電源をオンにする必要があります。また、起動プロセスおよび IP 情報を指定する場合に使用できるオプションについて理解するため、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。詳細については、「端末回線に対する Telnet パスワードの設定」(P.9-6)を参照してください。

次のいずれかの方法で、スイッチとの接続を確立できます。

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

Telnet アクセスのためのスイッチ設定については、「端末回線に対する Telnet パスワードの設定」(P.9-6)を参照してください。スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

SSH のためのスイッチ設定については、「SSH のためのスイッチの設定」(P.9-46)を参照してください。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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



CHAPTER 3

スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て

この章では、自動および手動の各方法で、Catalyst 3750 スwitchの初期設定（たとえば、スイッチ IP アドレスの割り当てやデフォルトのゲートウェイ情報）を作成する方法について説明します。スイッチのスタートアップ コンフィギュレーションを変更する方法についても説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スwitchおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「起動プロセスの概要」(P.3-2)
- 「スイッチ情報の割り当て」(P.3-3)
- 「実行コンフィギュレーションの確認および保存」(P.3-17)
- 「スタートアップ コンフィギュレーションの変更」(P.3-18)
- 「ソフトウェア イメージ リロードのスケジュール設定」(P.3-22)



(注)

IP アドレスおよび Dynamic Host Configuration Protocol (DHCP) の設定に関するこの章の情報は、IP バージョン 4 (IPv4) 固有の情報です。スイッチ上で IP バージョン 6 (IPv6) の転送をイネーブルにする場合は、第 39 章「IPv6 ユニキャストルーティングの設定」で、IPv6 アドレスのフォーマットおよび設定に固有の情報を参照してください。IPv6 機能をイネーブルにするには、スタック スwitchは拡張 IP サービス イメージを実行している必要があります。

起動プロセスの概要

スイッチを起動するには、『*Getting Started Guide*』または『*Hardware Installation Guide*』の手順に従って、スイッチを設置して電源をオンにし、スイッチの初期設定（IP アドレス、サブネットマスク、デフォルト ゲートウェイ、シークレットおよび Telnet パスワードなど）を行う必要があります。

通常の起動プロセスにはブートローダ ソフトウェアの動作が含まれます。ブート ローダは次のアクティビティを実行します。

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

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

また、OS が使用不可能になるほどの重大な障害が発生した場合は、ブート ローダはシステムにトラップドアからアクセスします。トラップドアからシステムへアクセスして、必要があれば、フラッシュ ファイル システムをフォーマットし、XMODEM プロトコルを使用して OS のソフトウェア イメージを再インストールし、失われたパスワードを回復し、最終的に OS を再起動できます。詳細については、「ソフトウェアで障害が発生した場合の回復」(P.49-2) および「パスワードを忘れた場合の回復」(P.49-3) を参照してください。



(注)

パスワードの回復をディセーブルにできます。詳細については、「パスワード回復のディセーブル化」(P.9-5) を参照してください。

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

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



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

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

スイッチ情報の割り当て

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

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

スイッチ スタックは単一の IP アドレスを使用して管理されます。IP アドレスは、システム レベルの設定値で、スタック マスターや他のスタック メンバー固有の設定ではありません。スタックからスタック マスターや他のスタック メンバーを削除しても、IP 接続は存続していれば、引き続き同じ IP アドレスを使用してスタックを管理できます。



(注) スイッチ スタックからスタック メンバーを削除した場合、各スタック メンバーは自身の IP アドレスを保持します。したがって、ネットワーク内で同じ IP アドレスを持つ 2 つのデバイスが競合するのを避けるため、スイッチ スタックから削除したスイッチの IP アドレスを変更しておきます。

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



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

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

ここでは、次の設定情報について説明します。

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

デフォルトのスイッチ情報

表 3-1 に、デフォルトのスイッチ情報を示します。

表 3-1 デフォルトのスイッチ情報

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

DHCP ベースの自動設定の概要

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

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

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



(注)

スイッチ スタックと DHCP、DNS、TFTP サーバの間では冗長接続を確立することを推奨します。接続されているスタック メンバーがスイッチ スタックから削除された場合でも、これらのサーバがアクセス可能なまま維持されるように保証する上で役立ちます。

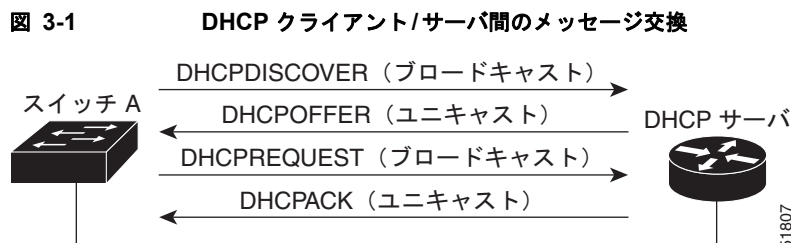
スイッチの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが異なる LAN 上で動作している場合、スイッチと DHCP サーバ間に、DHCP のリレー デバイスを設定する必要があります。リレー デバイスは、直接接続されている 2つの LAN 間でブロードキャスト トラフィックを転送します。ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

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

DHCP クライアントの要求プロセス

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

図 3-1 に、DHCP クライアントと DHCP サーバ間で交換される一連のメッセージを示します。



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

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

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバインドされ、クライアントはサーバから受信した設定情報を使用します。スイッチの受信する情報量は、DHCP サーバの設定方法によって異なります。詳細については、「[TFTP サーバの設定](#)」(P.3-8)を参照してください。

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

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

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

DHCP ホスト名オプションによって、スイッチのグループは一元管理 DHCP サーバからホスト名と標準設定を入手します。クライアント (スイッチ) は、DHCPDISCOVER メッセージに、DHCP サーバからホスト名とその他の設定パラメータを要求するために使用されるオプション 12 フィールドを含めます。すべてのクライアントの設定ファイルは、DHCP 入手ホスト名を除いて同一です。

クライアントにデフォルトのホスト名がある (`hostname name` グローバル コンフィギュレーション コマンドが設定されていない、または `no hostname` グローバル コンフィギュレーション コマンドが入力されてホスト名が削除されている) 場合、`ip address dhcp` インターフェイス コンフィギュレーション コマンドが入力されたときはパケットに DHCP ホスト名オプションが含まれません。この場合、クライアントがインターフェイスの IP アドレス取得中に DHCP ホスト名オプションを DHCP 相互作用から受信すると、クライアントは DHCP ホスト名オプションを受け取り、システムが現在ホスト名を設定していることを示すフラグを設定します。

DHCP ベースの自動設定およびイメージ アップデートの概要

DHCP サーバの設定に DHCP イメージ アップグレード機能を使用すると、ネットワーク内の複数のスイッチに新しいイメージファイルと新しいコンフィギュレーション ファイルの両方をダウンロードできます。この機能は、ネットワークに追加された複数の新しいスイッチにそれぞれ同じイメージと設定を受信させるのに効果的です。

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

DHCP 自動設定

DHCP 自動設定は、DHCP サーバからネットワーク内の複数のスイッチにコンフィギュレーション ファイルをダウンロードします。ダウンロードされたコンフィギュレーション ファイルはそのスイッチの実行コンフィギュレーション ファイルになります。フラッシュに保存されているブートアップ コンフィギュレーション ファイルは上書きされません。スイッチをリロードすることで上書きされます。

DHCP 自動イメージ アップデート

DHCP 自動設定の DHCP 自動イメージ アップグレードは、ネットワーク内の複数のスイッチに新しいイメージ ファイルと新しいコンフィギュレーション ファイルの両方をダウンロードします。新しいコンフィギュレーション ファイルとイメージ ファイルをダウンロードするスイッチには設定は必要ありません（または、工場出荷時のデフォルト設定だけが行われています）。

新しいコンフィギュレーション ファイルがすでに設定されているスイッチにダウンロードされた場合、ダウンロードされた設定はスイッチに保存されているコンフィギュレーション ファイルに追加されず（既存の設定はダウンロードされたファイルに上書きされません）。



(注)

スイッチで DHCP 自動イメージ アップデートをイネーブルにする場合、イメージとコンフィギュレーション ファイルが保存されている TFTP サーバのオプション 67（コンフィギュレーション ファイル名）とオプション 66（DHCP サーバ ホスト名）、オプション 150（TFTP サーバ アドレス）、オプション 125（ファイルの説明）を正確に設定する必要があります。

スイッチを DHCP サーバとして設定する場合の手順については、「[DHCP ベースの自動設定の設定 \(P.3-7\)](#)」および『[Cisco IOS IP Configuration Guide](#)』Release 12.2 の「IP Addressing and Services」セクションにある「[Configuring DHCP](#)」セクションを参照してください。

ネットワークにスイッチをインストールすると、自動イメージ アップデート機能が開始します。ダウンロードされたコンフィギュレーション ファイルはスイッチの実行コンフィギュレーション ファイルに保存され、次に新しいイメージのダウンロードとインストールが始まります。スイッチをリブートすると、そのコンフィギュレーション ファイルはスイッチに保存されます。

制限事項

次のような制限事項があります。

- ネットワーク内に IP アドレスが割り当てられてないアップ ステートのレイヤ 3 インターフェイスが最低 1 つ必要です。これがない場合、DHCP ベースの自動設定による保存設定プロセスは停止します。
- タイムアウトが設定されていない場合、DHCP ベースの自動設定による保存設定機能は IP アドレスを無制限にダウンロードしようとします。
- コンフィギュレーション ファイルをダウンロードすることができない、またはコンフィギュレーション ファイルが壊れている場合、自動インストール プロセスは停止します。



(注)

TFTP からダウンロードされたコンフィギュレーション ファイルは実行コンフィギュレーション ファイルの既存設定とマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを実行しないかぎり、NVRAM には保存されません。ダウンロードされた設定がスタートアップ コンフィギュレーション ファイルに保存されても、次のシステム再起動中には反映されないのに注意してください。

DHCP ベースの自動設定の設定

ここでは、次の設定情報について説明します。

- 「DHCP サーバ設定時の注意事項」 (P.3-7)
- 「TFTP サーバの設定」 (P.3-8)
- 「DNS の設定」 (P.3-9)
- 「リレー デバイスの設定」 (P.3-9)
- 「コンフィギュレーション ファイルの入手方法」 (P.3-10)
- 「構成例」 (P.3-11)

DHCP サーバ設定時の注意事項

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

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

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

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

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

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

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

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

スイッチは DHCP サーバとして機能します。デフォルトでは、Cisco IOS DHCP サーバおよびリレー エージェント機能はスイッチ上でイネーブルですが、設定されていません。これらの機能は動作しません。DHCP サーバがシスコ製の装置の場合、DHCP の設定の詳細については、『Cisco IOS IP Configuration Guide』の「IP Addressing and Services」セクションにある「Configuring DHCP」セクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

DHCP サーバとスイッチ スタック

データベースをバインドする DHCP は、スタック マスターで管理されます。新しいスタック マスターが割り当てられる場合は、新しいマスターは保存されているバインド データベースを TFTP サーバからダウンロードします。スタック マスターに障害が生じると、保存されていないバインド データベースは失われます。失われたバインドに関連する IP アドレスは、解除されます。`ip dhcp database url [timeout seconds | write-delay seconds]` グローバル コンフィギュレーション コマンドを使用して、自動バックアップを設定する必要があります。

スタック マージが発生すると、スタック メンバーとなるスタック マスターは、すべての DHCP リースのバインドを失います。スタックを分割すると、分割された新しいマスターは、既存の DHCP リースのバインドではなく、新しい DHCP サーバの動作をします。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

TFTP サーバの設定

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

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

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

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

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

使用する TFTP サーバが、スイッチとは異なる LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用してアクセスした場合 (前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生) は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。詳細については、「リレー デバイスの設定」(P.3-9) を参照してください。適切な解決方法は、必要なすべての情報を使用して DHCP サーバを設定することです。

DNS の設定

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

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

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

リレー デバイスの設定

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

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

図 3-2 では、ルータ インターフェイスを次のように設定しています。

インターフェイス 10.0.0.2 では、

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

インターフェイス 20.0.0.1 では、

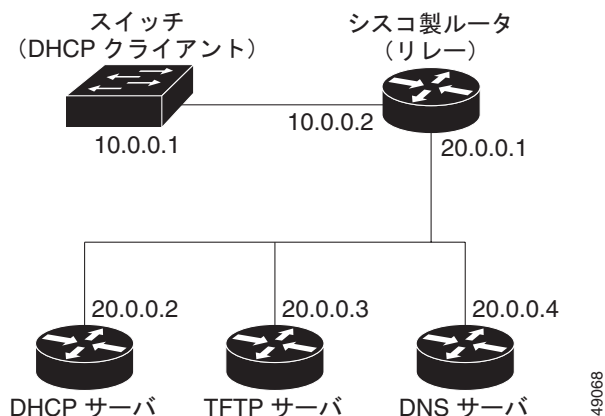
```
router(config-if)# ip helper-address 10.0.0.1
```



(注)

スイッチをリレー デバイスとして機能させる場合は、インターフェイスをルーテッド ポートに設定してください。詳細については、「ルーテッド ポート」(P.12-5) および「レイヤ 3 インターフェイスの設定」(P.12-28) を参照してください。

図 3-2 自動設定でのリレー デバイスの使用



コンフィギュレーション ファイルの入手方法

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

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

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

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

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

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

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

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

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

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



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

構成例

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

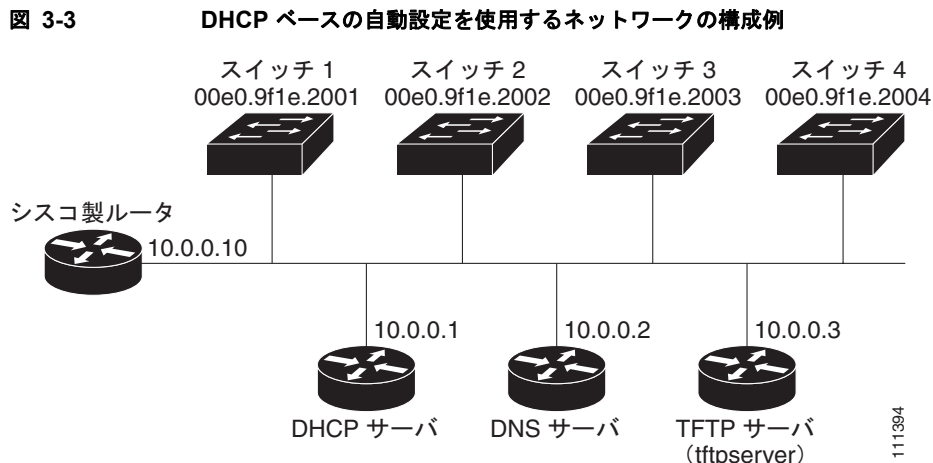


表 3-2 は、DHCP サーバ上の予約リースの設定例です。

表 3-2 DHCP サーバ コンフィギュレーション

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

DNS サーバ コンフィギュレーション

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

TFTP サーバ コンフィギュレーション (UNIX)

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

```
prompt> cd /tftpserver/work/
prompt> ls
network-config
switcha-config
```

```

switchb-config
switchc-config
switchd-config
prompt> cat network-config
ip host switcha 10.0.0.21
ip host switchb 10.0.0.22
ip host switchc 10.0.0.23
ip host switchd 10.0.0.24

```

DHCP クライアント コンフィギュレーション

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

コンフィギュレーションの説明

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

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

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

DHCP の自動設定およびイメージ アップデート機能の設定

DHCP を使用して新しいイメージや設定をスイッチにダウンロードするには、最低 2 つのスイッチが必要です (DHCP サーバ用および TFTP サーバ用)。クライアントのスイッチは、新しいコンフィギュレーション ファイルか、または新しいコンフィギュレーション ファイルと新しいイメージ ファイルをダウンロードするように設定します。

DHCP 自動設定の設定 (コンフィギュレーション ファイルのみ)

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dhcp poolname</code>	DHCP サーバのアドレス プール名を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 3	<code>bootfile filename</code>	ブート イメージとして使用するコンフィギュレーション ファイル名を指定します。
ステップ 4	<code>network network-number mask prefix-length</code>	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。 (注) プレフィクス長は、アドレス プレフィクスからなるビット数で指定します。クライアントのネットワーク マスクを指定する代わりにプレフィクスを使用できます。プレフィクス長はフォワード スラッシュ (/) の前に入力してください。

	コマンド	目的
ステップ 5	default-router <i>address</i>	DHCP クライアントにおけるデフォルト ルータの IP アドレスを指定します。
ステップ 6	option 150 <i>address</i>	TFTP サーバの IP アドレスを指定します。
ステップ 7	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	tftp-server flash: <i>filename.text</i>	TFTP サーバのコンフィギュレーション ファイルを指定します。
ステップ 9	interface <i>interface-id</i>	コンフィギュレーション ファイルを受信するクライアント アドレスを指定します。
ステップ 10	no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 11	ip address <i>address mask</i>	インターフェイスの IP アドレスとマスクを指定します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例で、スイッチを DHCP サーバとして設定してコンフィギュレーション ファイルをダウンロードする方法を示します。

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

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

TFTP および DHCP の DHCP 自動設定で新しいイメージおよび新しいコンフィギュレーション ファイルを新しいスイッチにダウンロードするには、特権 EXEC モードで次の手順を実行します。



(注) 表の手順に従う前に、スイッチにアップロードするテキスト ファイルを作成しておく必要があります (例: `autoinstall_dhcp`)。テキスト ファイルにダウンロードするイメージの名前を入力します。イメージは `bin` ではなく `tar` ファイルにする必要があります。

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

■ スイッチ情報の割り当て

	コマンド	目的
ステップ 4	network <i>network-number mask prefix-length</i>	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。 (注) プレフィクス長は、アドレスプレフィクスからなるビット数で指定します。クライアントのネットワーク マスクを指定する代わりにプレフィクスを使用できます。プレフィクス長はフォワードスラッシュ (/) の前に入力してください。
ステップ 5	default-router <i>address</i>	DHCP クライアントにおけるデフォルトルータの IP アドレスを指定します。
ステップ 6	option 150 <i>address</i>	TFTP サーバの IP アドレスを指定します。
ステップ 7	option 125 <i>hex</i>	イメージファイルへのパスが記述されているテキスト ファイルのパスを指定します。
ステップ 8	copy tftp flash <i>filename.txt</i>	スイッチにテキスト ファイルをアップロードします。
ステップ 9	copy tftp flash <i>imagename.tar</i>	スイッチに新しいイメージの tar ファイルをアップロードします。
ステップ 10	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	tftp-server flash: <i>config.text</i>	TFTP サーバの Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	tftp-server flash: <i>imagename.tar</i>	TFTP サーバのイメージ名を指定します。
ステップ 13	tftp-server flash: <i>filename.txt</i>	ダウンロードするイメージファイル名が記述されたテキスト ファイルを指定します。
ステップ 14	interface <i>interface-id</i>	コンフィギュレーション ファイルを受信するクライアントアドレスを指定します。
ステップ 15	no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 16	ip address <i>address mask</i>	インターフェイスの IP アドレスとマスクを指定します。
ステップ 17	end	特権 EXEC モードに戻ります。
ステップ 18	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例で、スイッチを DHCP サーバとして設定してコンフィギュレーション ファイルをダウンロードする方法を示します。

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c3750-ipservices-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash:autoinstall_dhcp
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

クライアントの設定

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

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

次の例で、VLAN 99 のレイヤ 3 SVI インターフェイスを使用して DHCP ベースの自動設定（保存した設定による）をイネーブルにする方法を示します。

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



(注) レイヤ 3 インターフェイスだけを設定し、イネーブルにします。IP アドレスまたは保存した設定による DHCP ベースの自動設定は割り当てないでください。

手動でのスイッチ情報の割り当て

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



(注)

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

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

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

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

実行コンフィギュレーションの確認および保存

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

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

Current configuration: 1363 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxEO
!
.
<output truncated>
.
interface gigabitethernet6/0/1
no switchport
ip address 172.20.137.50 255.255.255.0
!
interface gigabitethernet6/0/2
mvr type source

<output truncated>

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

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

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

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

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

スタートアップコンフィギュレーションの変更

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

- 「起動のデフォルト設定」(P.3-18)
- 「コンフィギュレーションファイルの自動ダウンロード」(P.3-18)
- 「手動で起動する場合」(P.3-19)
- 「特定のソフトウェアイメージを起動する場合」(P.3-20)
- 「環境変数の制御」(P.3-21)

スイッチ スタックのコンフィギュレーションファイルについては、「スタックのコンフィギュレーションファイル」(P.5-14) および付録 C 「Cisco IOS ファイル システム、コンフィギュレーションファイル、およびソフトウェアイメージの操作」を参照してください。

起動のデフォルト設定

表 3-3 に、起動のデフォルト設定を示します。

表 3-3 起動のデフォルト設定

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

コンフィギュレーション ファイルの自動ダウンロード

DHCP ベースの自動設定機能を使用することによって、スイッチにコンフィギュレーション ファイルを自動的にダウンロードできます。詳細については、「DHCP ベースの自動設定の概要」(P.3-4) を参照してください。

システム コンフィギュレーションを読み書きするためのファイル名の指定

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



(注) このコマンドは、スタンドアロン スイッチから使用した場合にだけ正常に動作します。

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

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

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

手動で起動する場合

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



(注) このコマンドは、スタンドアロン スイッチから使用した場合にだけ正常に動作します。

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

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

コマンド	目的
ステップ 4 show boot	<p>設定を確認します。</p> <p>boot manual グローバル コンフィギュレーション コマンドによって、MANUAL_BOOT 環境変数の設定が変更されます。</p> <p>次回、システムを再起動したときには、スイッチはブート ロード モードになり、ブート ロード モードであることが switch: プロンプトによって示されます。システムを起動するには、boot filesystem:/file-url ブート ロード コマンドを使用します。</p> <ul style="list-style-type: none"> • filesystem: に、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。 • file-url には、パス (ディレクトリ) および起動可能なイメージの名前を指定します。 <p>ファイル名およびディレクトリ名は、大文字と小文字が区別されません。</p>
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

特定のソフトウェア イメージを起動する場合

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

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

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 boot system filesystem:/file-url	<p>次回の起動時に、フラッシュ メモリ内の特定のイメージを起動するようにスイッチを設定します。</p> <ul style="list-style-type: none"> • filesystem: に、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。 • file-url には、パス (ディレクトリ) および起動可能なイメージの名前を指定します。 <p>このコマンドをスタック マスターで入力した場合、次の起動時に指定したソフトウェア イメージがスタック マスターにのみロードされます。</p> <p>ファイル名およびディレクトリ名は、大文字と小文字が区別されます。</p>
ステップ 3 boot system switch {number all}	<p>(任意) 次の起動時にシステム イメージがロードされるスイッチ メンバーを指定します。</p> <ul style="list-style-type: none"> • スタック メンバーを指定するには number を使用します。 • すべてのスタック メンバーを指定するには all を使用します。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show boot	設定を確認します。 boot system グローバル コンフィギュレーション コマンドによって、BOOT 環境変数の設定が変更されます。 次回の起動時に、スイッチは BOOT 環境変数の情報を使用して、システムを自動的に起動しようとします。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

環境変数の制御

正常に動作しているスイッチでは、9600 bps 対応に設定されたスイッチ コンソール接続でのみブートローダ モードが開始されます。スイッチの電源コードを外し、もう一度電源コードを接続したときに、スイッチの **Mode** ボタンを押します。ポート 1 の上の LED が消灯してから 1 ~ 2 秒後に、**Mode** ボタンを離します。ブートローダの *switch:* プロンプトが表示されます。

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

値を持つ環境変数は、フラッシュ ファイル システム以外のフラッシュ メモリに保存されます。

ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。このファイルに含まれていない変数には値がありません。ファイルに含まれている変数は、ヌル文字列も含めて値がありません。ヌル文字列 (“”) に設定された変数は、値を持つ変数です。多数の環境変数があらかじめ定義されていて、デフォルト値が与えられています。

環境変数には 2 種類のデータが保存されます。

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

環境変数の設定を変更するには、ブートローダにアクセスするか、Cisco IOS コマンドを使用します。通常、環境変数の設定変更は不要です。



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

表 3-4 で、代表的な環境変数の機能について説明します。

表 3-4 環境変数

変数	ブート ローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	<p>set BOOT <i>filesystem:/file-url ...</i></p> <p>自動起動時にロードして実行を試みる、セミコロンの区切られた実行可能ファイルのリスト。BOOT 環境変数が設定されていない場合、スイッチはフラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出した実行可能イメージをロードして実行しようとします。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。</p>	<p>boot system {<i>filesystem:/file-url ...</i> switch {<i>number</i> all}}</p> <p>次の起動時にロードする Cisco IOS イメージと、イメージがロードされるスタック メンバーを指定します。このコマンドによって、BOOT 環境変数の設定が変更されます。</p>
MANUAL_BOOT	<p>set MANUAL_BOOT yes</p> <p>スイッチの起動を自動で行うか手動で行うかを決定します。</p> <p>有効な値は 1、yes、0、および no です。no または 0 に設定されている場合、ブート ローダはシステムの自動起動を試みます。それ以外の値に設定されている場合は、ブート ローダ モードから手動でスイッチを起動しなければなりません。</p>	<p>boot manual</p> <p>次の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。</p> <p>次のシステム再起動時には、スイッチはブート ローダ モードになります。システムを起動するには、boot flash:filesystem:/file-url ブート ローダ コマンドを使用し、起動可能イメージの名前を指定します。</p>
CONFIG_FILE	<p>set CONFIG_FILE flash:/file-url</p> <p>Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。</p>	<p>boot config-file flash:/file-url</p> <p>Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。</p>
SWITCH_NUMBER	<p>set SWITCH_NUMBER <i>stack-member-number</i></p> <p>スタック メンバーのメンバー番号を変更します。</p>	<p>switch <i>current-stack-member-number</i> renumber <i>new-stack-member-number</i></p> <p>スタック メンバーのメンバー番号を変更します。</p>
SWITCH_PRIORITY	<p>set SWITCH_PRIORITY <i>stack-member-number</i></p> <p>スタック メンバーのプライオリティ値を変更します。</p>	<p>switch <i>stack-member-number</i> priority <i>priority-number</i></p> <p>スタック メンバーのプライオリティ値を変更します。</p>

ソフトウェア イメージ リロードのスケジュール設定

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



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

リロードのスケジュール設定

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

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

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

スイッチ スタック内の特定のスイッチをリロードするには、**reload slot stack-member-number** 特権 EXEC コマンドを使用します。

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

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



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

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

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

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

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

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

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

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

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

リロード スケジュール情報の表示

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

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



CHAPTER 4

Cisco IOS Configuration Engine の設定

この章では、Catalyst 3750 スイッチの機能を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

Cisco Configuration Engine の詳細な設定情報については、次を参照してください。

http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

この章で説明するコマンドの構文および使用法の詳細については、Cisco.com で次の URL にアクセスして『Cisco IOS Network Management Command Reference』 Release 12.4 を参照してください。

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

- 「Cisco Configuration Engine ソフトウェアの概要」 (P.4-1)
- 「Cisco IOS エージェントの概要」 (P.4-5)
- 「Cisco IOS エージェントの設定」 (P.4-6)
- 「CNS 設定の表示」 (P.4-14)

Cisco Configuration Engine ソフトウェアの概要

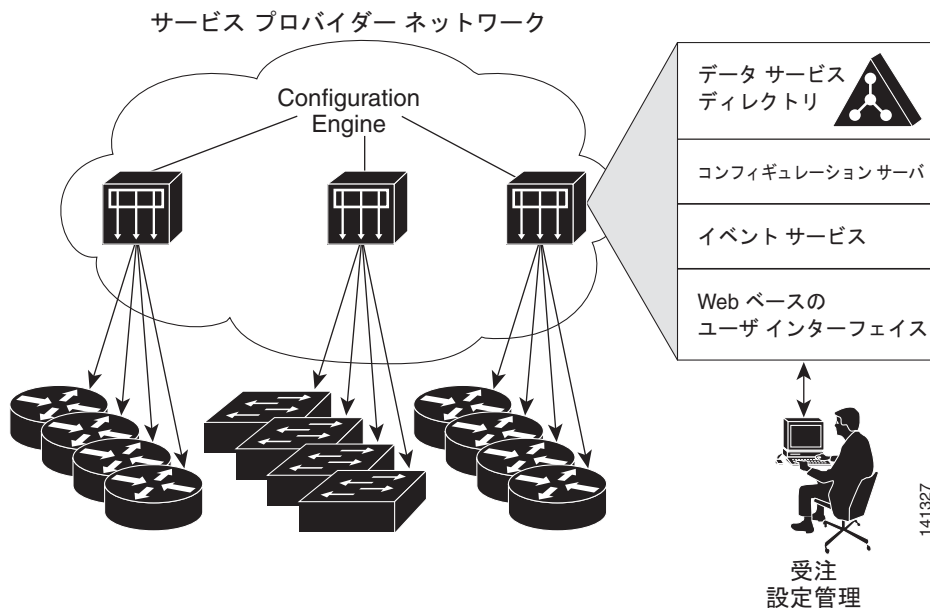
Cisco Configuration Engine は、ネットワーク管理ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します (図 4-1 を参照)。各 Configuration Engine は、シスコ デバイス (スイッチとルータ) のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Configuration Engine はデバイス固有の設定変更を生成してデバイスに送信し、設定変更を実行してその結果をロギングすることで、初期設定および設定の更新を自動化します。

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

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

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

図 4-1 Configuration Engine アーキテクチャの概要



- 「コンフィギュレーション サービス」(P.4-2)
- 「イベント サービス」(P.4-3)
- 「CNS ID およびデバイスのホスト名に関する重要事項」(P.4-3)

コンフィギュレーション サービス

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

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

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

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

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

イベント サービス

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

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

NSM

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

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

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

CNS ID およびデバイスのホスト名に関する重要事項

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

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

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

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

ConfigID

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

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

DeviceID

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

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

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

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

ホスト名および DeviceID

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

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

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



注意

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

ホスト名、DeviceID、ConfigID の使用方法

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

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

Configuration Engine で **Setup** を実行する場合、これらのアトリビュートおよび関連するアトリビュート (タグ値のペア) を設定します。



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

Cisco IOS エージェントの概要

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

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

初期設定

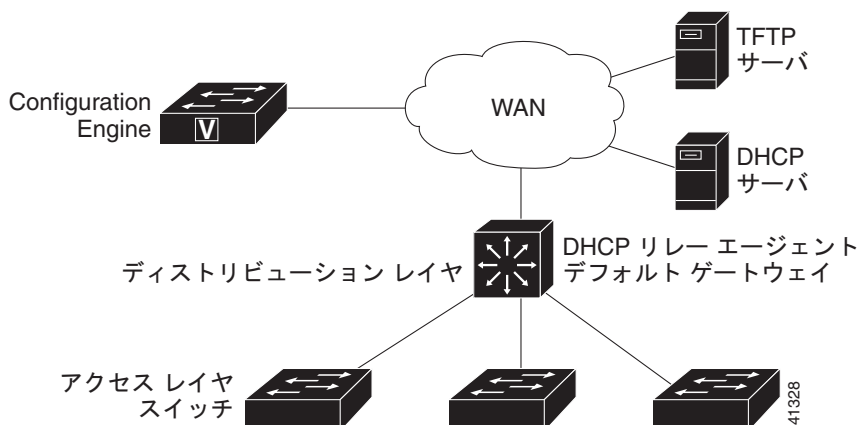
スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol (DHCP) 要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバの IP アドレス、ブートストラップ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

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

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

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

図 4-2 初期設定の概要



差分（部分）設定

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

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

同期設定

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

Cisco IOS エージェントの設定

スイッチの Cisco IOS ソフトウェアに組み込まれた Cisco IOS エージェントによって、スイッチを接続して自動的に設定できます（「[自動 CNS 設定のイネーブル化](#)」(P.4-7) を参照）。設定を変更する場合、またはカスタム コンフィギュレーションをインストールする場合は次の手順を参照してください。

- 「[CNS イベント エージェントのイネーブル化](#)」(P.4-8)
- 「[Cisco IOS CNS エージェントのイネーブル化](#)」(P.4-9)

自動 CNS 設定のイネーブル化

スイッチの自動 CNS 設定をイネーブルにするには、まず表 4-1 の条件を満たす必要があります。条件設定を完了したらスイッチの電源を入れます。**setup** プロンプトでは何も入力しません。スイッチは初期設定を開始します（「初期設定」(P.4-5) を参照）。コンフィギュレーションファイル全体がスイッチにロードされると作業は完了です。

表 4-1 自動設定イネーブル化の条件

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



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

CNS イベント エージェントのイネーブル化



(注)

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

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

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

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

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

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

Cisco IOS CNS エージェントのイネーブル化

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

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

初期設定のイネーブル化

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns template connect name	CNS テンプレート接続コンフィギュレーション モードを開始し、CNS 接続テンプレート名を指定します。
ステップ 3	cli config-text	CNS 接続テンプレートのコマンドラインを入力します。テンプレートのコマンドラインごとに、このステップを繰り返します。
ステップ 4		ステップ 2 ~ 3 を繰り返し、他の CNS 接続テンプレートを設定します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 6 cns connect <i>name</i> [retries <i>number</i>] [retry-interval <i>seconds</i>] [sleep <i>seconds</i>] [timeout <i>seconds</i>]	<p>CNS 接続コンフィギュレーション モードを開始し、CNS 接続プロファイル名を指定します。また、プロファイルのパラメータを定義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。</p> <ul style="list-style-type: none"> • CNS 接続プロファイル名を入力します。 • (任意) retries <i>number</i> に、接続の再試行回数を入力します。指定できる範囲は 1 ~ 30 です。デフォルトは 3 です。 • (任意) retry-interval <i>seconds</i> に、再試行時における Configuration Engine への接続間隔を入力します。指定できる範囲は 1 ~ 40 秒です。デフォルト値は 10 秒です。 • (任意) sleep <i>seconds</i> に、最初に接続を行う前の総時間を入力します。指定できる範囲は 0 ~ 250 秒です。デフォルトは 0 秒です。 • (任意) timeout <i>seconds</i> に、接続が終了したあとの総時間を入力します。指定できる範囲は 10 ~ 2000 秒です。デフォルトは 120 秒です。
ステップ 7 discover { controller <i>controller-type</i> dcli [subinterface <i>subinterface-number</i>] interface [<i>interface-type</i>] line <i>line-type</i> }	<p>CNS 接続プロファイルのインターフェイス パラメータを指定します。</p> <ul style="list-style-type: none"> • controller <i>controller-type</i> に、コントローラ タイプを入力します。 • dcli に、Active Data-Link Connection Identifiers (DLCI) を入力します。 (任意) subinterface <i>subinterface-number</i> に、アクティブ DLCI の検索に使用するポイントツーポイントのサブインターフェイス番号を指定します。 • interface [<i>interface-type</i>] に、インターフェイス タイプを入力します。 • line <i>line-type</i> に、ライン タイプを入力します。
ステップ 8 template <i>name</i> [... <i>name</i>]	<p>CNS 接続プロファイルの CNS 接続テンプレート リストを指定し、スイッチ設定に適用します。テンプレートは複数指定できます。</p>
ステップ 9	<p>ステップ 7 ~ 8 を繰り返し、CNS 接続プロファイルの他のインターフェイス パラメータと CNS 接続テンプレートを指定します。</p>
ステップ 10 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 11 hostname <i>name</i>	<p>スイッチのホスト名を入力します。</p>
ステップ 12 ip route <i>network-number</i>	<p>(任意) IP アドレスが <i>network-number</i> の Configuration Engine へのスタティック ルートを確立します。</p>

コマンド	目的
<p>ステップ 13 cns id <i>interface num</i> {dns-reverse ipaddress mac-address} [event] [image]</p> <p>または</p> <p>cns id {hardware-serial hostname string string udi} [event] [image]</p>	<p>(任意) Configuration Engine が使用する一意の EventID または ConfigID を設定します。</p> <ul style="list-style-type: none"> <i>interface num</i> に、インターフェイス タイプ (たとえば、イーサネット、Group-Async、Loopback、Virtual-Template) を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 {dns-reverse ipaddress mac-address} では、ホスト名を取得してそのホスト名を UID として割り当てるには dns-reverse を、IP アドレスを使用するには ipaddress を、MAC アドレスを一意の ID として使用するには mac-address を使用します。 (任意) ID をスイッチの識別に使用する event-id 値になるように設定するには、event を入力します。 (任意) ID をスイッチの識別に使用する image-id 値になるように設定するには、image を入力します。 <p>(注) event および image キーワードの両方を省略した場合、スイッチの特定に image-id 値が使用されます。</p> <ul style="list-style-type: none"> {hardware-serial hostname string string udi} では、hardware-serial に一意の ID として設定するスイッチのシリアル番号を、hostname に一意の ID として選択するスイッチのホスト名 (デフォルト) を、string string に一意の ID として任意のテキストストリングを、udi に一意の ID として設定する Unique Device Identifier (UDI) を入力します。

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

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

次の例で、スイッチ設定が不明の場合 (CNS Zero Touch 機能) におけるリモート スイッチの初期設定の設定方法を示します。

```

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

```

次の例で、スイッチの IP アドレスが判明している際のリモートスイッチの初期設定の設定方法を示します。Configuration Engine IP アドレスは 172.28.129.22 です。

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

部分設定のイネーブル化

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

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

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

CNS 設定の表示

表 4-2 特権 EXEC show コマンド

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



CHAPTER 5

スイッチ スタックの管理

この章では、Catalyst 3750 スイッチ スタックの管理に関する概念と手順について説明します。



(注)

コマンドの構文および使用方法については、スイッチ コマンド リファレンスを参照してください。

- 「スタックの概要」(P.5-1)
- 「スイッチ スタックの設定」(P.5-18)
- 「特定のスタック メンバーへの CLI アクセス」(P.5-23)
- 「スタック情報の表示」(P.5-23)
- 「スタックのトラブルシューティング」(P.5-24)

StackWise ポートを使用したスイッチの配線方法や LED を使用してスイッチ スタック ステータスを表示する方法など、スイッチ スタックに関するその他の情報については、『Hardware Installation Guide』を参照してください。

スタックの概要

スイッチ スタックは、StackWise ポートを介して接続された最大 9 台の Catalyst 3750 スイッチから構成されます。スイッチのうち 1 台がスタックの動作を制御し、このスイッチはスタック マスターといえます。スタック マスターとスタック内の他のスイッチが、スタック メンバーです。レイヤ 2 およびレイヤ 3 プロトコルは、ネットワークに対して、スイッチ スタック全体を単一のエンティティとして提供します。



(注)

スイッチ スタックは、スイッチ クラスタとは別物です。スイッチ クラスタは、10/100/1000 ポートなどのスイッチ自身の LAN ポートを使用して接続されたスイッチのセットです。スイッチ スタックとスイッチ クラスタの違いの詳細については、Cisco.com で入手できる『Getting Started with Cisco Network Assistant』の「Planning and Creating Clusters」の章を参照してください。

マスターは、スタック全体を管理するための単一拠点となります。マスターから、次のものを設定します。

- すべてのメンバーに適用されるシステム レベル (グローバル) の機能
- メンバーごとのインターフェイス レベルの機能

マスターが IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの暗号化 (暗号化をサポートする) バージョンを実行している場合は、暗号化機能を使用できます。

各メンバーは、専用のスタック メンバー番号によって一意に識別されます。

メンバーはすべて、マスターになる条件を満たしています。マスターが使用不能になると、残りのメンバーの中から新しいマスターが選択されます。そのファクタの 1 つが、スタック メンバー プライオリティ値です。最高のスタック メンバー プライオリティ値を持つスイッチが、マスターになります。

マスターでサポートされているシステム レベルの機能は、スタック全体でサポートされます。

IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの暗号化（暗号化をサポートする）バージョンを実行しているスイッチがスタックに存在する場合は、そのスイッチをスタック マスターにしてください。

マスターには、スタックの保存済みの実行コンフィギュレーション ファイルが格納されています。コンフィギュレーション ファイルには、スタックのシステム レベルの設定と、メンバーごとのインターフェイス レベルの設定が含まれます。各メンバーは、バックアップ目的で、これらのファイルの現在のコピーを保持します。

スタックは、単一の IP アドレスを使用して管理します。IP アドレスは、システム レベルの設定値で、マスターや他のメンバー固有の設定ではありません。スタックからマスターや他のメンバーを削除しても、同じ IP アドレスを使用してスタックを管理できます。

次の方法を使用して、スタックを管理できます。

- Network Assistant (Cisco.com から入手できます)
- すべてのメンバーのコンソール ポートへのシリアル接続を介した CLI (コマンドライン インターフェイス)
- SNMP (簡易ネットワーク管理プロトコル) を介したネットワーク管理アプリケーション



(注) SNMP を使用して、サポートされる MIB によって定義されるスタック全体のネットワーク機能を管理します。スイッチは、スタック メンバシップや選択などのスタック固有の機能を管理するための MIB をサポートしません。

- CiscoWorks ネットワーク管理ソフトウェア

スタックを管理するには、次のことを理解している必要があります。

- スタックの形成に関する概念：
 - 「スタック メンバシップ」 (P.5-3)
 - 「マスターの選択」 (P.5-4)
- スタックとメンバーの設定に関する概念：
 - 「スタック MAC アドレスとルータ MAC アドレス」 (P.5-5)
 - 「メンバー番号」 (P.5-6)
 - 「メンバーのプライオリティ値」 (P.5-6)
 - 「スタックのオフライン設定」 (P.5-7)
 - 「スイッチ スタックのハードウェア互換性と SDM 不一致モード」 (P.5-9)
 - 「スタックのソフトウェア互換性に関する推奨事項」 (P.5-9)
 - 「スタック プロトコルバージョンの互換性」 (P.5-10)
 - 「スイッチ間のメジャー バージョン番号の非互換性」 (P.5-10)
 - 「スイッチ間のマイナー バージョン番号の非互換性」 (P.5-10)
 - 「互換性のないソフトウェアおよびメンバー イメージのアップグレード」 (P.5-14)
 - 「スタックのコンフィギュレーション ファイル」 (P.5-14)

- 「スイッチ スタックのシステム全体の設定に関する補足考慮事項」 (P.5-15)
- 「スタックの管理接続」 (P.5-16)
- 「スタックの設定のシナリオ」 (P.5-17)

スタック メンバシップ

スタンドアロン スイッチは、マスターでもある単一のメンバーで構成されるスタックです。スタンドアロン スイッチを別のスイッチへ接続して (図 5-1 (P.5-3) を参照)、2つのスタック メンバー (どちらか一方がマスター) を持つスタックを作成することができます。スタンドアロン スイッチを既存のスタックに接続して (図 5-2 (P.5-4) を参照)、スタック メンバシップを増やすこともできます。

スタック メンバーを同一のモデルと交換した場合、新たなスイッチは交換されたスイッチと同じメンバー番号を使用すれば、交換されたスイッチと同じ設定で機能します。スイッチ スタックを割り当てる利点については、「スタックのオフライン設定」 (P.5-7) を参照してください。障害の発生したスイッチの交換については、『Hardware Installation Guide』の「Troubleshooting」の章を参照してください。

マスターを削除したり、電源の入ったスタンドアロン スイッチまたはスタックを追加したりしないかぎり、メンバシップの変更中も、スタックの動作は中断なく継続されます。



(注)

スタックの動作が中断されないようにするには、スタックに追加または削除するスイッチの電源が切断されていることを確認します。

メンバーを追加または削除したあとで、スタックがすべての帯域幅 (32 Gbps) で動作していることを確認します。スタック モード LED が点灯するまで、メンバーの Mode ボタンを押します。スタック内のすべてのスイッチの最後の2つのポート LED は、グリーンに点灯します。最後の2つのポート LED のいずれか、または両方がグリーンに点灯しない場合は、スタックがすべての帯域幅で動作していません。

- 電源が入っているスイッチを追加すると (マージ)、マージ中のスイッチ スタックの各スタック マスターは、自分達の中から1台のスタック マスターを選択します。新しいマスターは、マスターの役割と設定を保持し、メンバーもメンバーの役割と設定を保持します。それ以前のマスターを含む残りのすべてのスイッチは、リロードされ、メンバーとしてスタックに参加します。それらは、メンバー番号を使用可能な最小の番号に変更し、新しいマスターの設定を使用します。
- 電源がオンの状態のメンバーを取り外すと、スタックがそれぞれ同じ設定を持つ複数のスイッチ スタックに分割 (パーティション化) されます。そのため、ネットワーク内で IP アドレス設定が競合してしまうことがあります。スタックを分割状態のまま使用する場合は、新規に作成されたスタックの IP アドレスを変更します。

図 5-1 2台のスタンドアロン スイッチから構成されたスイッチ スタックの作成

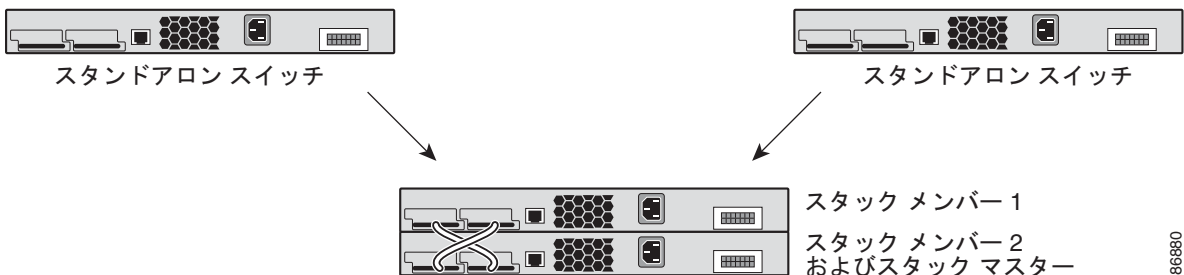
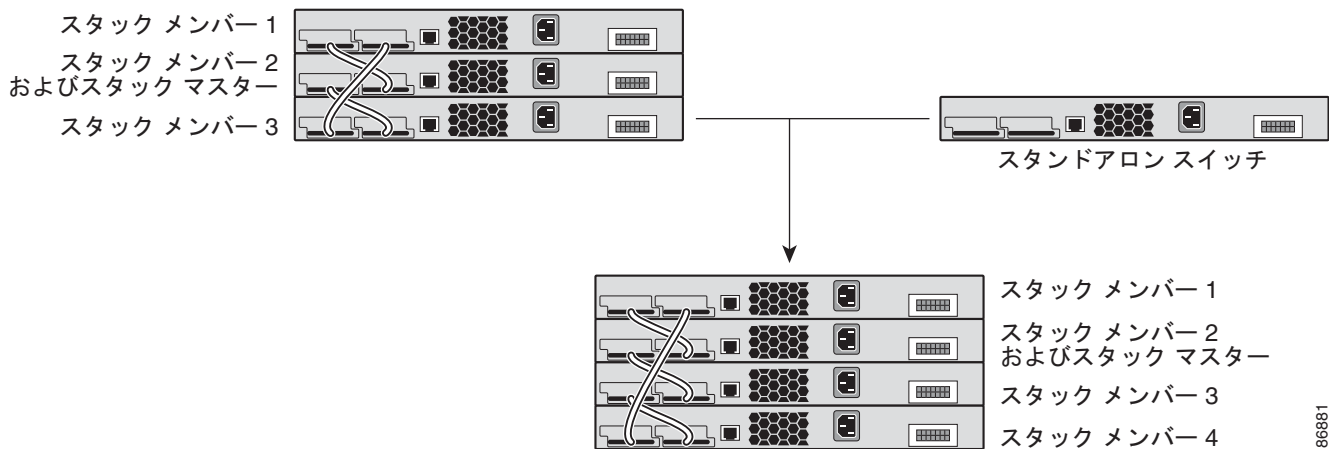


図 5-2 スタンドアロン スイッチのスイッチ スタックへの追加



スイッチ スタックの配線方法および電源の投入方法の詳細については、『Hardware Installation Guide』の「Switch Installation」の章を参照してください。

マスターの選択

スタック マスターは、次にリストした順番で、いずれかのファクタに基づいて選択されます。

1. 現在スタック マスターであるスイッチ
2. 最高のスタック メンバー プライオリティ値を持つスイッチ



(注) マスターにしたいスイッチには、最高のプライオリティ値を割り当てることを推奨します。これによって、再選択の実行時には、そのスイッチがマスターとして選択されます。

3. デフォルトのインターフェイス レベルの設定を使用していないスイッチ
4. よりプライオリティの高いスイッチ ソフトウェア バージョンのスイッチ。最高プライオリティから最低プライオリティへ順番にスイッチ ソフトウェア バージョンをリストすると、次のようになります。
 - 暗号化 IP サービス イメージ ソフトウェア
 - 非暗号化 IP サービス イメージ ソフトウェア
 - 暗号化 IP ベース イメージ ソフトウェア
 - 非暗号化 IP ベース イメージ ソフトウェア

スタック内の複数のスイッチが異なるソフトウェア イメージを使用する場合は、非暗号化 IP ベース イメージを稼動するスイッチがマスターとして選択されることがあります。暗号化 IP サービス イメージを稼動するスイッチの開始は、非暗号化イメージを稼動するスイッチよりも 10 秒以上長くかかります。暗号化イメージを稼動するスイッチは、10 秒間続くマスター選択プロセスから除外されます。この問題を防ぐには、IP ベース イメージを稼動するスイッチを Cisco IOS Release 12.1(11)AX 以降のソフトウェア リリースにアップグレードするか、手動でマスターを起動して新しいメンバーを起動するまで最低 8 秒待ちます。

5. MAC アドレスが最小のスイッチ

スタック マスターは、次のイベントのいずれかが発生しないかぎり、役割を維持します。

- スタックがリセットされた。*
- マスターがスタックから削除された。
- マスターがリセットされたか、電源が切れた。
- マスターに障害が発生した。
- 電源の入ったスタンドアロン スイッチまたはスイッチ スタックが追加され、スタック メンバシップが増えた。*

アスタリスク (*) がマークされたイベントでは、リストされたファクタに基づいて現在のスタック マスターが再選択される **可能性があります**。

スタック全体に電源を入れるかリセットすると、一部のスタック メンバーがマスター選択に参加しない場合があります。

- 再選択には、すべてのメンバーが参加します。
- 同じ 20 秒の間に電源が投入されたメンバーは、マスターの選択に参加し、マスターとして選択される可能性があります。
- 20 秒経過後に電源が投入されたメンバーは、この初回の選択には参加せず、単にメンバーになります。



(注)

Cisco IOS Release 12.2(20)SE3 より前のリリースが稼動するスイッチでは、10 秒経過後にスタック マスターが選択されます。

数秒後、新たなマスターが使用可能になります。その間、スイッチ スタックはメモリ内の転送テーブルを使用して、ネットワークの中断を最小限に抑えます。新たなスタック マスターが選択され、リセットされている間、他の使用可能なスタック メンバーの物理インターフェイスには何も影響はありません。

新たなマスターが選択され、以前のスタック マスターが使用可能になっても、以前のマスターはスタック マスターとしての役割は再開しません。

スタック マスターの選択に影響する電源投入の考慮事項の詳細については、『Hardware Installation Guide』の「Switch Installation」の章を参照してください。

スタック MAC アドレスとルータ MAC アドレス

マスターの MAC アドレスによってスタック MAC アドレスが決定します。

スタックが初期化すると、マスターの MAC アドレスによってブリッジ ID とルータ MAC アドレスが決定します。これにより、スタックがネットワーク内で識別されます。

マスターが変わると、**新たなマスターの MAC アドレスによって、新たなブリッジ ID とルータ MAC アドレスが決定します**。ただし、固定 MAC アドレス機能がイネーブルの場合、スタック MAC アドレスが変更されるまで約 4 分の遅延があります。この期間、前のマスターがスタックに復帰すると、スイッチがメンバーであってマスターではない場合でも、スタックはその MAC アドレスをスタック MAC アドレスとして使用し続けます。前のマスターがこの期間にスタックに復帰しない場合、スタックは新しいスタック マスターの MAC アドレスをスタック MAC アドレスとして取得します。詳細については、「[固定 MAC アドレスのイネーブル化](#)」(P.5-19) を参照してください。

メンバー番号

メンバー番号 (1 ~ 9) は、スタック内の各メンバーを識別します。また、メンバー番号によって、メンバーが使用するインターフェイス レベルの設定が決定します。

新品のスイッチ (スタックに参加していないか、手動でメンバー番号が割り当てられていないスイッチ) は、デフォルトのメンバー番号 1 が設定された状態で出荷されています。スタックに参加すると、デフォルトのスタック メンバー番号はスタック内の使用可能なメンバー番号の中で最小の番号に変更されます。

同じスタック内のメンバーは、同じメンバー番号を持つことはできません。

- **switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用して手動でメンバー番号を変更した場合は、その番号がまだ変更されていないときにだけ、そのメンバーのリセット後 (または、**reload slot stack-member-number** 特権 EXEC コマンドの使用後) に、新たな番号が有効となります。

スタック メンバー番号は、**SWITCH_NUMBER** 環境変数を使用して変更することもできます。

その番号がスタック内の別のメンバーによって使用されている場合、スイッチはスタック内で使用可能な最小の番号を選択します。

手動でメンバー番号を変更し、その番号にインターフェイス レベルの設定が関連付けられていない場合は、メンバーをデフォルト設定にリセットします。

割り当てられたスイッチでは、**switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用できません。このコマンドを使用した場合、コマンドは拒否されます。

- スタック メンバーを別のスイッチ スタックへ移動した場合、スタック メンバーは、自分の番号がスタック内の別のメンバーによって使用されていないときにだけ、その番号を保持します。その番号がスタック内の別のメンバーによって使用されている場合、スイッチはスタック内で使用可能な最小の番号を選択します。

詳細については、以下を参照してください。

- メンバー番号を変更する手順については、「[メンバー番号の割り当て](#)」(P.5-21) を参照してください。
- **SWITCH_NUMBER** 環境変数については、「[環境変数の制御](#)」(P.3-21) を参照してください。
- メンバー番号と設定については、「[スタックのコンフィギュレーション ファイル](#)」(P.5-14) を参照してください。
- スタックのマージについては、「[スタック メンバシップ](#)」(P.5-3) を参照してください。

メンバーのプライオリティ値

メンバーのプライオリティ値が高いほど、マスターとして選択され、自分のメンバー番号を保持できる可能性が高くなります。指定できるプライオリティ値は 1 ~ 15 です。デフォルトのプライオリティ値は 1 です。



(注)

スタック マスターにしたいスイッチには、最高のプライオリティ値を割り当てることを推奨します。これによって、再選択の実行時には、そのスイッチがマスターとして選択されます。

新しいプライオリティ値はすぐに有効となりますが、現在のマスターまたはスタックがリセットされるまでは現在のマスターに影響しません。

スタックのオフライン設定

オフライン設定機能を使用すると、新しいスイッチがスタックに参加する前に、スイッチに割り当て（スイッチを設定）できます。まだスタックに属していないスイッチに関連したメンバー番号、スイッチタイプ、インターフェイスを設定できます。その設定が、割り当てられた設定になります。スタックに追加され、この設定を受信するスイッチは、割り当てられたスイッチです。

スイッチが Cisco IOS Release 12.2(20)SE 以降で稼動するスタックに追加された場合に、割り当てられた設定が存在しないと、割り当てられた設定が自動的に作成されます。**switch stack-member-number provision type** グローバル コンフィギュレーション コマンドを使用すると、割り当てられた設定を手動で作成できます。

割り当てられたスイッチのインターフェイスを（たとえば、VLAN の一部として）設定すると、その情報は、その割り当てられたスイッチがスタックに属するかどうかに関係なく、スタックの実行コンフィギュレーションに表示されます。その割り当てられたスイッチのインターフェイスはアクティブではなく、特定機能のディスプレイ（**show vlan** ユーザ EXEC コマンドの出力など）には表示されません。**no shutdown** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。

スタートアップ コンフィギュレーション ファイルでは、割り当てられたスイッチがスタックに属するかどうかに関係なく、スタックは保存した情報をリロードして使用できます。

割り当てられたスイッチのスタックへの追加による影響

割り当てられたスイッチをスイッチ スタックに追加する場合、スタックは割り当てられた設定、またはデフォルト設定のいずれかを適用します。表 5-1 では、スイッチ スタックが割り当てられた設定と割り当てられたスイッチを比較するときに発生するイベントを示します。

表 5-1 割り当てられた設定と割り当てられたスイッチとの比較結果

シナリオ		結果
スタック メンバー番号およびスイッチ タイプが適合する	<ol style="list-style-type: none"> 1. 割り当てられたスイッチのスタック メンバー番号と、スタック上で割り当てられた設定のスタック メンバー番号が一致する場合で、 2. 割り当てられたスイッチのスイッチ タイプと、スタック上で割り当てられた設定のスイッチ タイプが一致する場合 	スイッチ スタックは、割り当てられた設定を割り当てられたスイッチに適用し、スタックに追加します。
スタック メンバー番号は一致するが、スイッチ タイプが一致しない	<ol style="list-style-type: none"> 1. 割り当てられたスイッチのスタック メンバー番号と、スタック上で割り当てられた設定のスタック メンバー番号が一致する場合で、 2. 割り当てられたスイッチのスイッチ タイプと、スタック上で割り当てられた設定のスイッチ タイプが一致しない場合 	<p>スイッチ スタックは、デフォルト設定を割り当てられたスイッチに適用し、スタックに追加します。</p> <p>割り当てられた設定は、新しい情報を反映するために変更されます。</p>
割り当てられた設定でスタック メンバー番号が検出されない		<p>スイッチ スタックは、デフォルト設定を割り当てられたスイッチに適用し、スタックに追加します。</p> <p>割り当てられた設定は、新しい情報を反映するために変更されます。</p>

表 5-1 割り当てられた設定と割り当てられたスイッチとの比較結果 (続き)

シナリオ	結果
割り当てられたスイッチでスタックメンバー番号が既存のスタックメンバーと競合する	スイッチスタックは、割り当てられた設定を割り当てられたスイッチに適用し、スタックに追加します。 割り当てられた設定は、新しい情報を反映するために変更されます。
割り当てられたスイッチのスタックメンバー番号が、割り当てられた設定で検出されない	スイッチスタックは、デフォルト設定を割り当てられたスイッチに適用し、スタックに追加します。

割り当てられた設定で指定したスイッチタイプとは異なるスイッチを、電源が切られたスイッチスタックに追加して電力供給すると、スイッチスタックはスタートアップコンフィギュレーションファイルの **switch stack-member-number provision type** グローバルコンフィギュレーションコマンド (現在は正しくないコマンド) を拒否します。ただし、スタックの初期化中は、スタートアップコンフィギュレーションファイルのデフォルトでないインターフェイスコンフィギュレーション情報が、(間違っただけの可能性はある) 割り当てられたインターフェイス向けに実行されます。実際のスイッチタイプと前述の割り当てられたスイッチタイプの違いによって、拒否されるコマンドと、受け入れられるコマンドがあります。

たとえば、Power over Ethernet (PoE; イーサネット経由の電源供給) を装備した 48 ポートスイッチ用にスイッチスタックを割り当てて、設定を保存し、スタックの電源を切った後、PoE を装備していない 24 ポートスイッチをスイッチスタックに接続して、スタックの電源を入れたとします。この状況では、ポート 25 ~ 48 の設定は拒否され、エラーメッセージが初期化中のスタックマスタースイッチコンソール上に表示されます。さらに、PoE 対応インターフェイスで有効な、設定済み PoE 関連コマンドは、ポート 1 ~ 24 に対しても拒否されます。



(注)

スイッチスタックが Cisco IOS Release 12.2(20)SE 以降で稼動し、新しいスイッチ用に割り当てられた設定を含まない場合、スイッチはデフォルトのインターフェイスコンフィギュレーションでスタックに参加します。スイッチスタックは、新しいスイッチと一致する **switch stack-member-number provision type** グローバルコンフィギュレーションコマンドを実行コンフィギュレーションに追加します。

設定手順については、「スタックへの新しいメンバーの割り当て」(P.5-22)を参照してください。

スタックの割り当てられたスイッチの交換による影響

スイッチスタック内で割り当てられたスイッチが故障し、スタックから取り外され、別のスイッチと交換する場合、スタックは割り当てられた設定、またはデフォルト設定をこのスイッチに適用します。スイッチスタックが、割り当てられた設定と割り当てられたスイッチを比較するときに発生するイベントは、「割り当てられたスイッチのスタックへの追加による影響」(P.5-7)に記載のイベントと同じです。

割り当てられたスイッチのスタックからの削除による影響

スイッチスタックが Cisco IOS Release 12.2(20)SE 以降で稼働し、割り当てられたスイッチをスイッチスタックから削除した場合、削除されたスタックメンバーと関連する設定は、割り当てられた情報として実行コンフィギュレーションにあります。設定を完全に削除するには、**no switch stack-member-number provision** グローバルコンフィギュレーションコマンドを使用します。

スイッチスタックのハードウェア互換性と SDM 不一致モード

Catalyst 3750-12S スイッチは、デスクトップおよびアグリゲータ Switch Database Management (SDM; スイッチデータベース管理) テンプレートをサポートします。他のすべての Catalyst 3750 スイッチは、デスクトップ SDM テンプレートのみをサポートします。

スタックメンバーはすべて、スタックマスターに設定された SDM テンプレートを使用します。スタックマスターがアグリゲータテンプレートを使用している場合は、Catalyst 3750-12S スイッチだけがスタックメンバーになることができます。このスイッチスタックに参加しようとする他のスイッチはすべて、SDM 不一致モードになります。これらのスイッチは、スタックマスターがデスクトップ SDM テンプレート稼働している場合にだけ、スタックに参加できます。

Catalyst 3750-12S スイッチのスイッチスタックを作成予定の場合にかぎり、スタックマスターにアグリゲータテンプレートを使用させることを推奨します。異なる Catalyst 3750 スイッチモデルを持つスイッチスタックを作成予定の場合は、いずれかのデスクトップテンプレートを使用するようにスタックマスターを設定してください。



(注)

Version-mismatch (VM; バージョン不一致) モードは、SDM 不一致モードより優先されます。VM モード条件と SDM 不一致モードが存在する場合、スイッチスタックは先に VM モード条件を解決しようとします。

show switch 特権 EXEC コマンドを使用すると、スタックメンバーが SDM 不一致モードになっているかどうかを確認できます。

SDM テンプレートと SDM 不一致モードの詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

スタックのソフトウェア互換性に関する推奨事項

メンバー間でスタックプロトコルバージョンの互換性を確保するには、すべてのスタックメンバーが同じ Cisco IOS ソフトウェアバージョンを稼働している必要があります。

スタック プロトコルバージョンの互換性

スタック プロトコルバージョンには、メジャーバージョン番号とマイナーバージョン番号があります (たとえば 1.4 の場合は、1 がメジャーバージョン番号で、4 がマイナーバージョン番号になります)。

Cisco IOS ソフトウェアのバージョンが同じスイッチは、スタック プロトコルのバージョンも同じです。すべての機能がスタック全体にわたって適切に動作します。マスターとソフトウェアバージョンが同じスイッチは、すぐにスタックに参加します。

非互換性が混在する場合は、特定のスタック メンバーの非互換の原因を示すシステム メッセージが生成されます。マスターは、すべてのメンバーに対してメッセージを送信します。

詳細については、「[スイッチ間のメジャーバージョン番号の非互換性](#)」の手順 (P.5-10) および「[スイッチ間のマイナーバージョン番号の非互換性](#)」の手順 (P.5-10) を参照してください。

スイッチ間のメジャーバージョン番号の非互換性

多くの場合、異なる Cisco IOS ソフトウェアバージョンのスイッチは、スタック プロトコルバージョンも異なります。メジャーバージョン番号が異なるスイッチは非互換で、同じスタック内には存在できません。

スイッチ間のマイナーバージョン番号の非互換性

マスターとメジャーバージョン番号は同じだがマイナーバージョン番号が異なるスイッチは、部分的に互換可能であると見なされます。スタックに接続されている場合、部分的に互換可能なスイッチはバージョン不一致モードになり、完全な機能を備えたメンバーとしてはスタックに参加できません。ソフトウェアは不一致ソフトウェアを検出すると、スタック イメージまたはスタック フラッシュ メモリの tar ファイル イメージを使用して、バージョン不一致モードのスイッチをアップグレード (またはダウングレード) しようとします。ソフトウェアでは、自動的なアップグレード (自動アップグレード) 機能または自動的なアドバイス (自動アドバイス) 機能を使用します。

バージョン不一致モードのスイッチ上のポート LED も、オフのままです。Mode ボタンを押しても、LED モードは変更されません。



(注)

自動アドバイスおよび自動コピーでは、スイッチスタック上の info ファイルの調査およびディレクトリ構造の検索により、実行中のイメージを識別します。archive download-sw 特権 EXEC コマンドではなく copy tftp: コマンドを使用してイメージをダウンロードすると、正確なディレクトリ構造が適切に作成されません。info ファイルの詳細については、「[サーバまたは Cisco.com 上のイメージの tar ファイル形式](#)」(P.C-26) を参照してください。

自動アップグレードおよび自動アドバイスの概要

ソフトウェアが不一致ソフトウェアを検出し、バージョン不一致モードのスイッチをアップグレードしようとする場合は、2つのソフトウェア プロセスを行います。それは自動的なアップグレードと自動的なアドバイスです。

- 自動的なアップグレード（自動アップグレード）には、自動コピー プロセスと自動抽出プロセスが含まれています。デフォルトでは、自動アップグレードはイネーブル（**boot auto-copy-sw** グローバル コンフィギュレーション コマンドがイネーブル）です。自動アップグレードをディセーブルにするには、マスター上で **no boot auto-copy-sw** グローバル コンフィギュレーション コマンドを使用します。 **show boot** 特権 EXEC コマンドを使用して、表示される *Auto upgrade* 行を確認することにより、自動アップグレードのステータスを確認できます。
 - 自動コピーは、メンバーで稼動するソフトウェア イメージをバージョン不一致モードのスイッチにコピーして、これをアップグレード（自動アップグレード）します。自動コピーが発生するのは、自動アップグレードがイネーブルの場合、バージョン不一致モードのスイッチに十分なフラッシュ メモリ容量がある場合、スタックで稼動中のソフトウェア イメージがバージョン不一致モードのスイッチに適している場合です。



(注) バージョン不一致モードのスイッチでは、すべてのリリース済みのソフトウェアが稼動するとは限りません。たとえば、新しいスイッチ ハードウェアは以前のソフトウェア バージョンでは認識されません。

- 自動アップグレードプロセスで、バージョン不一致モードのスイッチにコピーするための適切なソフトウェアがスタックで見つからない場合は、自動的な抽出（自動抽出）が発生します。この場合、スイッチ スタックまたはバージョン不一致モードのスイッチをアップグレードするために必要な **tar** ファイルについて、バージョン不一致モードであるかどうかに関係なくスタック内のすべてのスイッチが自動検出プロセスで検索されます。**tar** ファイルは、スタック（バージョン不一致モードのスイッチを含む）内のいずれかのフラッシュ ファイル システムにある可能性があります。バージョン不一致モードのスイッチに適した **tar** ファイルが検出された場合、このプロセスでファイルが抽出されてそのスイッチが自動的にアップグレードされます。

自動アップグレード（自動コピーおよび自動抽出）プロセスは、不一致のソフトウェアが検出された後開始されるまで数分かかります。

自動アップグレードプロセスが完了すると、バージョン不一致モードであったスイッチはリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。リロード中に両方の **StackWise** ケーブルが接続されている場合、スタックは2つのリング上で動作するため、ネットワーク ダウンタイムが発生しません。



(注) 自動アップグレードでは、別のパッケージング レベルのイメージをロードしているスイッチをアップグレードしません。たとえば、**IP** ベース イメージが稼動中のスイッチを **IP** サービスにアップグレードするのに自動アップグレードを使用することができません。ただし、自動アップグレードは同じパッケージングレベルの暗号化イメージと非暗号化イメージとの間のアップグレードはサポートしています。

- 自動的なアドバイス（自動アドバイス）：自動アップグレードプロセスにより、バージョン不一致モードのスイッチにコピーするのに適したバージョン不一致メンバー ソフトウェアが検出されない場合、自動アドバイス プロセスにより、スイッチ スタックまたはバージョン不一致モードのスイッチを手動でアップグレードするのに必要なコマンド（**archive copy-sw** または **archive download-sw** 特権 EXEC コマンド）およびイメージ名（**tar** ファイル名）が指定されます。推奨されるイメージは実行中のスタック イメージ、またはスタック（バージョン不一致モードのスイッチを含む）内のいずれかのフラッシュ ファイル システムの **tar** ファイルです。スタック フラッシュ ファイル システムで適切なイメージが見つからない場合、自動アドバイス プロセスでスタックに新規ソフトウェアをインストールするように指示されます。自動アドバイスは、ディセーブルにはできません。また、この機能のステータスを確認するコマンドはありません。

スタック ソフトウェアおよびバージョン不一致モードのスイッチのソフトウェアに同じフィアチャセットが含まれない場合は、自動アドバイス ソフトウェアからの指示もありません。たとえば、IP ベース イメージが稼動するスイッチ スタックに、IP サービス イメージが稼動するスイッチを追加した場合、自動アドバイス ソフトウェアは推奨ソフトウェアを提示しません。暗号化イメージおよび非暗号化イメージが稼動する場合も、同様です。

archive-download-sw /allow-feature-upgrade 特権 EXEC コマンドを使用して、別のフィアチャセットを持つイメージをインストールすることができます。

自動アップグレードおよび自動アドバイスのメッセージ例

マイナー バージョン番号が異なるスイッチをスタックに追加すると、メッセージが連続して表示されます（スイッチがその他のシステム メッセージを生成しない場合）。

次に、スタックが、スタックと異なるマイナー バージョン番号を実行する新しいスイッチを検出した例を示します。自動コピーが起動し、メンバーからバージョン不一致モードのスイッチにコピーするのに適したソフトウェアを検出し、バージョン不一致モードのスイッチをアップグレードして、リロードします。

```
*Mar 11 20:31:19.247:%STACKMGR-6-STACK_LINK_CHANGE:Stack Port 2 Switch 2 has changed to
state UP
*Mar 11 20:31:23.232:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
*Mar 11 20:31:23.291:%STACKMGR-6-SWITCH_ADDED_VM:Switch 1 has been ADDED to the stack
(VERSION_MISMATCH) (Stack_1-3)
*Mar 11 20:33:23.248:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED:Auto-copy-software process
initiated for switch number(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Searching for stack member to act
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:as software donor...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Found donor (system #2) for
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:member(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System software to be uploaded:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:System Type:                0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving c3750-ipservices-mz.122-25.SEB
(directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving
c3750-ipservices-mz.122-25.SEB/c3750-ipservices-mz.122-25.SEB.bin (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving
c3750-ipservices-mz.122-25.SEB/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:archiving info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:examining image...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting
c3750-ipservices-mz.122-25.SEB/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:Stacking Version Number:1.4
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
```



```

*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: System Type: 0x00000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Ios Image File Size: 0x004BA200
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Total Image File Size: 0x00818A00
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Minimum Dram required: 0x08000000
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Image Suffix: ipservices-122-25.SEB
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Image
Directory: c3750-ipservices-mz.122-25.SEB
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Image Name: c3750-ipservices-mz.122-25.SEB
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Image
Feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Old image for switch
1: flash1: c3750-ipservices-mz.122-25.SEB
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Old image will be deleted after download.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Extracting images from archive into flash on
switch 1...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: c3750-i5-mz.122-0.0.313.SE (directory)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: extracting
c3750-i5-mz.122-0.0.313.SE/c3750-ipservices-mz.122-25.SEB (4945851 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: extracting
c3750-ipservices-mz.122-25.SEB/info (450 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: extracting info (104 bytes)
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Installing
(renaming): `flash1:update/c3750-i5-mz.122-0.0.313.SE' ->
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
`flash1: c3750-ipservices-mz.122-25.SEB'
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: New software image installed in
flash1: c3750-i5-mz.122-0.0.313.SE
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Removing old
image: flash1: c3750-i5-mz.121-19.EA1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: All software images installed.
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Requested system reload in progress...
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Software successfully copied to
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: system(s) 1
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Done copying software
*Mar 11 20:36:15.038:%IMAGEMGR-6-AUTO_COPY_SW: Reloading system(s) 1

```

次に、スタックが、スタックと異なるマイナーバージョン番号を実行する新しいスイッチを検出した例を示します。自動コピーは起動しますが、スタックと互換可能にするための、バージョン不一致モードのスイッチにコピーするソフトウェアをスタック内で検出できません。自動アドバイス処理が起動し、ネットワークからバージョン不一致モードのスイッチに tar ファイルをダウンロードするように推奨されます。

```

*Mar 1 00:01:11.319:%STACKMGR-6-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to
state UP
*Mar 1 00:01:15.547:%STACKMGR-6-SWITCH_ADDED_VM: Switch 1 has been ADDED to the stack
(VERSION_MISMATCH)
stack_2#
*Mar 1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW_INITIATED: Auto-copy-software process
initiated for switch number(s) 1
*Mar 1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW:
*Mar 1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW: Searching for stack member to act
*Mar 1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW: as software donor...
*Mar 1 00:03:15.554:%IMAGEMGR-6-AUTO_COPY_SW: Software was not copied
*Mar 1 00:03:15.562:%IMAGEMGR-6-AUTO_ADVISE_SW_INITIATED: Auto-advise-software process
initiated for switch number(s) 1
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:

```

```
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:Systems with incompatible software
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:have been added to the stack. The
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:storage devices on all of the stack
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:members have been scanned, and it has
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:been determined that the stack can be
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:repaired by issuing the following
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:command(s):
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW: archive download-sw /force-reload
/overwrite /dest 1 flash1:c3750-ipservices-mz.122-25.SEB.tar
*Mar 1 00:04:22.537:%IMAGEMGR-6-AUTO_ADVISE_SW:
```

archive download-sw 特権 EXEC コマンドの使用の詳細については、「ソフトウェアイメージの操作」(P.C-25) を参照してください。

互換性のないソフトウェアおよびメンバーイメージのアップグレード

互換性のないソフトウェアイメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のメンバーからソフトウェアイメージをコピーします。このスイッチは、新しいイメージを使用して自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

詳細については、「スタックメンバー間のイメージファイルのコピー」(P.C-41) を参照してください。

スタックのコンフィギュレーションファイル

マスターには、スタックの保存済みの実行コンフィギュレーションファイルが格納されています。すべてのメンバーは、定期的に、マスターからコンフィギュレーションファイルの同期化されたコピーを受け取ります。マスターが使用不能になると、マスターの役割を引き受けたメンバーが最新のコンフィギュレーションファイルを保持します。

- すべてのメンバーに適用されるシステムレベル（グローバル）コンフィギュレーション設定：IP、Spanning-Tree Protocol (STP; スパニング ツリー プロトコル)、VLAN、SNMP 設定など
- メンバーのインターフェイス固有のコンフィギュレーション設定：各メンバーに固有



(注)

すべてのメンバーで Cisco IOS Release 12.1(14)EA1 以降を稼動することを推奨します。これによって、実行コンフィギュレーションがスタートアップコンフィギュレーションに保存されていない状態でマスターが交換されても、マスターのインターフェイス固有のコンフィギュレーションは確実に保存されます。

スタックに参加する新規のスイッチは、そのスタックのシステムレベルの設定を使用します。スイッチが別のスタックに移動された場合、そのスイッチは保存済みのコンフィギュレーションファイルを失い、新たなスタックのシステムレベルの設定を使用します。

各メンバーのインターフェイス固有のコンフィギュレーションには、そのメンバー番号が関連付けられます。スタックメンバーは、メンバー番号が手動で変更されるか、同じスタック内の別のメンバーによってすでに使用されているかしないかぎり、自分の番号を保持します。

- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在しない場合は、メンバーはデフォルトのインターフェイス固有のコンフィギュレーションを使用します。
- そのメンバー番号に対応するインターフェイス固有のコンフィギュレーションが存在する場合は、メンバーはそのメンバー番号に関連付けられたインターフェイス固有のコンフィギュレーションを使用します。

障害の発生したメンバーを同一のモデルと交換した場合、交換後のメンバーは自動的に同じインターフェイス固有のコンフィギュレーションを使用します。インターフェイス設定を再設定する必要はありません。交換後のスイッチは、障害の生じたスイッチと同じメンバー番号を持つ必要があります。

スタンドアロンスイッチのコンフィギュレーションの場合と同じ方法で、スタックコンフィギュレーションをバックアップし復元します。

詳細については、以下を参照してください。

- スイッチスタックを割り当てる利点については、「[スタックのオフライン設定](#)」(P.5-7)を参照してください。
- ファイルシステムとコンフィギュレーションファイルについては、[付録C「Cisco IOS ファイルシステム、コンフィギュレーションファイル、およびソフトウェアイメージの操作」](#)を参照してください。

スイッチスタックのシステム全体の設定に関する補足考慮事項

- 『*Getting Started with Cisco Network Assistant*』(Cisco.com から入手できます)の「[Planning and Creating Clusters](#)」の章
- 「[MAC アドレスおよびスイッチスタック](#)」(P.7-22)
- 「[SDM テンプレートの設定](#)」(P.8-6)
- 「[802.1X 認証とスイッチスタック](#)」(P.10-11)
- 「[VTP とスイッチスタック](#)」(P.15-8)
- 「[プライベート VLAN およびスイッチスタック](#)」(P.17-6)
- 「[スパニングツリーとスイッチスタック](#)」(P.19-12)
- 「[MSTP とスイッチスタック](#)」(P.20-9)
- 「[DHCP スヌーピングおよびスイッチスタック](#)」(P.23-9)
- 「[IGMP スヌーピングおよびスイッチスタック](#)」(P.25-7)
- 「[ポートセキュリティおよびスイッチスタック](#)」(P.26-20)
- 「[CDP およびスイッチスタック](#)」(P.27-2)
- 「[SPAN/RSPAN およびスイッチスタック](#)」(P.30-10)
- 「[ACL およびスイッチスタック](#)」(P.35-7)
- 「[EtherChannel およびスイッチスタック](#)」(P.37-10)
- 「[IP ルーティングおよびスイッチスタック](#)」(P.38-3)
- 「[IPv6 とスイッチスタック](#)」(P.39-10)
- 「[HSRP およびスイッチスタック](#)」(P.42-5)
- 「[マルチキャストルーティングおよびスイッチスタック](#)」(P.46-11)
- 「[フォールバックブリッジングおよびスイッチスタック](#)」(P.48-3)

スタックの管理接続

マスターを使用して、スタックとメンバー インターフェイスを管理します。CLI、SNMP、Network Assistant、CiscoWorks ネットワーク管理アプリケーションを使用できます。個々のスイッチとしてメンバーを管理することはできません。

- 「IP アドレスによるスタックへの接続」(P.5-16)
- 「SSH セッションによるスタックへの接続」(P.5-16)
- 「コンソール ポートによるスタックへの接続」(P.5-16)
- 「特定のメンバーへの接続」(P.5-16)

IP アドレスによるスタックへの接続

スタックはシステム レベルの IP アドレスを使用して管理されます。スタックからマスターや他のスタック メンバーを削除しても、IP 接続が存続していれば、引き続き同じ IP アドレスを使用してスタックを管理できます。



(注)

スタックからメンバーを削除した場合、各メンバーは自身の IP アドレスを保持します。したがって、ネットワーク内に同じ IP アドレスを持つデバイスが 2 つある状態を避けるために、スタックから削除したスイッチの IP アドレスは変更します。

スイッチ スタックの設定に関する情報は、「スタックのコンフィギュレーション ファイル」(P.5-14) を参照してください。

SSH セッションによるスタックへの接続

IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの暗号化バージョンを稼動するマスターに障害が生じたか、それが非暗号化バージョンを稼動するスイッチと交換された場合には、スタックへの Secure Shell (SSH; セキュア シェル) 接続が失われることがあります。IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの暗号化バージョンを稼動しているスイッチをマスターにすることを推奨します。

コンソール ポートによるスタックへの接続

1 つまたは複数のメンバーのコンソール ポートを経由してマスターへ接続できます。

マスターに複数の CLI セッションを使用する場合は、慎重に行ってください。特定のセッションで入力したコマンドは、他のセッションに表示されません。したがって、コマンドを入力したセッションを識別できなくなることがあります。

スタックを管理する場合は、CLI セッションを 1 つだけ使用することを推奨します。

特定のメンバーへの接続

特定のメンバー ポートを設定する場合は、CLI の指定部分にスタック メンバー番号を指定する必要があります。

特定のメンバーへのアクセスについては、「特定のスタック メンバーへの CLI アクセス」(P.5-23) を参照してください。

スタックの設定のシナリオ

表 5-2 の大半のシナリオは、少なくとも 2 台のスイッチが StackWise ポートを使用して接続されていることを前提にしています。

表 5-2 スイッチスタックの設定のシナリオ

シナリオ		結果
既存のマスターによって、明確に決定されるマスター選択	StackWise ポートを使用して、2 つの電源の入ったスタックを接続します。	2 つのマスターの一方だけが、新たなスタック マスターになります。
メンバーのプライオリティ値によって、明確に決定されるマスター選択	<ol style="list-style-type: none"> StackWise ポートを使用して、2 台のスイッチを接続します。 <code>switch stack-member-number priority new-priority-number</code> グローバル コンフィギュレーション コマンドを使用して、1 つのメンバーに、より高いメンバー プライオリティ値を設定します。 両方のメンバーを同時に再起動します。 	より高いプライオリティ値を持つメンバーがマスターとして選択されます。
コンフィギュレーションファイルによって、明確に決定されるマスター選択	<p>両方のメンバーが同じプライオリティ値を持つものと仮定します。</p> <ol style="list-style-type: none"> 1 つのメンバーがデフォルトのコンフィギュレーションを持ち、他のメンバーが保存済み（デフォルトでない）のコンフィギュレーションファイルを持つことを確認します。 両方のメンバーを同時に再起動します。 	保存済みのコンフィギュレーションファイルを持つメンバーがマスターとして選択されます。
暗号化 IP サービス イメージソフトウェアによって、明確に決定されるマスター選択	<p>すべてのメンバーが同じプライオリティ値を持つものと仮定します。</p> <ol style="list-style-type: none"> 1 つのメンバーに暗号化 IP サービス イメージソフトウェアがインストールされ、他のメンバーには非暗号化 IP サービス イメージソフトウェアがインストールされていることを確認します。 両方のメンバーを同時に再起動します。 	暗号化 IP サービス イメージソフトウェアがインストールされたメンバーがマスターとして選択されます。
暗号化 IP ベース イメージソフトウェアによって、明確に決定されるマスター選択	<p>すべてのメンバーが同じプライオリティ値を持つものと仮定します。</p> <ol style="list-style-type: none"> 1 つのメンバーに暗号化 IP ベース イメージソフトウェアがインストールされ、他のメンバーには非暗号化 IP ベース イメージソフトウェアがインストールされていることを確認します。 両方のメンバーを同時に再起動します。 	暗号化 IP ベース イメージソフトウェアがインストールされたメンバーがマスターとして選択されます。

表 5-2 スイッチ スタックの設定のシナリオ (続き)

シナリオ		結果
MAC アドレスによって、明確に決定されるマスター選択	両方のメンバーが同じプライオリティ値、コンフィギュレーション ファイル、ソフトウェア イメージを持つものと仮定し、両方のスタック メンバーを同時に再起動します。	より小さい MAC アドレスを持つメンバーがマスターとして選択されます。
メンバー番号の競合	1 つのメンバーが他のメンバーより高いプライオリティ値を持つものと仮定します。 1. 両方のメンバーが同じメンバー番号を持っていることを確認します。必要に応じて、 switch current-stack-member-number renumber new-stack-member-number グローバル コンフィギュレーション コマンドを使用します。 2. 両方のメンバーを同時に再起動します。	より高いプライオリティ値を持つメンバーが、自分のメンバー番号を保持します。他のメンバーは、新たなスタック メンバー番号を持ちます。
メンバーの追加	1. 新しいスイッチの電源を切ります。 2. StackWise ポートを使用して、新たなスイッチを電源の入ったスタックに接続します。 3. 新しいスイッチの電源を入れます。	マスターはそのままです。新たなスイッチがスタックに追加されます。
マスターの障害	マスターを削除します (または、電源を切ります)。	残りのスタック メンバーのいずれかが新たなマスターになります。スタック内の他のすべてのメンバーはメンバーのままで、再起動はされません。
9 台を超えるメンバーの追加	1. StackWise ポートを使用して、10 台のスイッチを接続します。 2. すべてのスイッチの電源を入れます。	2 台のスイッチがマスターになります。一方のマスターが 9 つのスタック メンバーを制御します。もう一方のマスターは、スタンドアロン スイッチとして維持されます。 Mode ボタンとスイッチのポート LED を使用して、どのスイッチがマスターで、どのスイッチがどちらのマスターに属しているかを識別できます。 Mode ボタンと LED の詳細については、『Hardware Installation Guide』を参照してください。

スイッチ スタックの設定

- 「デフォルトのスイッチ スタック コンフィギュレーション」 (P.5-19)
- 「固定 MAC アドレスのイネーブル化」 (P.5-19)
- 「スタック メンバー情報の割り当て」 (P.5-21)
- 「スタック メンバシップの変更」 (P.5-23)

デフォルトのスイッチ スタック コンフィギュレーション

表 5-3 に、デフォルトのスイッチ スタック コンフィギュレーションを示します。

表 5-3 デフォルトのスイッチ スタック コンフィギュレーション

機能	デフォルト設定
スタック MAC アドレス タイマー	ディセーブル
メンバー番号	1
メンバーのプライオリティ値	1
オフライン設定	スイッチ スタックは割り当てられていません。
固定 MAC アドレス	ディセーブル

固定 MAC アドレスのイネーブル化

マスターの MAC アドレスによってスタック MAC アドレスが決定します。マスターがスタックから削除されて新しいマスターに引き継がれた場合、新しいマスターの MAC アドレスが新しいスタック MAC ルータ アドレスになります。ただし、スタック MAC アドレスを変更する前の時間遅延を使用して、固定 MAC アドレス機能を設定できます。この間に前のマスターがスタックに復帰すると、スイッチがメンバーであってマスターではない場合でも、スタックはその MAC アドレスをスタック MAC アドレスとして使用し続けます。スタック MAC アドレスが新規マスター MAC アドレスに変更されないように、スタック MAC を固定的に設定することも可能です。



注意

この機能を設定する際に、設定の結果を示す警告メッセージが表示されます。この機能は、慎重に使う必要があります。古いマスター MAC アドレスをドメイン内の別の場所で使用している場合、トラフィックが失われる可能性があります。

期間は 0 ～ 60 分に設定できます。

- コマンドを値なしで入力する場合、デフォルトの遅延は 4 分です。常に値を入力することを推奨します。明示的なタイマー値の 4 分が時間遅延としてコンフィギュレーション ファイルに表示されます。
- 0 を入力した場合、**no stack-mac persistent timer** コマンドを入力するまで前のマスターのスタック MAC アドレスが使用されます。このコマンドは、スタック MAC アドレスを現在のマスターの MAC アドレスに変更するものです。このコマンドを入力しない場合、スタック MAC アドレスは変更されません。
- 1 ～ 60 分の間で時間遅延を入力した場合、設定した期間が満了するか **no stack-mac persistent timer** コマンドを入力するまで、前のマスターのスタック MAC アドレスが使用されます。

前のマスターがこの期間中にスタックに復帰しない場合、スタックは新しいマスターの MAC アドレスをスタック MAC アドレスとして使用します。




(注)

スイッチ スタック全体をリロードする場合、マスターの MAC アドレスがスタック MAC アドレスとして取得されます。

固定 MAC アドレスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

■ スイッチ スタックの設定

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	stack-mac persistent timer [0 time-value]	<p>スタック マスターの変更後に、スタック MAC アドレスが新しいスタック マスターの MAC アドレスに変更されるまでの、時間遅延をイネーブルにします。この間中に前のスタック マスターがスタックに復帰する場合、スタックはその MAC アドレスをスタック MAC アドレスとして使用します。</p> <ul style="list-style-type: none"> • コマンドを値なしで入力して、デフォルトの遅延の 4 分を設定します。常に値を設定することを推奨します。 • 0 を入力して、現在のマスターの MAC アドレスを無期限に使用します。 • <i>time-value</i> に 1 ~ 60 を入力して、スタック MAC アドレスが新しいマスターに変更されるまでの期間 (分単位) を設定します。 <p> 注意 このコマンドを入力する場合、古いマスター MAC アドレスがネットワーク ドメインのどこかに出現した場合に、トラフィックが失われる可能性がある旨の警告が表示されます。</p> <p>新しいスタック マスターが引き継いだあとで期間が満了する前に no stack-mac persistent timer を入力した場合、スタックは現在のマスター MAC アドレスを使用します。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config または show switch	<p>スタック MAC アドレス タイマーがイネーブルであることを確認します。</p> <p>stack-mac persistent timer と分単位の時間が出力に表示されます。</p> <p>Mac persistency wait time に設定した分単位の値とスタック MAC アドレスが出力に表示されます。</p>
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

no stack-mac persistent timer グローバル コンフィギュレーション コマンドを使用して固定 MAC アドレス機能をディセーブルにします。

次に、7 分の時間遅延で固定 MAC アドレス機能を設定し、設定を確認する例を示します。

```
Switch(config)# stack-mac persistent timer 7
WARNING: The stack continues to use the base MAC of the old Master
WARNING: as the stack MAC after a master switchover until the MAC
WARNING: persistency timer expires. During this time the Network
WARNING: Administrators must make sure that the old stack-mac does
WARNING: not appear elsewhere in this network domain. If it does,
WARNING: user traffic may be blackholed.
Switch(config)# end
Switch# show switch
Switch/Stack Mac Address : 0016.4727.a900
Mac persistency wait time: 7 mins

                H/W   Current
Switch#  Role   Mac Address   Priority Version  State
-----
*1      Master 0016.4727.a900   1       0       Ready
```


スタックメンバー情報の割り当て

- 「メンバー番号の割り当て」(P.5-21) (任意)
- 「スタックメンバープライオリティ値の設定」(P.5-21) (任意)
- 「スタックへの新しいメンバーの割り当て」(P.5-22) (任意)

メンバー番号の割り当て



(注) この作業は、マスターからに限り実行できます。

メンバー番号をメンバーに割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch current-stack-member-number renumber new-stack-member-number	メンバーの現在のメンバー番号と新しいメンバー番号を指定します。指定できる範囲は 1 ~ 9 です。 show switch ユーザ EXEC コマンドを使用すると、現在のメンバー番号を表示できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload slot stack-member-number	スタック メンバーをリセットします。
ステップ 5	show switch	スタック メンバー番号を確認します。
ステップ 6	copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

スタックメンバープライオリティ値の設定



(注) この作業は、マスターからに限り実行できます。

プライオリティ値をメンバーに割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch stack-member-number priority new-priority-number	メンバーのメンバー番号と新しいプライオリティを指定します。メンバー番号の範囲は 1 ~ 9 です。プライオリティ値の範囲は 1 ~ 15 です。 show switch ユーザ EXEC コマンドを使用すると、現在のプライオリティ値を表示できます。 新しいプライオリティ値はすぐに有効となりますが、現在のマスターまたはスタックがリセットされるまでは現在のマスターに影響しません。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ4	<code>reload slot stack-member-number</code>	メンバーをリセットし、このコンフィギュレーションを適用します。
ステップ5	<code>show switch stack-member-number</code>	メンバー プライオリティ値を確認します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

SWITCH_PRIORITY 環境変数を設定することもできます。詳細については、「[環境変数の制御](#)」(P.3-21) を参照してください。

スタックへの新しいメンバーの割り当て



(注) この作業は、マスターからに限り実行できます。

新しいメンバーをスタックに割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ1	<code>show switch</code>	スタックのサマリー情報を表示します。
ステップ2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>switch stack-member-number provision type</code>	割り当てられたスイッチのメンバー番号を指定します。デフォルトでは、スイッチは割り当てられません。 <i>stack-member-number</i> の範囲は 1 ~ 9 です。スタックに使用されていないメンバー番号を入力します。ステップ 1 を参照してください。 <i>type</i> には、メンバーのモデル番号を入力します。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show running-config</code>	設定のインターフェイスの番号付けが正しいか確認します。
ステップ6	<code>show switch stack-member-number</code>	割り当てられたスイッチのステータスを確認します。 <i>stack-member-number</i> については、ステップ 2 と同じ番号を入力します。
ステップ7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

割り当てられた情報を削除し、エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用する前に、スタックから指定されたスイッチを削除します。

次に、スタック メンバー番号 2 の付いた Catalyst 3750G-12S スイッチをスイッチ スタックに割り当てる例を示します。**show running-config** コマンド出力では、割り当てられたスイッチと関連するインターフェイスを示します。

```
Switch(config)# switch 2 provision WS-C3750G-12S
Switch(config)# end
Switch# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

スタック メンバシップの変更

スタックを分割せずに電源がオンの状態のメンバーを削除するには、次の手順を実行します。

- ステップ 1 新規に作成したスタックの電源をオフにします。
- ステップ 2 新しいスイッチ スタックを、StackWise ポートを通じて元のスイッチ スタックに再度接続します。
- ステップ 3 スイッチの電源をオンにします。

特定のスタック メンバーへの CLI アクセス



(注) この作業は、デバッグだけを目的としており、マスターからに限り実行できます。

remote command {all | stack-member-number} 特権 EXEC コマンドを使用して、すべてまたは特定のメンバーにアクセスできます。スタック メンバー番号の範囲は、1 ~ 9 です。

session stack-member-number 特権 EXEC コマンドを使用して、特定のメンバーにアクセスできます。メンバー番号は、システム プロンプトに付加されます。たとえば、メンバー 2 のシステム プロンプトは Switch-2# となります。また、マスターのシステム プロンプトは Switch# となります。**exit** と入力し、マスターの CLI セッションに戻ります。特定のメンバーに対して使用できるコマンドは、**show** と **debug** だけです。

詳細については、「[インターフェイス コンフィギュレーション モードの使用法](#)」(P.12-12) を参照してください。

スタック情報の表示

特定のメンバーまたはスタックをリセットしたあとで保存した設定変更を表示するには、次の特権 EXEC コマンドを使用します。

表 5-4 スタック情報を表示するコマンド

コマンド	説明
show platform stack manager all	スタック プロトコルバージョンなどのスタック情報をすべて表示します。
show platform stack ports {buffer history}	StackWise ポートのイベントと履歴を表示します。
show switch	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックのサマリー情報を表示します。
show switch stack-member-number	特定のメンバーに関する情報を表示します。
show switch detail	スタック リングに関する詳細情報を表示します。
show switch neighbors	スタックのネイバーを表示します。

表 5-4 スタック情報を表示するコマンド (続き)

コマンド	説明
<code>show switch stack-ports [summary]</code>	スタックのポート情報を表示します。StackWise ケーブル長、スタック リンク ステータス、ループバック ステータスを表示するには、 summary キーワードを使用します。
<code>show switch stack-ring activity [detail]</code>	メンバー単位でスタック リングに送信されるフレーム数を表示します。 detail キーワードを使用すると、メンバー単位でスタック リングに送信されるフレーム数、受信キュー、および ASIC が表示されます。

スタックのトラブルシューティング

- 「手動での StackWise ポートのディセーブル化」(P.5-24)
- 「他のメンバーの起動中に StackWise ポートを再度イネーブルにする方法」(P.5-25)
- 「show switch stack-ports summary コマンド出力の概要」(P.5-25)
- 「ループバック問題の特定」(P.5-26)
- 「切断されている StackWise ケーブルの検出」(P.5-31)
- 「StackWise ポート間の接続障害の解決」(P.5-32)

手動での StackWise ポートのディセーブル化

StackWise ポートがフラッピングし、スタック リングが不安定な状態になっている場合にポートをディセーブルにするには、**switch stack-member-number stack port port-number disable** 特権 EXEC コマンドを入力します。ポートを再度イネーブルにするには、**switch stack-member-number stack port port-number enable** コマンドを入力します。



(注)

switch stack-member-number stack port port-number disable コマンドを使用する場合には十分に注意してください。StackWise ポートをディセーブルにすると、スタックの動作帯域幅が半分になります。

- すべてのメンバーが StackWise ポートを介して接続されていて、ステートがレディの場合、スタックのステートは**完全リング**です。
- 次の場合のスタックのステートは、**部分リング**です。
 - すべてのメンバーが StackWise ポートを介して接続されているが、一部のメンバーのステートがレディではない場合。
 - 一部のメンバーが StackWise ポートを介して接続されていない場合。

switch stack-member-number stack port port-number disable 特権 EXEC コマンドを入力すると、次のようになります。

- スタックのステートが完全リングの場合、StackWise ポートを 1 つだけディセーブルにできます。このとき、次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

- スタックのステートが部分リングの場合、ポートをディセーブルにできません。このとき、次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

他のメンバーの起動中に StackWise ポートを再度イネーブルにする方法

スイッチ 1 の StackWise ポート 1 は、スイッチ 4 のポート 2 に接続されています。ポート 1 がフラッピングしている場合、**switch 1 stack port 1 disable** 特権 EXEC コマンドを使用して、ポート 1 をディセーブルにします。

スイッチ 1 のポート 1 がディセーブルになっていて、スイッチ 1 の電源がオンのままになっている間に、次の手順を実行します。

1. スイッチ 1 のポート 1 とスイッチ 4 のポート 2 の間のスタック ケーブルを取り外します。
2. スタックからスイッチ 4 を削除します。
3. スイッチ 4 の代わりにスイッチを追加し、その追加したスイッチにスイッチ番号 4 を割り当てます。
4. スイッチ 1 のポート 1 とスイッチ 4 (取り替えたスイッチ) のポート 2 の間のケーブルを再度接続します。
5. スイッチ間のリンクを再度イネーブルにします。**switch 1 stack port 1 enable** 特権 EXEC コマンドを入力し、スイッチ 1 のポート 1 をイネーブルにします。
6. スイッチ 4 の電源をオンにします。



注意

スイッチ 1 のポート 1 をイネーブルにする前にスイッチ 4 の電源をオンにすると、スイッチの 1 つがリロードする場合があります。

先にスイッチ 4 の電源をオンにしてしまうと、**switch 1 stack port 1 enable** および **switch 4 stack port 2 enable** 特権 EXEC コマンドを入力して、リンクを起動する必要がある場合があります。

show switch stack-ports summary コマンド出力の概要

スタック メンバー 2 のポート 1 だけがディセーブルになっています。

```
Switch# show switch stack-ports summary
Switch#/  Stack  Neighbor  Cable  Link  Link  Sync  #  In
Port#    Port   Status   Length OK   Active OK  Changes  Loopback
To LinkOK
-----  -
1/1      OK      3        50 cm  Yes   Yes   Yes   1      No
1/2      Down    None     3 m    Yes   No    Yes   1      No
2/1      Down    None     3 m    Yes   No    Yes   1      No
2/2      OK      3        50 cm  Yes   Yes   Yes   1      No
3/1      OK      2        50 cm  Yes   Yes   Yes   1      No
3/2      OK      1        50 cm  Yes   Yes   Yes   1      No
```

表 5-5 show switch stack-ports summary コマンド出力

フィールド	説明
Switch#/Port#	メンバー番号とその StackWise ポート番号です。
Stack Port Status	<ul style="list-style-type: none"> • Absent : StackWise ポートのケーブルが検出されない。 • Down : ケーブルは検出されるが、接続されているネイバーが稼動していないか、StackWise ポートがディセーブルになっている。 • OK : ケーブルが検出され、接続されているネイバーが稼動している。

表 5-5 show switch stack-ports summary コマンド出力 (続き)

フィールド	説明
Neighbor	StackWise ケーブルの他端にあるアクティブ メンバーのスイッチ番号です。
Cable Length	有効な長さは、50 cm、1 m、または 3 m です。 スイッチがケーブル長を検出できない場合、この値は <i>no cable</i> になります。ケーブルが接続されていないか、リンクの信頼性が低いことが考えられます。
Link OK	リンクが安定しているかどうかを示します。 リンクの相手側は、近接スイッチの StackWise ポートです。 <ul style="list-style-type: none"> • No : リンクの相手側がポートから無効なプロトコル メッセージを受信する。 • Yes : リンクの相手側がポートから有効なプロトコル メッセージを受信する。
Link Active	StackWise ポートのステータスがリンクの相手側と同じかどうかを示します。 <ul style="list-style-type: none"> • No : ポートからリンクの相手側にトラフィックを送信できない。 • Yes : ポートからリンクの相手側にトラフィックを送信できる。
Sync OK	<ul style="list-style-type: none"> • No : リンクの相手側が StackWise ポートに有効なプロトコル メッセージを送信しない。 • Yes : リンクの相手側がポートに有効なメッセージを送信する。
# Changes to LinkOK	リンクの相対的な安定性を示します。 短時間に多数の変更を行うと、リンクのフラッピングが発生する場合があります。
In Loopback	<ul style="list-style-type: none"> • No : メンバーの少なくとも 1 つの StackWise ポートに、StackWise ケーブルが接続されている。 • Yes : メンバーの StackWise ポートに、StackWise ケーブルが接続されていない。

ループバック問題の特定

- 「ソフトウェア ループバック」 (P.5-27)
- 「ソフトウェア ループバックの例 : StackWise ケーブルが接続されていない場合」 (P.5-28)
- 「ソフトウェア ループバックの例 : StackWise ケーブルが接続されている場合」 (P.5-28)
- 「ハードウェア ループバック」 (P.5-29)
- 「ハードウェア ループバックの例 : LINK OK イベント」 (P.5-29)
- 「ハードウェア ループバックの例 : LINK NOT OK イベント」 (P.5-30)

ソフトウェア ループバック

3つのメンバーのスタックにおいて、すべてのメンバーが StackWise ケーブルで接続されています。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 OK 3 50 cm Yes Yes Yes 1 No
1/2 OK 2 3 m Yes Yes Yes 1 No
2/1 OK 1 3 m Yes Yes Yes 1 No
2/2 OK 3 50 cm Yes Yes Yes 1 No
3/1 OK 2 50 cm Yes Yes Yes 1 No
3/2 OK 1 50 cm Yes Yes Yes 1 No
```

スイッチ 1 のポート 1 からスタック ケーブルを取り外すと、次のメッセージが表示されます。

```
01:09:55: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 3 has changed to state DOWN
01:09:56: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state DOWN
```

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 Absent None No cable No No No 1 No
1/2 OK 2 3 m Yes Yes Yes 1 No
2/1 OK 1 3 m Yes Yes Yes 1 No
2/2 OK 3 50 cm Yes Yes Yes 1 No
3/1 OK 2 50 cm Yes Yes Yes 1 No
3/2 Down None 50 cm No No No 1 No
```

スイッチ 1 のポート 2 からスタック ケーブルを取り外すと、スタックが分割されます。

スイッチ 2 とスイッチ 3 は、スタック ケーブルで接続された、2つのメンバーを持つスタックになります。

```
Switch# show sw stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
2/1 Down None 3 m No No No 1 No
2/2 OK 3 50 cm Yes Yes Yes 1 No
3/1 OK 2 50 cm Yes Yes Yes 1 No
3/2 Down None 50 cm No No No 1 No
```

スイッチ 1 は、スタンドアロン スイッチになります。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 Absent None No cable No No No 1 Yes
1/2 Absent None No cable No No No 1 Yes
```

ソフトウェア ループバックの例 : StackWise ケーブルが接続されていない場合

Catalyst 3750 スイッチ ポートのステータスは、次のようになります。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 Absent None No cable Yes No Yes 1 Yes
1/2 Absent None No cable Yes No Yes 1 Yes
```

Catalyst 3750-E スイッチ ポートのステータスは、次のようになります。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 Absent None No cable No No No 1 Yes
1/2 Absent None No cable No No No 1 Yes
```

ソフトウェア ループバックの例 : StackWise ケーブルが接続されている場合

- スイッチ 1 のポート 1 のポート ステータスは *Down* で、ケーブルは接続されています。
スイッチ 1 のポート 2 のポート ステータスは *Absent* で、ケーブルは接続されていません。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 Down None 50 Cm No No No 1 No
1/2 Absent None No cable No No No 1 No
```

- 物理ループバックでは、ケーブルでスイッチの両方のスタック ポートを接続します。この構成を使用すると、次のものをテストできます。
 - 正常に稼動しているスイッチに接続されているケーブル
 - 正常に機能しているケーブルが接続されている StackWise ポート

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
2/1 OK 2 50 cm Yes Yes Yes 1 No
2/2 OK 2 50 cm Yes Yes Yes 1 No
```

このポート ステータスは次のことを示しています。

- スイッチ 2 は、スタンドアロン スイッチである。
- ポートはトラフィックの送受信を行うことができる。

ハードウェア ループバック

show platform stack ports buffer 特権 EXEC コマンド出力では、ハードウェア ループバック値が表示されます。

```
Switch# show platform stack ports buffer
Stack Debug Event Data Trace
=====
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
=====

Event Count Stack Port Stack PCS Info Ctrl-Status Loopback Cable
Count Port Info Status IOS / HW length
=====
Event type: LINK OK Stack Port 1
0000000011 1 FF08FF00 860302A5 AA55FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000011 2 FF08FF00 86031805 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
Event type: LINK OK Stack Port 2
0000000012 1 FF08FF00 860302A5 AA55FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000012 2 FF08FF00 86031805 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
Event type: RAC
0000000013 1 FF08FF00 860302A5 AA55FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000013 2 FF08FF00 86031805 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
```

Catalyst 3750v2 メンバーの場合、*Loopback HW* の値が常に *N/A* になります。

Catalyst 3750 メンバーの場合、

- 少なくとも1つのスタックポートにスタックケーブルが接続されている場合、両方のスタックポートの *Loopback HW* の値が *No* になります。
- どちらのスタックポートにもスタックケーブルが接続されていない場合、両方のスタックポートの *Loopback HW* の値が *Yes* になります。

Catalyst 3750-E メンバーの場合、

- 1つのスタックポートにスタックケーブルが接続されている場合、そのスタックポートの *Loopback HW* の値が *No* になります。
- スタックポートにスタックケーブルが接続されていない場合、スタックポートの *Loopback HW* の値が *Yes* になります。

ハードウェア ループバックの例：LINK OK イベント

Catalyst 3750 スイッチの場合：

```
Switch# show platform stack ports buffer
Stack Debug Event Data Trace
=====
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
=====

Event Count Stack Port Stack PCS Info Ctrl-Status Loopback Cable
Count Port Info Status IOS / HW length
=====
Event type: LINK OK Stack Port 1
0000000008 1 FF08FF00 8603F083 55AAFFFF FFFFFFFF 0CE60C10 No /No 50 cm
0000000008 2 FF08FF00 0001DBDF 01000B00 FFFFFFFF 0CE60C10 No /No No cable
```

■ スタックのトラブルシューティング

```
Event type: RAC
0000000009 1 FF08FF00 8603F083 55AAFFFF FFFFFFFF 0CE60C10 No /No 50 cm
0000000009 2 FF08FF00 0001DC1F 02000100 FFFFFFFF 0CE60C10 No /No No cable
```

Catalyst 3750-E スイッチの場合：

```
Switch# show platform stack ports buffer
```

```
Stack Debug Event Data Trace
=====
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
=====

Event Count Stack Port Stack PCS Info Ctrl-Status Loopback Cable
          IOS / HW length
=====
Event type: LINK OK Stack Port 1
0000000153 1 FF01FF00 860351A5 55A5FFFF FFFFFFFF 0CE60C10 No /No 50 cm
0000000153 2 FF01FF00 00017C07 00000000 0000FFFF 0CE60C10 No /No 3 m
Event type: RAC
0000000154 1 FF01FF00 860351A5 55A5FFFF FFFFFFFF 0CE60C10 No /No 50 cm
0000000154 2 FF01FF00 00017C85 00000000 0000FFFF 0CE60C10 No /No 3 m
```

ハードウェア ループバックの例：LINK NOT OK イベント

Catalyst 3750 スイッチの場合：

```
Switch# show platform stack ports buffer
```

```
Stack Debug Event Data Trace
=====
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
=====

Event Count Stack Port Stack PCS Info Ctrl-Status Loopback Cable
          IOS / HW length
=====
Event type: LINK OK Stack Port 2
0000000005 1 FF08FF00 0001FBD3 0801080B EFFFFFFF 0C100CE6 No /No No cable
0000000005 2 FF08FF00 8603E4A9 5555FFFF FFFFFFFF 0C100CE6 No /No 50 cm
Event type: RAC
0000000006 1 FF08FF00 0001FC14 08050204 EFFFFFFF 0C100CE6 No /No No cable
0000000006 2 FF08FF00 8603E4A9 5555FFFF FFFFFFFF 0C100CE6 No /No 50 cm
Event type: LINK NOT OK Stack Port 2
0000000939 1 FF08FF00 00016879 00010000 EFFFFFFF 0C100C14 No /No No cable
0000000939 2 FF08FF00 0001901F 00000000 FFFFFFFF 0C100C14 No /No No cable
Event type: RAC
0000000940 1 FF08FF00 000168BA 00010001 EFFFFFFF 0C100C14 No /No No cable
0000000940 2 FF08FF00 0001905F 00000000 FFFFFFFF 0C100C14 No /No No cable
Event type: LINK OK Stack Port 1
0000000956 1 FF08FF00 86034DAC 5555FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000956 2 FF08FF00 86033431 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
Event type: LINK OK Stack Port 2
0000000957 1 FF08FF00 86034DAC 5555FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000957 2 FF08FF00 86033431 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
Event type: RAC
0000000958 1 FF08FF00 86034DAC 5555FFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
0000000958 2 FF08FF00 86033431 55AAFFFF FFFFFFFF 1CE61CE6 Yes/Yes No cable
```

Catalyst 3750-E スイッチの場合：

```
Switch# show platform stack ports buffer
Stack Debug Event Data Trace
=====
Event type LINK: Link status change
Event type RAC: RAC changes to Not OK
Event type SYNC: Sync changes to Not OK
=====

Event Count Stack Port Stack PCS Info Ctrl-Status Loopback Cable
          Port                               IOS / HW length
=====
Event type: LINK OK Stack Port 1
0000000014 1 FF01FF00 860204A7 5555FFFF 00000000 0CE60CA6 No /No 50 cm
0000000014 2 FF01FF00 85020823 AAAAFFFF 00000000 0CE60CA6 No /No 3 m
Event type: RAC
0000000015 1 FF01FF00 860204A7 5555FFFF 00000000 0CE60CA6 No /No 50 cm
0000000015 2 FF01FF00 85020823 AAAAFFFF 00000000 0CE60CA6 No /No 3 m
Event type: LINK OK Stack Port 2
0000000029 1 FF01FF00 860204A7 5555FFFF 00000000 1CE61CE6 No /No 50 cm
0000000029 2 FF01FF00 86020823 AAAAFFFF 00000000 1CE61CE6 No /No 3 m
Event type: RAC
0000000030 1 FF01FF00 860204A7 5555FFFF 00000000 1CE61CE6 No /No 50 cm
0000000030 2 FF01FF00 86020823 AAAAFFFF 00000000 1CE61CE6 No /No 3 m
Event type: LINK NOT OK Stack Port 1
0000009732 1 FF01FF00 00015B12 5555FFFF A49CFFFF 0C140CE4 No /No 50 cm
0000009732 2 FF01FF00 86020823 AAAAFFFF 00000000 0C140CE4 No /No 3 m
Event type: RAC
0000009733 1 FF01FF00 00015B4A 5555FFFF A49CFFFF 0C140CE4 No /No 50 cm
0000009733 2 FF01FF00 86020823 AAAAFFFF 00000000 0C140CE4 No /No 3 m
Event type: LINK NOT OK Stack Port 2
0000010119 1 FF01FF00 00010E69 25953FFF FFFFFFFF 0C140C14 No /Yes No cable
0000010119 2 FF01FF00 0001D98C 81AAC7FF 0300FFFF 0C140C14 No /No 3 m
Event type: RAC
0000010120 1 FF01FF00 00010EEA 25953FFF FFFFFFFF 0C140C14 No /Yes No cable
0000010120 2 FF01FF00 0001DA0C 81AAC7FF 0300FFFF 0C140C14 No /No 3 m
```

切断されている StackWise ケーブルの検出

StackWise ケーブルですべてのスタック メンバーを接続しています。スイッチ 1 のポート 2 は、スイッチ 2 のポート 1 に接続しています。

メンバーのポート ステータスは次のとおりです。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
          Status To LinkOK
-----
1/1 OK 2 50 cm Yes Yes Yes 0 No
1/2 OK 2 50 cm Yes Yes Yes 0 No
2/1 OK 1 50 cm Yes Yes Yes 0 No
2/2 OK 1 50 cm Yes Yes Yes 0 No
```

スイッチ 1 のポート 2 からケーブルを取り外すと、次のようなメッセージが表示されます。

```
%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state DOWN
```

```
%STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DOWN
```

現在のポート ステータスは次のとおりです。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 OK 2 50 cm Yes Yes Yes 1 No
1/2 Absent None No cable No No No 2 No
2/1 Down None 50 cm No No No 2 No
2/2 OK 1 50 cm Yes Yes Yes 1 No
```

ケーブルの一方の端だけが StackWise ポート（スイッチ 2 のポート 1）に接続しています。

- *Stack Port Status* の値は、スイッチ 1 のポート 2 では *Absent*、スイッチ 2 のポート 1 では *Down* です。
- *Cable Length* の値は、*No cable* です。

問題を診断します。

- スイッチ 1 のポート 2 のケーブル接続を確認します。
- 次の条件に該当する場合、スイッチ 1 のポート 2 でポートまたはケーブルの問題が発生しています。
 - *In Loopback* の値が *Yes* である。
または
 - *Link OK*、*Link Active*、または *Sync OK* の値が *No* である。

StackWise ポート間の接続障害の解決

StackWise ケーブルですべてのメンバーを接続しています。スイッチ 1 のポート 2 は、スイッチ 2 のポート 1 に接続しています。

ポート ステータスは次のとおりです。

```
Switch# show switch stack-ports summary
Switch#/ Stack Neighbor Cable Link Link Sync # In
Port# Port Length OK Active OK Changes Loopback
Status To LinkOK
-----
1/1 OK 2 50 cm Yes Yes Yes 1 No
1/2 Down None 50 cm No No No 2 No
2/1 Down None 50 cm No No No 2 No
2/2 OK 1 50 cm Yes Yes Yes 1 No
```

問題を診断します。

- *Stack Port Status* の値は *Down* です。
- *Link OK*、*Link Active*、および *Sync OK* の値は、*No* です。
- *Cable Length* の値は、*50 cm* です。スイッチはケーブルを検出して、正しく識別しています。

スイッチ 1 のポート 2 とスイッチ 2 のポート 1 間の接続において、コネクタ ピンの少なくとも 1 つで信頼性が低下しています。



CHAPTER 6

スイッチのクラスタ化

この章では、Catalyst 3750 スイッチ クラスタの作成と管理に関する概念と手順を説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

Cisco Network Assistant アプリケーション（以降、Network Assistant）、CLI（コマンドライン インターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を使用してスイッチ クラスタを作成、管理できます。具体的な手順については、オンラインヘルプを参照してください。CLI クラスタ コマンドについては、スイッチ コマンド リファレンスを参照してください。



(注) Network Assistant でもスイッチをクラスタ化できますが、Cisco ではスイッチをグループ化してコミュニティにすることを推奨します。Network Assistant には Cluster Conversion Wizard が用意されており、クラスタを簡単にコミュニティに変換できます。スイッチ クラスタの管理やスイッチ クラスタのコミュニティ変換の概要も含め、Network Assistant に関する詳細は、Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。

この章では、Catalyst 3750 スイッチ クラスタを中心に説明します。クラスタ内に、他のクラスタに対応した Catalyst スイッチが混在している場合の注意事項や制限事項も紹介しますが、これらのスイッチに対するクラスタ機能の詳細な説明は割愛しています。特定の Catalyst プラットフォームにおけるクラスタの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してください。

この章で説明する内容は、次のとおりです。

- 「スイッチ クラスタの概要」(P.6-2)
- 「スイッチ クラスタのプランニング」(P.6-5)
- 「CLI によるスイッチ クラスタの管理」(P.6-17)
- 「SNMP によるスイッチ クラスタの管理」(P.6-18)



(注) 特定のホストまたはネットワークに対してアクセスを制限する場合、**ip http access-class** グローバル コンフィギュレーション コマンドは使用しないことを推奨します。アクセスを制御するには、クラスタ コマンド **switch** を使用するか、または IP アドレスが設定されているインターフェイス上に Access Control List (ACL; アクセス コントロール リスト) を適用します。ACL の詳細については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。

スイッチ クラスタの概要

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

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



(注)

スイッチ クラスタは、スイッチ スタックとは別物です。スイッチ スタックは、スタック ポートを使用して接続された Catalyst 3750 スイッチから構成されています。スイッチ スタックとスイッチ クラスタの相違の詳細については、「[スイッチ クラスタとスイッチ スタック](#)」(P.6-15) を参照してください。

スイッチのクラスタ化には次のような利点があります。

- 物理的な接続や場所に左右されず Catalyst スイッチの管理ができます。スイッチは同じ場所に設置することも、レイヤ 2 またはレイヤ 3 ネットワークを介して設置することもできます (Catalyst 3550、Catalyst 3560、または Catalyst 3750 スイッチを、クラスタのレイヤ 2 の間に設置するレイヤ 3 のルータとして使用している場合)。

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

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

表 6-1 に、クラスタ化に対応している Catalyst スイッチを示します。クラスタ コマンド スイッチになれるスイッチおよびクラスタ メンバー スイッチにしかできないスイッチ、さらに、それらに必要なソフトウェア バージョンも示します。

表 6-1 スイッチ ソフトウェアおよびクラスタへの対応性

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 3750-E または Catalyst 3560-E	12.2(35)SE2 以降	メンバーまたはコマンド スイッチ
Catalyst 3750	12.1(11)AX 以降	メンバーまたはコマンド スイッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバーまたはコマンド スイッチ

表 6-1 スイッチ ソフトウェアおよびクラスタへの対応性 (続き)

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 3550	12.1(4)EA1 以降	メンバーまたはコマンド スイッチ
Catalyst 2975	12.2(46)EX 以降	メンバーまたはコマンド スイッチ
Catalyst 2970	12.1(11)AX 以降	メンバーまたはコマンド スイッチ
Catalyst 2960	12.2(25)FX 以降	メンバーまたはコマンド スイッチ
Catalyst 2955	12.1(12c)EA1 以降	メンバーまたはコマンド スイッチ
Catalyst 2950	12.0(5.2)WC(1) 以降	メンバーまたはコマンド スイッチ
Catalyst 2950 LRE	12.1(11)JY 以降	メンバーまたはコマンド スイッチ
Catalyst 2940	12.1(13)AY 以降	メンバーまたはコマンド スイッチ
Catalyst 3500 XL	12.0(5.1)XU 以降	メンバーまたはコマンド スイッチ
Catalyst 2900 XL (8 MB スイッチ)	12.0(5.1)XU 以降	メンバーまたはコマンド スイッチ
Catalyst 2900 XL (4 MB スイッチ)	11.2(8.5)SA6 (推奨)	メンバー スイッチのみ
Catalyst 1900 および Catalyst 2820	9.00 (-A または -EN) 以降	メンバー スイッチのみ

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS Release 12.1(11)AX 以降を実行している。
- IP アドレスが指定されている。
- Cisco Discovery Protocol (CDP) バージョン 2 がイネーブル (デフォルト) に設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバー スイッチではない。
- 管理 VLAN を介してスタンバイ クラスタ コマンド スイッチに、共通 VLAN を介してクラスタ メンバー スイッチに接続されている。

スタンバイ クラスタ コマンド スイッチの特性

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

- Cisco IOS 12.1(11)AX 以降を実行している。
- IP アドレスが指定されている。
- CDP バージョン 2 がイネーブルに設定されている。

- 管理 VLAN を介してコマンド スイッチに接続されていて、なおかつ他のスタンバイ コマンド スイッチに接続されている。
- 共通 VLAN を介して (クラスタ コマンド スイッチおよびスタンバイ コマンド スイッチを除く) 他のすべてのクラスタ メンバー スイッチに接続されている。
- クラスタ メンバー スイッチとの接続能力を維持するために、クラスタに冗長接続されている。
- 他のクラスタのコマンド スイッチまたはメンバー スイッチではない。



(注) スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同タイプのスイッチでなければなりません。たとえば、クラスタ コマンド スイッチが Catalyst 3750 スイッチの場合、スタンバイ クラスタ コマンド スイッチも Catalyst 3750 スイッチにする必要があります。スタンバイ クラスタ コマンド スイッチの要件については、他のクラスタ対応スイッチのコンフィギュレーション ガイドを参照してください。

候補スイッチおよびクラスタ メンバー スイッチの特性

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

クラスタに加入する候補スイッチは、次の要件を満たしている必要があります。

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



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

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

スイッチ クラスタのプランニング

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

- 「クラスタ候補およびクラスタ メンバーの自動検出」 (P.6-5)
- 「HSRP およびスタンバイ クラスタ コマンド スイッチ」 (P.6-11)
- 「IP アドレス」 (P.6-14)
- 「ホスト名」 (P.6-14)
- 「パスワード」 (P.6-15)
- 「SNMP コミュニティ スtring」 (P.6-15)
- 「スイッチ クラスタとスイッチ スタック」 (P.6-15)
- 「Terminal Access Controller Access Control System Plus (TACACS+) および Remote Authentication Dial In User Service (RADIUS)」 (P.6-17)
- 「LRE プロファイル」 (P.6-17)

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

クラスタ候補およびクラスタ メンバーの自動検出

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



(注)

クラスタ コマンド スイッチを使用してクラスタに対応したスイッチを検出する場合、クラスタ コマンド スイッチ、クラスタ メンバー、またはクラスタ対応スイッチの CDP を無効にしないでください。CDP の詳細については、第 27 章「CDP の設定」を参照してください。

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

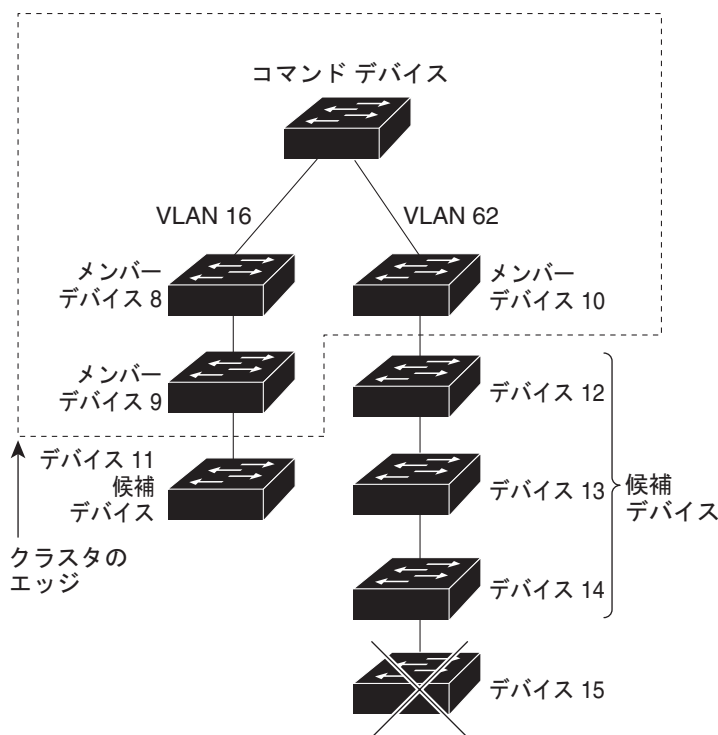
- 「CDP ホップを使用しての検出」 (P.6-6)
- 「CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出」 (P.6-6)
- 「異なる VLAN からの検出」 (P.6-7)
- 「異なる管理 VLAN からの検出」 (P.6-8)
- 「RP による検出」 (P.6-9)
- 「新しくインストールしたスイッチの検出」 (P.6-10)

CDP ホップを使用しての検出

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

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

図 6-1 CDP ホップを使用しての検出

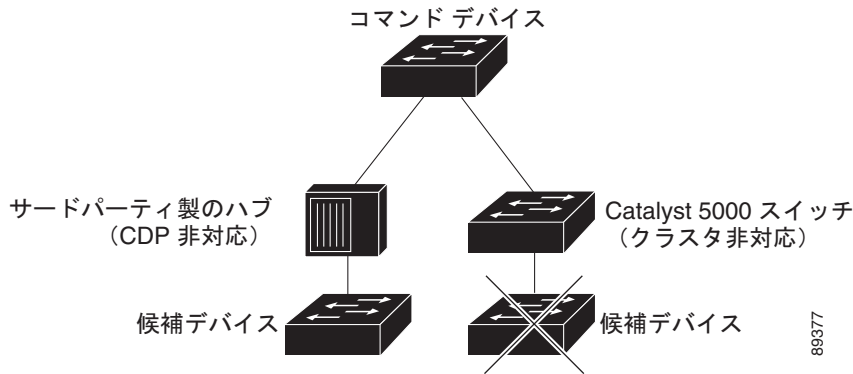


CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

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

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

図 6-2 CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出



異なる VLAN からの検出

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

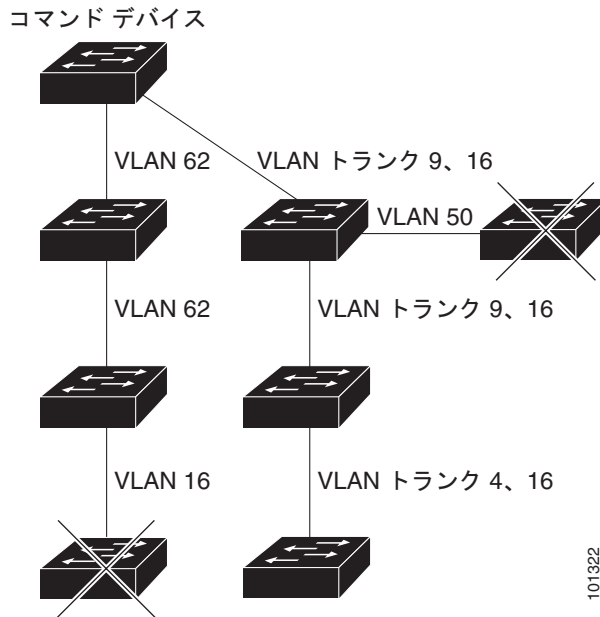
Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL のクラスタ メンバー スイッチは、それぞれの管理 VLAN を介してクラスタ コマンド スイッチに接続している必要があります。管理 VLAN からの検出については、「異なる管理 VLAN からの検出」(P.6-8) を参照してください。VLAN の詳細については、第 14 章「VLAN の設定」を参照してください。



(注)

スイッチ スタック内の VLAN に関するその他の考慮事項については、「スイッチ クラスタとスイッチ スタック」(P.6-15) を参照してください。

図 6-3 異なる VLAN からの検出



異なる管理 VLAN からの検出

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



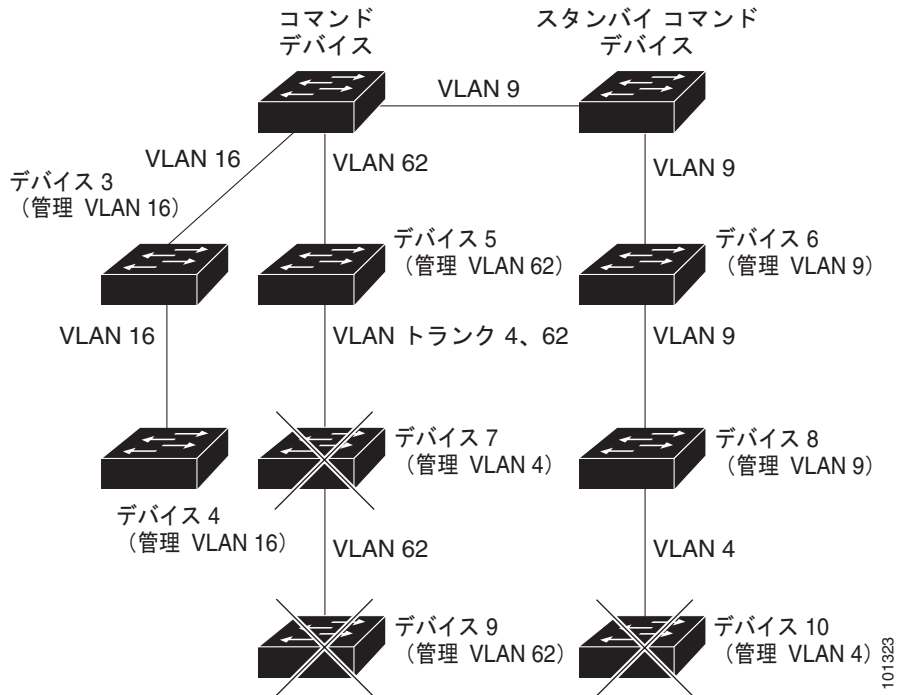
(注)

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

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

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

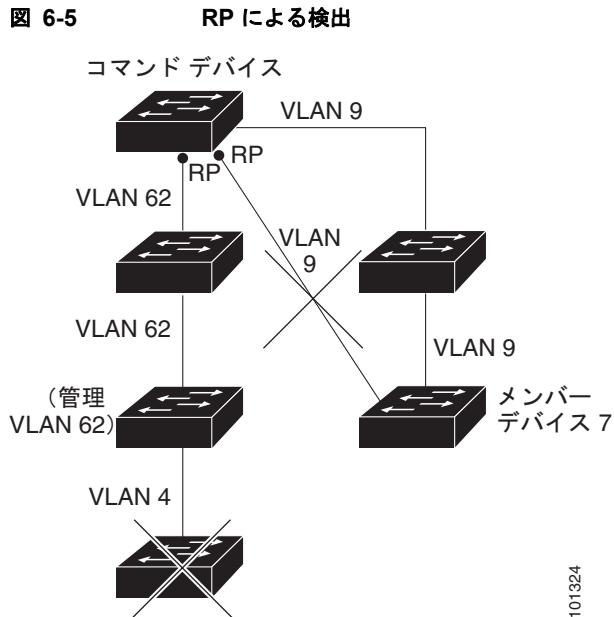
図 6-4 レイヤ3 クラスタ コマンド スイッチを使用して異なる管理 VLAN から検出



RP による検出

Routed Port (RP; ルーテッド ポート) が設定されているクラスタ コマンド スイッチは、RP と同じ VLAN 内の候補スイッチおよびクラスタ メンバー スイッチだけを検出します。RP の詳細については、「ルーテッド ポート」(P.12-5) を参照してください。

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



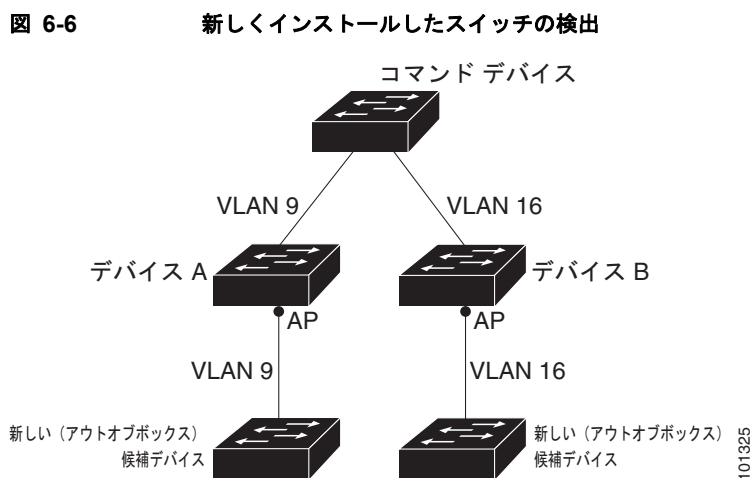
新しくインストールしたスイッチの検出

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

新しいスイッチがクラスタに加入すると、デフォルトの VLAN は即座に上流近接ルータの VLAN に変わります。また、新しいスイッチも自身のアクセス ポートを変更して、その上流近接ルータの VLAN に加わります。

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

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



HSRP およびスタンバイ クラスタ コマンド スイッチ

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

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

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



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

クラスタ スタンバイ グループのスイッチは、HSRP プライオリティに基づいてランク付けされています。グループ内でプライオリティの高いスイッチは、*Active Cluster Command Switch* (AC; アクティブ クラスタ コマンド スイッチ) です。グループ内で次にプライオリティの高いスイッチは、*Standby Cluster Command Switch* (SC; スタンバイ クラスタ コマンド スイッチ) です。クラスタ スタンバイ グループの他のスイッチは、*Passive Cluster Command Switch* (PC; パッシブ クラスタ コマンド スイッチ) です。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時に無効になった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。自動検出の制限事項については、「[クラスタ設定の自動復旧](#)」(P.6-13) を参照してください。HSRP プライオリティ値の変更については、「[HSRP のプライオリティの設定](#)」(P.42-8) を参照してください。クラスタ スタンバイ グループのメンバーおよびルータ冗長構成グループのメンバーのプライオリティ変更には、同じ HSRP `standby priority` インターフェイス コンフィギュレーション コマンドを使用します。



(注) HSRP スタンバイのホールド タイム インターバルは、Hello タイム インターバルの3倍以上必要です。デフォルトの HSRP スタンバイのホールド タイム インターバルは 10 秒です。デフォルトの HSRP スタンバイの Hello タイム インターバルは 3 秒です。スタンバイのホールド タイムおよび Hello タイム インターバルの詳細については、「[HSRP 認証およびタイマーの設定](#)」(P.42-11) を参照してください。

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

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

仮想 IP アドレス

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

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

クラスタ スタンバイ グループに関する他の考慮事項



(注)

スイッチ スタック内のクラスタ スタンバイ グループに関するその他の考慮事項については、「スイッチ クラスタとスイッチ スタック」(P.6-15) を参照してください。

次の要件も満たす必要があります。

- スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同タイプのスイッチでなければなりません。たとえば、クラスタ コマンド スイッチが Catalyst 3750 スイッチの場合、スタンバイ クラスタ コマンド スイッチも Catalyst 3750 スイッチにする必要があります。スタンバイ クラスタ コマンド スイッチの要件については、他のクラスタ対応スイッチのコンフィギュレーション ガイドを参照してください。

スイッチ クラスタに Catalyst 3750 スイッチまたはスイッチ スタックがある場合は、クラスタ コマンド スイッチになります。

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

1 つの HSRP グループをクラスタ スタンバイ グループとルータ冗長構成グループの両方にすることができます。ただし、ルータ冗長構成グループがクラスタ スタンバイ グループになった場合、そのグループ上でのルータ冗長構成はディセーブルになります。CLI を使用すれば、冗長構成を再びイネーブルにすることができます。HSRP およびルータ冗長構成の詳細については、第 42 章「HSRP の設定」を参照してください。

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



(注)

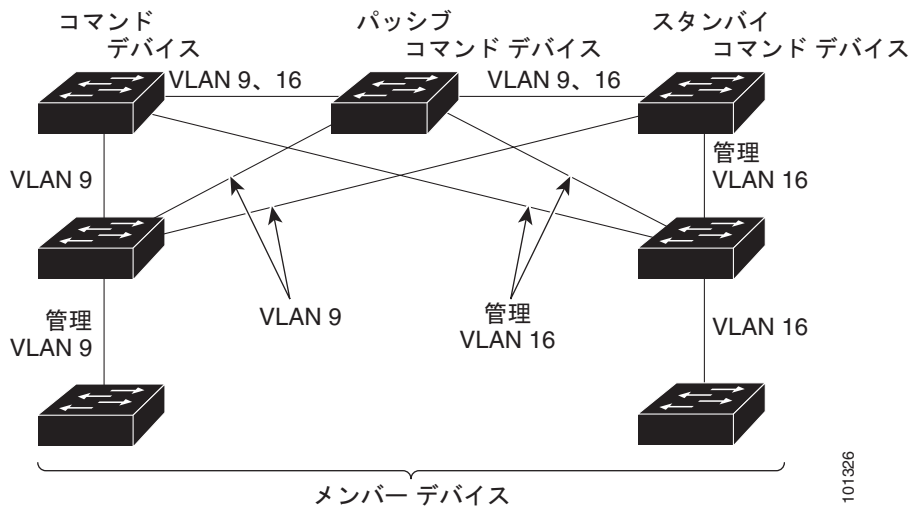
スタンバイ クラスタ コマンド スイッチとして割り当てることができるスイッチ数に制限はありません。ただし、クラスタのスイッチの総数（アクティブ クラスタ コマンド スイッチ、スタンバイ グループ メンバー、およびクラスタ メンバー スイッチを含む）は 16 以内にする必要があります。

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

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

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

図 6-7 スタンバイグループメンバーとクラスタメンバー間の VLAN 接続



クラスタ設定の自動復旧

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

自動検出には次のような制限があります。

- この制限は、Catalyst 2950、Catalyst 3550、Catalyst 3560、Catalyst 3750 のコマンド スイッチおよびスタンバイ クラスタ スイッチを含むクラスタだけに該当します。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチが同時に無効になった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一番高いものがアクティブ クラスタ コマンド スイッチになります。ただし、前回パッシブ スタンバイ クラスタ コマンド スイッチだったため、以前のクラスタ コマンド スイッチはクラスタ設定情報を送信していません。アクティブ クラスタ コマンド スイッチは、スタンバイ クラスタ コマンド スイッチにクラスタ設定情報だけを送信します。そのため、クラスタを再設定する必要があります。
- この制限は、すべてのクラスタに該当します。クラスタ スタンバイ グループに 2 台を超えるスイッチを持つアクティブ クラスタ コマンド スイッチに障害が発生した場合、新しいクラスタ コマンド スイッチは、いかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL のクラスタ メンバー スイッチも検出しません。これらのクラスタ メンバー スイッチをクラスタにもう一度追加する必要があります。

- この制限は、すべてのクラスタに該当します。アクティブ クラスタ コマンド スイッチに障害が発生してダウンしたあと、再びアクティブになった場合、そのスイッチはいかなる Catalyst 1900、Catalyst 2820、および Catalyst 2916M XL クラスタ メンバー スイッチも検出しません。これらのクラスタ メンバー スイッチをクラスタにもう一度追加する必要があります。

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

IP アドレス

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

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

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

IP アドレスの詳細については、第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

ホスト名

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

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

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

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

パスワード

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

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

パスワードの詳細については、「[スイッチへの不正アクセスの防止](#)」(P.9-1) を参照してください。

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

SNMP コミュニティ スtring

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

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

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

スイッチのコミュニティ スtring数とその長さには制限がありません。SNMP およびコミュニティ スtringの詳細については、[第 33 章「SNMP の設定」](#) を参照してください。

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

スイッチ クラスタとスイッチ スタック

スイッチ クラスタには、1 つまたは複数の Catalyst 3750 スイッチ スタックを含めることができます。各スイッチ スタックは、クラスタ コマンド スイッチまたは単一クラスタ メンバーとして機能します。[表 6-2](#) に、スイッチ スタックとスイッチ クラスタとの間の基本的な相違を示します。スイッチ スタックの詳細については、[第 5 章「スイッチ スタックの管理」](#) を参照してください。

表 6-2 スイッチ スタックとスイッチ クラスタの基本的な比較

スイッチ スタック	スイッチ クラスタ
Catalyst 3750 スイッチだけで構成	Catalyst 3750、Catalyst 3550、および Catalyst 2950 スイッチなどのクラスタ対応スイッチで構成
スタック メンバーは StackWise ポートを介して接続	クラスタ メンバーは LAN ポートを介して接続
1 台のスタック マスターを必要とし、8 台までのスタック メンバーをサポート	1 台のクラスタ コマンド スイッチと 15 台までのクラスタ メンバー スイッチが必要

表 6-2 スイッチ スタックとスイッチ クラスタの基本的な比較 (続き)

スイッチ スタック	スイッチ クラスタ
クラスタ コマンド スイッチまたはクラスタ メンバー スイッチになれる	スタック マスターまたはスタック メンバーになれない
スタック マスターが、特定のスイッチ スタック内のすべてのスタック メンバーを完全に管理するシングル ポイント	クラスタ コマンド スイッチが、特定のスイッチ クラスタ内のすべてのクラスタ メンバーの管理の一部を行うシングル ポイント
スタック マスターの障害時に、バックアップ スタック マスターが自動的に決定される	クラスタ コマンド スイッチの障害に備えて、スタンバイ クラスタ コマンド スイッチを事前に割り当てる必要がある
スイッチ スタックは 8 台までのスタック マスターの同時障害に対応可能	スイッチ クラスタは同時に 1 台のみのクラスタ コマンド スイッチの障害に対応可能
スタック メンバーは (スイッチ スタックとして) ネットワーク内で単一の統合型システムとして機能する	クラスタ メンバーは別個の独立したスイッチであり、統合型システムとしては管理されず、機能しない
単一の設定ファイルを使用してスタック メンバーを統合管理	クラスタ メンバーは別個の独立した設定ファイルを保有
スタック レベルとインターフェイス レベルの設定は各スタック メンバーに保存	クラスタ設定は、クラスタ コマンド スイッチとスタンバイ クラスタ コマンド スイッチに保存される
新しいスタック メンバーは自動的にスイッチ スタックに追加される	新しいクラスタ メンバーは手動でスイッチ クラスタに追加される必要がある

スタック メンバーはネットワーク内で、統合型システム (単一のスイッチ スタック) として動作し、レイヤ 2 およびレイヤ 3 プロトコルによって、そのようにネットワークに示されることに留意してください。したがって、スイッチ クラスタは、スイッチ スタックを個別のスタック メンバーとしてでなく、クラスタ メンバーになりうる対象として認識します。個々のスタック メンバーはスイッチ クラスタに加わったり、個別のクラスタ メンバーとして加わったりすることはできません。スイッチ クラスタには 1 台のクラスタ コマンド スイッチが必要であり、15 台までのクラスタ メンバーを保有できるため、クラスタには 16 台までのスイッチ スタック、合計で 144 台のデバイスを含むことができます。

スイッチ スタックのクラスタ設定はスタック マスターを介して行います。

スイッチ クラスタ内にスイッチ スタックを含める場合は、以下のことに留意してください。

- クラスタ コマンド スイッチが Catalyst 3750 スイッチまたはスイッチ スタックでなく、クラスタ メンバー スイッチ スタック内で新しいスタック マスターが選出された場合、スイッチ スタックとクラスタ コマンド スイッチ間に冗長接続がないと、スイッチ スタックとスイッチ クラスタ間の接続が失われます。スイッチ スタックをスイッチ クラスタに追加する必要があります。
- クラスタ コマンド スイッチがスイッチ スタックであり、新しいスタック マスターがクラスタ コマンド スイッチ スタックとクラスタ メンバー スイッチ スタックで同時に選出された場合、スイッチ スタックとクラスタ コマンド スイッチ間に冗長接続がなければ、スイッチ スタック間の接続が失われます。クラスタ コマンド スイッチ スタックを含むスイッチ スタックをクラスタに追加する必要があります。
- すべてのスタック メンバーは、スイッチ クラスタ内のすべての VLAN に対して冗長接続を保持する必要があります。そうしない場合は、新しいスタック マスターが選出されると、新しいスタック マスターで設定されていない VLAN に接続されていたスタック メンバーはスイッチ クラスタへの接続を失います。スタック マスターまたはスタック メンバーの VLAN 設定を変更し、スタック メンバーをスイッチ クラスタに再接続する必要があります。
- クラスタ メンバー スイッチ スタックがリロードし、新しいスタック マスターが選出されると、スイッチ スタックはクラスタ コマンド スイッチとの接続を失います。スイッチ スタックをスイッチ クラスタに再追加する必要があります。

- クラスタ コマンドスイッチ スタックがリロードし、元のスタック マスターが再選出されない場合、スイッチ クラスタ全体を再構築する必要があります。

スイッチ スタックの詳細については、第5章「スイッチ スタックの管理」を参照してください。

Terminal Access Controller Access Control System Plus (TACACS+) および Remote Authentication Dial In User Service (RADIUS)

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

TACACS+ の詳細については、「TACACS+ によるスイッチ アクセスの制御」(P.9-10) を参照してください。RADIUS の詳細については、「RADIUS によるスイッチ アクセスの制御」(P.9-18) を参照してください。

LRE プロファイル

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

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

CLIによるスイッチ クラスタの管理

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

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

```
switch# rcommand 3
```

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

Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチの CLI にアクセスします。そのあと、Cisco IOS コマンドを通常どおりに使用できます。スイッチの Telnet セッションの設定手順については、「パスワード回復のディセーブル化」(P.9-5) を参照してください。



(注) CLI は、最大 16 のスイッチ スタックを持つスイッチ クラスタの作成と維持をサポートしています。スイッチ スタックとスイッチ クラスタの詳細については、「[スイッチ クラスタとスイッチ スタック](#)」(P.6-15) を参照してください。

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

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

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

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



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

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

SNMP によるスイッチ クラスタの管理

スイッチの最初の起動時にセットアップ プログラムを使用して IP 情報を入力し、提示されたコンフィギュレーションを採用した場合、SNMP はイネーブルに設定されています。セットアップ プログラムを使用して IP 情報を入力していない場合は、SNMP はイネーブルではありません。その場合は、「[SNMP の設定](#)」(P.33-6) の説明に従って、SNMP をイネーブルに設定します。Catalyst 1900 および Catalyst 2820 スイッチでは、SNMP はデフォルトでイネーブルに設定されています。

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

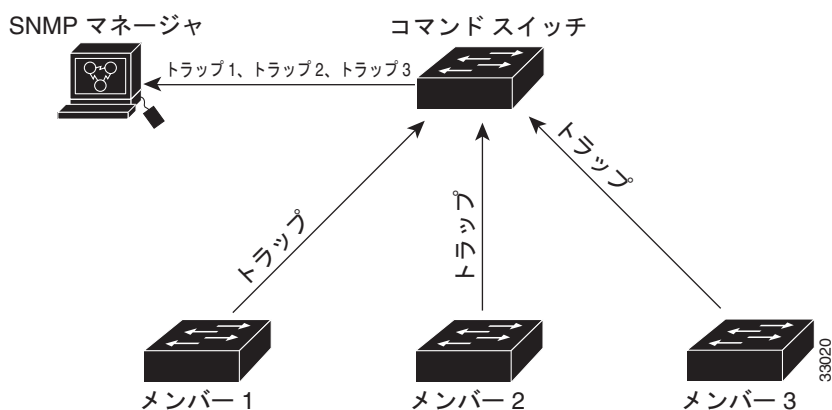


(注) クラスタ スタンバイ グループを設定すると、ユーザが気付かないうちにクラスタ コマンド スイッチが変更される場合があります。クラスタにクラスタ スタンバイ グループを設定している場合は、クラスタ コマンド スイッチとの通信には、最初に設定された Read-Write および Read-Only コミュニティ ストリングを使用してください。

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

クラスタメンバースイッチに専用のIPアドレスとコミュニティストリングが割り当てられている場合、クラスタコマンドスイッチによるアクセスの他に、そのIPアドレスとコミュニティストリングも使用できます。SNMPおよびコミュニティストリングの詳細については、第33章「SNMPの設定」を参照してください。

図 6-8 SNMPによるクラスタ管理





CHAPTER 7

スイッチの管理

この章では、Catalyst 3750 スイッチを管理するための 1 回限りの手順について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

この章で説明する内容は、次のとおりです。

- 「システム日時の管理」 (P.7-1)
- 「システム名とプロンプトの設定」 (P.7-15)
- 「バナーの作成」 (P.7-18)
- 「MAC アドレス テーブルの管理」 (P.7-20)
- 「ARP テーブルの管理」 (P.7-32)

システム日時の管理

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



(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

ここでは、次の設定情報について説明します。

- 「システムクロックの概要」 (P.7-2)
- 「NTP の概要」 (P.7-2)
- 「NTP の設定」 (P.7-4)
- 「手動での日時の設定」 (P.7-11)

システムクロックの概要

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

システムクロックは、次のソースにより設定できます。

- NTP
- 手動設定

システムクロックは、次のサービスに時刻を提供します。

- ユーザの **show** コマンド
- ログおよびデバッグメッセージ

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

システムクロックは、時刻に**信頼性**があるかどうか (つまり、信頼できると見なされるタイムソースによって時刻が設定されているか) を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。設定手順については、「[手動での日時の設定](#)」(P.7-11) を参照してください。

NTP の概要

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

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

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

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

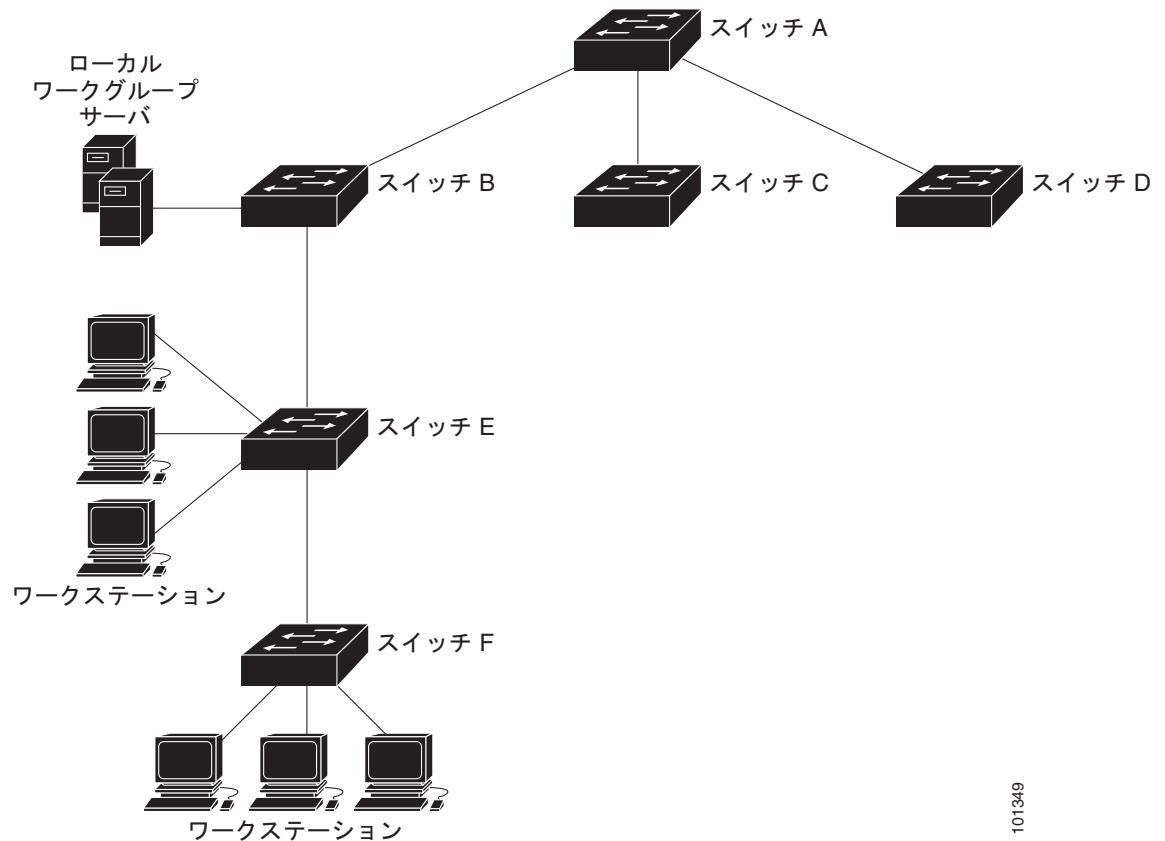
NTP が稼動するデバイス間の通信 (アソシエーション) は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、この場合は、情報の流れは一方にに限られます。

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

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

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

図 7-1 一般的な NTP ネットワークの構成



101349

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

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

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

NTP の設定

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

ここでは、次の設定情報について説明します。

- 「NTP のデフォルト設定」(P.7-4)
- 「NTP 認証の設定」(P.7-5)
- 「NTP アソシエーションの設定」(P.7-6)
- 「NTP ブロードキャスト サービスの設定」(P.7-7)
- 「NTP アクセス制限の設定」(P.7-8)
- 「NTP パケット用の送信元 IP アドレスの設定」(P.7-10)
- 「NTP 設定の表示」(P.7-11)

NTP のデフォルト設定

表 7-1 に、NTP のデフォルト設定を示します。

表 7-1 NTP のデフォルト設定

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

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

NTP 認証の設定

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp authenticate</code>	デフォルトではディセーブルに設定されている NTP 認証機能をイネーブルにします。
ステップ 3	<code>ntp authentication-key number md5 value</code>	<p>認証鍵を定義します。デフォルトでは何も定義されていません。</p> <ul style="list-style-type: none"> <code>number</code> には、鍵の番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 <code>md5</code> は、Message Digest Algorithm 5 (MD5) を使用してメッセージ認証サポートが行われるように指定します。 <code>value</code> には、鍵に対する 8 文字までの任意のストリングを入力します。 <p>スイッチとデバイスの双方がいずれかの認証鍵を持ち、<code>ntp trusted-key key-number</code> コマンドによって鍵番号が指定されていないかぎり、スイッチはデバイスと同期化しません。</p>
ステップ 4	<code>ntp trusted-key key-number</code>	<p>1 つまたは複数の鍵番号（ステップ 3 で定義したもの）を指定します。ピア NTP デバイスは、このスイッチと同期化するため、このスイッチへの NTP パケット内にこの鍵番号を設定しなければなりません。</p> <p>デフォルト設定では、信頼される鍵は定義されていません。</p> <p><code>key-number</code> には、ステップ 3 で定義された鍵を指定します。</p> <p>このコマンドは、スイッチが、信頼されていないデバイスと誤って同期化することを防ぎます。</p>
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

NTP アソシエーションの設定

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

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

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 ntp peer ip-address [version number] [key keyid] [source interface] [prefer] または ntp server ip-address [version number] [key keyid] [source interface] [prefer]	<p>スイッチのシステム クロックをピアに同期化するか、ピアによって同期化する（ピア アソシエーション）ように設定します。</p> <p>または</p> <p>スイッチのシステム クロックをタイム サーバによって同期化する（サーバアソシエーション）ように設定します。</p> <p>ピアまたはサーバアソシエーションはデフォルトでは定義されていません。</p> <ul style="list-style-type: none"> ピア アソシエーションの <i>ip-address</i> には、クロックの同期化を行う、または同期化の対象となるピアの IP アドレスを指定します。サーバアソシエーションでは、クロックの同期化を行うタイム サーバの IP アドレスを指定します。 (任意) <i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は 1 ~ 3 です。デフォルトではバージョン 3 が選択されています。 (任意) <i>keyid</i> には、ntp authentication-key グローバル コンフィギュレーション コマンドで定義された認証鍵を入力します。 (任意) <i>interface</i> には、IP の送信元アドレスを取得するインターフェイスを指定します。デフォルトでは、送信元 IP アドレスは発信インターフェイスから取得します。 (任意) prefer キーワードを指定すると、このピアまたはサーバが同期化を行う優先ピアまたはサーバになります。このキーワードは、ピアとサーバ間の切り替えを減らします。
ステップ3 end	特権 EXEC モードに戻ります。
ステップ4 show running-config	設定を確認します。
ステップ5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アソシエーションの一端しか設定する必要がありません。もう一方のデバイスには自動的にアソシエーションが設定されます。デフォルトの NTP バージョン（バージョン 3）を使用していて、同期化が発生しない場合は、NTP のバージョン 2 を使用してください。インターネット上の多くの NTP サーバは、バージョン 2 で稼動しています。

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

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

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

NTP ブロードキャスト サービスの設定

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

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	NTP ブロードキャスト パケットを送信するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ntp broadcast [version number] [key keyid] [destination-address]</code>	NTP ブロードキャスト パケットをピアに送信するインターフェイスをイネーブルにします。 デフォルトでは、この機能はすべてのインターフェイスでディセーブルです。 <ul style="list-style-type: none"> （任意）<i>number</i> には、NTP のバージョン番号を指定します。指定できる範囲は 1 ～ 3 です。バージョンを指定しなかった場合は、バージョン 3 が使用されます。 （任意）<i>keyid</i> には、ピアにパケットを送信するときに使用する認証鍵を指定します。 （任意）<i>destination-address</i> には、スイッチにクロックを同期化しているピアの IP アドレスを指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 7		次の手順で説明するように、接続されているピアが NTP ブロードキャスト パケットを受信するように設定します。

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

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

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast version 2
```

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

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

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

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

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ntp broadcast client
```

NTP アクセス制限の設定

以降で説明するように、2 つのレベルで NTP アクセスを制御できます。

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

アクセス グループの作成と基本 IP アクセス リストの割り当て

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp access-group {query-only serve-only serve peer} access-list-number</code>	アクセス グループを作成し、基本 IP アクセス リストを割り当てます。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • query-only : NTP 制御クエリーに限り許可します。 • serve-only : 時刻要求に限り許可します。 • serve : 時刻要求と NTP 制御クエリーは許可しますが、スイッチがリモートデバイスと同期化することは許可しません。 • peer : 時刻要求と NTP 制御クエリーを許可し、スイッチがリモートデバイスと同期化することを許可します。 <i>access-list-number</i> には、1 ~ 99 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number permit source [source-wildcard]</code>	アクセス リストを作成します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • permit キーワードを入力すると、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、スイッチへのアクセスが許可されたデバイスの IP アドレスを入力します。 • (任意) <i>source-wildcard</i> には、送信元に適用するワイルドカードビットを入力します。 (注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

複数のアクセス タイプについて送信元 IP アドレスがアクセス リストに一致する場合は、最初のタイプが認可されます。アクセス グループが指定されなかった場合は、すべてのアクセス タイプがすべてのデバイスに認可されます。いずれかのアクセス グループが指定されている場合は、指定されたアクセス タイプに限り認可されます。

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

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

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

特定のインターフェイスでの NTP サービスのディセーブル化

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

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

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

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

NTP パケット用の送信元 IP アドレスの設定

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

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

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

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションに使用する場合は、「[NTP アソシエーションの設定](#)」(P.7-6) に説明したように、`ntp peer` または `ntp server` グローバル コンフィギュレーション コマンド内で `source` キーワードを使用します。

NTP 設定の表示

次の2つの特権 EXEC コマンドを使用して NTP 情報を表示できます。

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



(注)

これらの表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

手動での日時の設定

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



(注)

システム クロックを手動で設定し、スタック マスターに障害が生じて別のスタック メンバーがスタック マスターの役割を再開した場合は、この設定をリセットする必要があります。

ここでは、次の設定情報について説明します。

- 「[システム クロックの設定](#)」(P.7-12)
- 「[日時設定の表示](#)」(P.7-12)
- 「[タイム ゾーンの設定](#)」(P.7-13)
- 「[夏時間の設定](#)」(P.7-14)

システムクロックの設定

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

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

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

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

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

日時設定の表示

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

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

show clock の表示の前にある記号は、次の意味があります。

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

タイムゾーンの設定

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

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

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

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

夏時間の設定

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

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

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

次に、夏時間が 4 月の第 1 日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

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

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

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

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

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

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

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

システム名とプロンプトの設定

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

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

スタック マスターを経由してスタック メンバーにアクセスしている場合は、**session stack-member-number** 特権 EXEC コマンドを使用する必要があります。スタック メンバー番号の範囲は、1 ~ 9 です。このコマンドを使用すると、スタック メンバー番号がシステム プロンプトに付加されます。たとえば、Switch-2# はスタック メンバー 2 の特権 EXEC モードのプロンプトです。Switch は、スイッチ スタックのシステム プロンプトです。

このセクションで使用するコマンドの構文および使用方法の詳細については、Cisco.com のホームページから、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] の順に選択して、『Cisco IOS Configuration Fundamentals Command Reference』および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』を参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.7-16)
- 「システム名の設定」(P.7-16)
- 「DNS の概要」(P.7-16)

デフォルトのシステム名およびプロンプトの設定

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

システム名の設定

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

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

システム名を設定すると、システム プロンプトとしても使用されます。

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

DNS の概要

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

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

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

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」 (P.7-17)
- 「DNS の設定」 (P.7-17)
- 「DNS の設定の表示」 (P.7-18)

DNS のデフォルト設定

表 7-2 に、DNS のデフォルト設定を示します。

表 7-2 DNS のデフォルト設定

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

DNS の設定

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

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

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

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

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

DNS の設定の表示

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

バナーの作成

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

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



(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」(P.7-19)
- 「MoTD ログイン バナーの設定」(P.7-19)
- 「ログイン バナーの設定」(P.7-20)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

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

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

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

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

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

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

次に、前の設定により表示されたバナーの例を示します。

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

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

User Access Verification

Password:
```

ログイン バナーの設定

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

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

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

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

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

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

MAC アドレス テーブルの管理

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

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

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



(注)

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

ここでは、次の設定情報について説明します。

- 「アドレス テーブルの作成」 (P.7-21)
- 「MAC アドレスおよび VLAN」 (P.7-21)
- 「MAC アドレスおよびスイッチ スタック」 (P.7-22)
- 「MAC アドレス テーブルのデフォルト設定」 (P.7-22)
- 「アドレス エージング タイムの変更」 (P.7-22)
- 「ダイナミック アドレス エントリの削除」 (P.7-23)
- 「MAC アドレス変更通知トラップの設定」 (P.7-23)
- 「MAC アドレス移行通知トラップの設定」 (P.7-25)
- 「MAC しきい値通知トラップの設定」 (P.7-27)
- 「スタティック アドレス エントリの追加および削除」 (P.7-28)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.7-29)
- 「VLAN での MAC アドレス ラーニングのディセーブル化」 (P.7-30)
- 「アドレス テーブル エントリの表示」 (P.7-32)

アドレス テーブルの作成

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

有効期間は、スタンドアロン スイッチまたはスイッチ スタックにグローバルに設定されます。ただし、スイッチは VLAN ごとにアドレス テーブルを維持し、STP (スパニング ツリー プロトコル) によって VLAN 単位で有効期間を短縮できます。

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

MAC アドレスおよび VLAN

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

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

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

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

プライベート VLAN の詳細については、第 17 章「プライベート VLAN の設定」を参照してください。

MAC アドレスおよびスイッチ スタック

すべてのスタック メンバーの MAC アドレス テーブルは、同期されています。常に、各スタック メンバーは、各 VLAN に対応するアドレス テーブルの同一のコピーを持っています。アドレスが期限切れになると、そのアドレスはすべてのスタック メンバーのアドレス テーブルから削除されます。スイッチがスイッチ スタックに加入すると、そのスイッチは他のスタック メンバーが学習した各 VLAN に対応するアドレスを受け取ります。スタック メンバーがスイッチ スタックから削除されると、残りのスタック メンバーは、以前のスタック メンバーが学習したアドレスをすべて期限切れにするか削除します。

MAC アドレス テーブルのデフォルト設定

表 7-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 7-3 MAC アドレス テーブルのデフォルト設定

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

アドレス エージング タイムの変更

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

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mac address-table aging-time [0 10-1000000] [vlan vlan-id]</code>	ダイナミック エントリが使用または更新されたあと、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ~ 1000000 秒です。デフォルト値は 300 です。0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることはありません。 <i>vlan-id</i> の有効範囲は、1 ~ 4094 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mac address-table aging-time</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

ダイナミック アドレス エントリの削除

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

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

MAC アドレス変更通知トラップの設定

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

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

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。<code>snmp-server host</code> コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、<code>snmp-server community</code> コマンドを使用し、次に <code>snmp-server host</code> コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3 <code>snmp-server enable traps mac-notification change</code>	スイッチが MAC アドレス変更通知トラップを NMS に送信できるようにします。
ステップ 4 <code>mac address-table notification change</code>	MAC アドレス変更通知機能をイネーブルにします。
ステップ 5 <code>mac address-table notification change [interval value] [history-size value]</code>	<p>トラップ インターバル タイムと履歴テーブルのサイズを入力します。</p> <ul style="list-style-type: none"> (任意) interval value には、NMS に対して生成される各トラップセット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。 (任意) history-size value には、MAC 通知履歴テーブルの最大エン트리数を指定します。指定できる範囲は 0 ~ 500 です。デフォルトは 1 です。
ステップ 6 <code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。

	コマンド	目的
ステップ7	<code>snmp trap mac-notification change {added removed}</code>	インターフェイスの MAC アドレス変更通知トラップをイネーブルにします。 <ul style="list-style-type: none"> このインターフェイスに MAC アドレスが追加されると、トラップをイネーブルにします。 このインターフェイスから MAC アドレスが削除されると、トラップをイネーブルにします。
ステップ8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ9	<code>show mac address-table notification change interface</code> <code>show running-config</code>	設定を確認します。
ステップ10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# snmp trap mac-notification change added
```

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

MAC アドレス移行通知トラップの設定

MAC 移行通知を設定すると、同一の VLAN 内であるポートから別のポートへ MAC アドレスが移行したときに SNMP 通知が生成され、ネットワーク管理システムに送信されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。<code>snmp-server host</code> コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、<code>snmp-server community</code> コマンドを使用し、次に <code>snmp-server host</code> コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification move</code>	スイッチが MAC アドレス移行通知トラップを NMS に送信できるようにします。
ステップ 4	<code>mac address-table notification mac-move</code>	MAC アドレス移行通知機能をイネーブルにします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show mac address-table notification mac-move</code> <code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

MAC しきい値通知トラップの設定

MAC しきい値通知を設定すると、MAC アドレス テーブルしきい値制限に達したか、またはそれを越えたときに、SNMP 通知が生成され、ネットワーク管理システムに送信されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、NMS の名前または IP アドレスを指定します。 SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、informs を指定します。 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト) を使用できません。 <code>community-string</code> には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できませんが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することを推奨します。 <code>notification-type</code> には、mac-notification キーワードを使用します。
ステップ 3	<code>snmp-server enable traps mac-notification threshold</code>	スイッチが MAC しきい値通知トラップを NMS に送信できるようにします。
ステップ 4	<code>mac address-table notification threshold</code>	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ 5	<code>mac address-table notification threshold [limit percentage] [interval time]</code>	<p>MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。</p> <ul style="list-style-type: none"> (任意) <code>limit percentage</code> には、MAC アドレス テーブル使用の割合を指定します。有効な値は 1 ~ 100% です。デフォルト値は 50% です。 (任意) <code>interval time</code> には、通知の間隔の時間を指定します。有効な値は 120 秒以上です。デフォルトは 120 秒です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show mac address-table notification threshold</code> <code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

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

スタティック アドレス エントリの追加および削除

スタティック アドレスには、次の特性があります。

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

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

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

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

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mac address-table static mac-addr vlan vlan-id interface interface-id</code>	MAC アドレス テーブルにスタティック アドレスを追加します。 <ul style="list-style-type: none"> <code>mac-addr</code> には、アドレス テーブルに追加する宛先 MAC ユニキャスト アドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 <code>vlan-id</code> には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。 <code>interface-id</code> には、受信したパケットの転送先インターフェイスを指定します。有効なインターフェイスには、物理ポートまたはポートチャネルがあります。スタティック マルチキャスト アドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャスト アドレスの場合、インターフェイスは同時に 1 つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mac address-table static</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet1/0/1
```

ユニキャスト MAC アドレス フィルタリングの設定

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

この機能を使用する場合は、次の注意事項に従ってください。

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

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

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

- CPU に転送されるパケットもサポートされていません。

- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定すると、最後に入力したコマンドに応じて、スイッチは MAC アドレスをスタティック アドレスとして追加するか、MAC アドレスを持つパケットを廃棄します。2 番めに入力したコマンドは、1 番めのコマンドより優先されます。

たとえば、**mac address-table static mac-addr vlan vlan-id interface interface-id** グローバル コンフィギュレーション コマンドに続けて、**mac address-table static mac-addr vlan vlan-id drop** コマンドを入力すると、スイッチは、送信元または宛先として MAC アドレスを持つパケットを廃棄します。

mac address-table static mac-addr vlan vlan-id drop グローバル コンフィギュレーション コマンドに続けて、**mac address-table static mac-addr vlan vlan-id interface interface-id** コマンドを入力すると、スイッチは、スタティック アドレスとして MAC アドレスを追加します。

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table static mac-addr vlan vlan-id drop	ユニキャスト MAC アドレス フィルタリングをイネーブルにし、スイッチが指定した送信元または宛先ユニキャスト スタティック アドレスを持つパケットを廃棄するように設定します。 <ul style="list-style-type: none"> mac-addr には、送信元または宛先ユニキャスト MAC アドレスを指定します。この MAC アドレスを持つパケットは廃棄されます。 vlan-id には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table static	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次にユニキャスト MAC アドレス フィルタリングをイネーブルにし、送信元または宛先アドレスが c2f3.220a.12f4 であるパケットをスイッチが廃棄するように設定する例を示します。この MAC アドレスを送信元または宛先アドレスとしたパケットを VLAN 4 で受信すると、パケットは廃棄されます。

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

VLAN での MAC アドレス ラーニングのディセーブル化

デフォルトでは、MAC アドレス ラーニングがスイッチのすべての VLAN でイネーブルです。VLAN 上の MAC アドレス ラーニングを制御して、どの VLAN (つまり、ポート) で MAC アドレス ラーニングが可能であるかを指定することにより、使用可能な MAC アドレス テーブル スペースを管理できます。MAC アドレス ラーニングをディセーブルにする前に必ず、ネットワーク トポロジとスイッチ システム設定をよく理解しておいてください。VLAN で MAC アドレス ラーニングをディセーブルにすると、ネットワーク上でフラッドを引き起こす可能性があります。

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

- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) が設定された VLAN で MAC アドレス ラーニングをディセーブルにするときは、注意が必要です。スイッチはレイヤ 2 ドメインのすべての IP パケットをフラッドします。
- MAC アドレス学習は、1 つの VLAN ID (例: **no mac address-table learning vlan 223**) または一連の VLAN ID (例: **no mac address-table learning vlan 1-20, 15**) でディセーブルにすることができます。
- MAC アドレス ラーニングは、2 つのポートを備えた VLAN でのみディセーブルにすることを推奨します。3 つ以上のポートを備えた VLAN で MAC アドレス ラーニングをディセーブルにすると、スイッチが受信するすべてのパケットが VLAN ドメインでフラディングされます。
- スイッチにより内部的に使用される VLAN では、MAC アドレス ラーニングをディセーブルにすることはできません。入力した VLAN ID が内部 VLAN である場合は、スイッチがエラーメッセージを生成し、そのコマンドを拒否します。使用中の内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。
- プライベート VLAN、プライマリ VLAN として設定された VLAN で MAC アドレス ラーニングをディセーブルにしても、MAC アドレスは、プライマリ VLAN に属しており、プライマリ VLAN に複製されたセカンダリ VLAN で学習されます。プライベート VLAN のプライマリ VLAN ではないセカンダリ VLAN で MAC アドレス ラーニングをディセーブルにすると、MAC アドレス ラーニングは、プライマリ VLAN 上で発生する VLAN で実行され、セカンダリ VLAN に複製されます。
- RSPAN VLAN で MAC アドレス ラーニングをディセーブルにすることはできません。その設定は許可されていません。
- セキュア ポートを含む VLAN での MAC アドレス ラーニングをディセーブルにしても、そのポートでは MAC アドレス ラーニングはディセーブルになりません。ポート セキュリティをディセーブルにした場合、設定済みの MAC アドレス ラーニング ステートはイネーブルです。

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

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 no mac address-table learning vlan <i>vlan-id</i>	特定の VLAN で MAC アドレス ラーニングをディセーブルにします。単一の VLAN ID または VLAN ID 範囲を、ハイフンまたはカンマで区切って指定できます。有効な VLAN ID は 1 ~ 4094 です。
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show mac address-table learning [vlan <i>vlan-id</i>]	設定を確認します。
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN で MAC アドレス ラーニングを再度イネーブルにするには、**default mac address-table learning vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用します。また、**mac address-table learning vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して、VLAN で MAC アドレス ラーニングを再度イネーブルにすることもできます。前者の (**default**) コマンドを使用すると、デフォルトの状態に戻るようになるため、設定は **show running-config** コマンドによる出力には含まれません。後者のコマンドを使用すると、設定が **show running-config** 特権 EXEC コマンドの表示に含まれます。

次に、VLAN 200 で MAC アドレス ラーニングをディセーブルにする方法の例を示します。

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

`show mac-address-table learning [vlan vlan-id]` 特権 EXEC コマンドを入力すると、すべての VLAN または特定の VLAN の MAC アドレス ラーニングのステータスを表示することができます。

アドレス テーブル エントリの表示

表 7-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 7-4 MAC アドレス テーブル表示用のコマンド

コマンド	説明
<code>show ip igmp snooping groups</code>	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
<code>show mac address-table address</code>	指定された MAC アドレスに対する MAC アドレス テーブル情報を表示します。
<code>show mac address-table aging-time</code>	すべての VLAN または指定された VLAN のエイジング タイムを表示します。
<code>show mac address-table count</code>	すべての VLAN または指定された VLAN に存在するアドレスの数を表示します。
<code>show mac address-table dynamic</code>	ダイナミック MAC アドレス テーブル エントリのみを表示します。
<code>show mac address-table interface</code>	指定されたインターフェイスに対する MAC アドレス テーブル情報を表示します。
<code>show mac address-table learning</code>	すべての VLAN または特定の VLAN での MAC アドレス ラーニングのステータスを表示します。
<code>show mac address-table notification</code>	MAC 通知パラメータおよび履歴テーブルを表示します。
<code>show mac address-table static</code>	スタティック MAC アドレス テーブル エントリのみを表示します。
<code>show mac address-table vlan</code>	指定された VLAN に対する MAC アドレス テーブル情報を表示します。

ARP テーブルの管理

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

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

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



(注) CLI の手順については、Cisco.com ホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline]) にある Cisco IOS Release 12.2 のマニュアルを参照してください。



CHAPTER 8

SDM テンプレートの設定

Catalyst 3750 スイッチ コマンド リファレンスには、コマンドの構文と使用方法が記載されています。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

- 「SDM テンプレートの概要」(P.8-1)
- 「スイッチ SDM テンプレートの設定」(P.8-5)
- 「SDM テンプレートの表示」(P.8-7)

SDM テンプレートの概要

ネットワークでのスイッチの使用状況に応じて、SDM テンプレートを使用して、特定の機能に対するサポートを最適化するようにスイッチのシステム リソースを設定できます。一部の機能にシステムを最大限に利用させるようにテンプレートを選択したり、デフォルト テンプレートを使用してリソースを均衡化することができます。

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

- **アクセス** : アクセス テンプレートは、多数の ACL に対応できるように ACL のシステム リソースを最大化します。
- **デフォルト** : デフォルト テンプレートは、すべての機能に均等にリソースを割り当てます。
- **ルーティング** : ルーティング テンプレートは、一般的に、ネットワークの中心にあるルータまたはアグリゲータが必要となります。IPv4 ユニキャスト ルーティングに対して、システム リソースを最大化します。
- **VLAN** : VLAN (仮想 LAN) テンプレートは、ルーティングをディセーブルにし、最大数のユニキャスト MAC (メディア アクセス制御) アドレスをサポートします。通常は、レイヤ 2 スイッチ用に選択されます。

さらに、デュアル IPv4/IPv6 テンプレートにより、2 重のスタック環境が実現します。「[デュアル IPv4/IPv6 SDM テンプレート](#)」(P.8-2) を参照してください。

各テンプレートには 2 つのバージョンがあります。デスクトップ テンプレートとアグリゲータ テンプレートです。Catalyst 3750-12S スイッチは、アグリゲータ テンプレートの、より大きなサイズの TCAM を使用することも、標準のデスクトップ テンプレートを使用することもできます。他のすべての Catalyst 3750 スイッチは、デスクトップ テンプレートのみをサポートしています。アグリゲータ スイッチで **desktop** キーワードを入力しなかった場合は、アグリゲータ テンプレートが選択されます。

表 8-1 デスクトップスイッチまたはアグリゲータ スイッチの各テンプレートが許容する機能リソースの概数

リソース	デスクトップ テンプレート				アグリゲータ テンプレート			
	アクセス	デフォルト値	ルーティング	VLAN	アクセス	デフォルト値	ルーティング	VLAN
ユニキャスト MAC アドレス	4 K	6 K	3 K	12 K	6 K	6 K	6 K	12 K
IGMP グループとマルチキャスト ルート	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K
ユニキャスト ルート	6 K	8 K	11 K	0	12 K	12 K	20 K	0
• 直接接続されたホスト	4 K	6 K	3 K	0	6 K	6 K	6 K	0
• 間接ルート	2 K	2 K	8 K	0	6 K	6 K	14 K	0
ポリシーベース ルーティング ACE	512	0	512	0	512	0	512	0
QoS 分類 ACE	512	512	512	512	896	896	512	896
セキュリティ ACE	2 K	1 K	1 K	1 K	4 K	1 K	1 K	1 K
レイヤ 2 VLAN	1 K	1 K	1 K	1 K	1 K	1 K	1 K	1 K

表の最初の 8 行 (ユニキャスト MAC アドレスからセキュリティ ACE (アクセス コントロール エントリ) まで) は、各テンプレートが選択されたときに設定されるハードウェアのおおよその限度を表します。ハードウェア リソースのある部分が一杯の場合は、処理のオーバーフローはすべて CPU に送られ、スイッチのパフォーマンスに重大な影響が出ます。最後の行は、スイッチのレイヤ 2 VLAN の数に関連するハードウェア リソース消費量を計算するための目安です。

デュアル IPv4/IPv6 SDM テンプレート

SDM テンプレートを選択して IP バージョン 6 (IPv6) をサポートすることができます。IPv6 の詳細および IPv6 ルーティングの設定手順については、第 38 章「IP ユニキャスト ルーティングの設定」を参照してください。

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

デュアル IPv4/IPv6 テンプレートを使用することにより、(IPv4 と IPv6 の両方をサポートする) デュアル スタック環境でスイッチを使用できるようになります。デュアル スタック テンプレートを使用すると、各リソースで許容できる TCAM 容量が少なくなります。IPv4 トラフィックのみを転送する場合は、使用しないでください。

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

- デスクトップ デュアル IPv4/IPv6 デフォルト テンプレート: デスクトップ スイッチ (Catalyst 3750-12S を除くすべての Catalyst 3750 スイッチ) 上で、IPv4 のレイヤ 2、マルチキャスト、ルーティング、QoS、ACL、および IPv6 のレイヤ 2、ルーティング、ACL をサポートします。
- デスクトップ デュアル IPv4/IPv6 ルーティング テンプレート: デスクトップ スイッチ (Catalyst 3750-12S を除くすべての Catalyst 3750 スイッチ) 上で、IPv4 のレイヤ 2、マルチキャスト、ルーティング (ポリシーベース ルーティングも含め)、QoS、ACL、および IPv6 のレイヤ 2、ルーティング、ACL をサポートします。
- デスクトップ デュアル IPv4/IPv6 VLAN テンプレート: デスクトップ スイッチ上で IPv4 の基本レイヤ 2、マルチキャスト、QoS、ACL、および IPv6 の基本レイヤ 2 と ACL をサポートします。

- アグリゲータ デュアル IPv4/IPv6 デフォルト テンプレート : Catalyst 3750-12S アグリゲータ スイッチ上で IPv4 のレイヤ 2、マルチキャスト、ルーティング、QoS、ACL、および IPv6 のレイヤ 2 とルーティングをサポートします。
- アグリゲータ デュアル IPv4/IPv6 ルーティング テンプレート : Catalyst 3750-12S アグリゲータ スイッチ上で IPv4 のレイヤ 2、マルチキャスト、ルーティング (ポリシーベース ルーティングを含む)、QoS、ACL、および IPv6 のレイヤ 2、ACL、およびルーティングをサポートします。
- アグリゲータ デュアル IPv4/IPv6 VLAN テンプレート : Catalyst 3750-12S スイッチ上で IPv4 の基本レイヤ 2、マルチキャスト、QoS、ACL、および IPv6 の基本レイヤ 2 をサポートします。



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

表 8-2 デュアル IPv4/IPv6 テンプレートで割り当てられる機能リソースの概数¹

リソース	デスクトップ デフォルト	デスクトップ ルーティング	デスクトッ プ VLAN	アグリゲータ デフォルト	アグリゲータ ルーティング	アグリゲータ VLAN
ユニキャスト MAC アドレス	2 K	1536	8 K	2 K	2K	8 K
IPv4 IGMP グループとマルチキャスト ルート	1 K	1 K	1 K	1 K	1 K	0
IPv4 ユニキャスト ルートの総数	3 K	2816	0	3 K	8 K	0
• 直接接続された IPv4 ホスト	2 K	1536	0	2 K	2K	0
• 間接的な IPv4 ルート	1 K	1280	0	1 K	6 K	1 K
IPv6 マルチキャスト グループ	1 K	1152	1 K	1 K	2176	1 K
IPv6 ユニキャスト ルートの総数	3 K	2816	0	3 K	8 K	0
• 直接接続された IPv6 アドレス	2 K	1536	0	2 K	2K	0
• 間接的な IPv6 ユニキャスト ルート	1 K	1280	0	1 K	6 K	0
IPv4 ポリシーベース ルーティング ACE	0	256	0	0	512	0
IPv4 または MAC QoS ACE (総数)	512	512	512	876	896	876
IPv4 または MAC セキュリティ ACE (総数)	1 K	512	1 K	512	1 K	1 K
IPv6 PBR ACE ²	0	255	0	0	510	0
IPv6 QoS ACE	510	510	510	876	510	876
IPv6 セキュリティ ACE	510	510	510	876	510	876

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

SDM テンプレートとスイッチ スタック

すべてのスタック メンバーは、スタック マスターに格納されているものと同じ SDM デスクトップまたはアグリゲータ テンプレートを使用します。新たなスイッチがスタックに追加されると、スイッチのコンフィギュレーション ファイルや VLAN データベース ファイルと同様に、スタック マスターに格納された SDM コンフィギュレーション ファイルによって、個々のスイッチに設定されているテンプレートが上書きされます。スタッキングの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

スタック マスターがデスクトップ スイッチで、アグリゲータ テンプレートを稼動する Catalyst 3750-12S がスタック メンバーとして追加された場合、スタックはスタック マスター上で選択されたデスクトップ テンプレートを使用して動作します。この結果、Catalyst 3750-12S 上の TCAM エントリ の数がデスクトップ テンプレート サイズを超えた場合には、Catalyst 3750-12S 上の設定は失われてしまいます。

スタック マスターがアグリゲータ テンプレートを使用する Catalyst 3750-12S スイッチで、新たなスタック メンバーが Catalyst 3750-12S ではない場合は、スタック メンバーはスタック マスター上で稼動するテンプレートをサポートできません。スタックへの参加を試みるスイッチは SDM 不一致モードとなり、スタック マスターは SDM テンプレートの変更は行いません。さらに、スイッチは正常に機能するスタックのメンバーになることはできません。

スタック マスターが Catalyst 3750-12S の場合、テンプレートを変更すると次の結果を引き起こすことがあります。

- テンプレートをアグリゲータ テンプレートからデスクトップ テンプレートへ変更し、スイッチをリロードすると、スタック全体が、選択されたデスクトップ テンプレートを使用して動作します。このため、TCAM エントリ の数がデスクトップ テンプレートのサイズを超えた場合には、設定が失われることがあります。
- テンプレートをデスクトップ テンプレートからアグリゲータ テンプレートに変更し、スイッチをリロードした場合、スタックに属していたデスクトップ スイッチは SDM 不一致モードになります。これが生じた場合は、スタック メンバーが SDM 不一致モードになったことを通知し、そのスイッチを不一致モードから脱却させるための手順を示した Syslog メッセージがスタック マスターに送信されます。

show switch 特権 EXEC コマンドを使用すると、スタック メンバーが SDM 不一致モードになっているかどうかを確認できます。この例は、SDM 不一致が存在するときの **show switch** 特権 EXEC コマンドの出力を示しています。

```
Switch# show switch
Switch# Role      Mac Address      Priority    Current
-----
*2      Master    000a.fdfd.0100   5          Ready
4       Member    0003.fd63.9c00   5          SDM Mismatch
```

次は、スタック マスターにスタック メンバーが SDM 不一致モードであることを通知する Syslog メッセージの一例です。

```
2d23h:%STACKMGR-6-SWITCH_ADDED_SDM:Switch 2 has been ADDED to the stack (SDM_MISMATCH)

2d23h:%SDM-6-MISMATCH_ADVISE:
2d23h:%SDM-6-MISMATCH_ADVISE:
2d23h:%SDM-6-MISMATCH_ADVISE:System (#2) is incompatible with the SDM
2d23h:%SDM-6-MISMATCH_ADVISE:template currently running on the stack and
2d23h:%SDM-6-MISMATCH_ADVISE:will not function unless the stack is
2d23h:%SDM-6-MISMATCH_ADVISE:downgraded.Issuing the following commands
2d23h:%SDM-6-MISMATCH_ADVISE:will downgrade the stack to use a smaller
2d23h:%SDM-6-MISMATCH_ADVISE:compatible desktop SDM template:
```

```
2d23h:%SDM-6-MISMATCH_ADVICE:
2d23h:%SDM-6-MISMATCH_ADVICE: "sdm prefer vlan desktop"
2d23h:%SDM-6-MISMATCH_ADVICE: "reload"
```

スイッチ SDM テンプレートの設定

ここでは、次の設定情報について説明します。

- 「デフォルトの SDM テンプレート」(P.8-5)
- 「SDM テンプレートの設定時の注意事項」(P.8-5)
- 「SDM テンプレートの設定」(P.8-6)

デフォルトの SDM テンプレート

デスクトップ スイッチのデフォルト テンプレートは、デフォルトのデスクトップ テンプレートです。Catalyst 3750-12S のデフォルト テンプレートは、デフォルト アグリゲータ テンプレートです。

SDM テンプレートの設定時の注意事項

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

- SDM テンプレートを選択して設定する場合、設定した内容を有効にするには、スイッチをリロードする必要があります。
- **sdm prefer vlan** グローバル コンフィギュレーション コマンドは、ルーティングしないレイヤ 2 スイッチングのスイッチでだけ使用します。VLAN テンプレートを使用している場合は、ルーティング エントリ用のシステム リソースは予約されないため、ルーティングはソフトウェアを通じて実行されます。この場合、CPU に負荷がかかり、ルーティングのパフォーマンスが大幅に低下します。
- スイッチでのルーティングをイネーブルにしない場合は、ルーティング テンプレートを使用しないでください。**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用すると、他の機能がルーティング テンプレート内のユニキャスト ルーティングに割り振られたメモリを使用するのを防ぐことができます。
- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 機能を設定しようとする、警告メッセージが生成されます。
- デュアル スタック テンプレートを使用すると、リソースごとに使用可能な TCAM 容量が少なくなるため、IPv4 トラフィックのみを転送する場合は、このテンプレートを使用しないでください。

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>sdm prefer {access default dual-ipv4-and-ipv6 {default routing vlan} routing vlan} [desktop]</code>	<p>スイッチで使用する SDM テンプレートを指定します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • access : ACL のシステム リソースを最大化します。 • default : すべての機能に対してリソースを均衡化します。 <p>desktop キーワードを使用してデフォルト デスクトップ テンプレートが設定されている Catalyst 3750-12S スイッチ上でのみ表示されます (<code>no sdm prefer</code> コマンドを使用して、デスクトップ スイッチをデフォルト デスクトップ テンプレートに設定するか、アグリゲータ スイッチをデフォルト アグリゲータ テンプレートに設定できます)。</p> <ul style="list-style-type: none"> • dual-ipv4-and-ipv6 : IPv4 と IPv6 ルーティングを両方サポートするテンプレートを選択します。 <ul style="list-style-type: none"> – default : IPv4/IPv6 のレイヤ 2 およびレイヤ 3 機能を均衡化します。 – routing : IPv4 ポリシーベース ルーティングを含む IPv4 および IPv6 ルーティングを最大限に使用します。 – vlan : IPv4/IPv6 VLAN を最大限に使用します。 • routing : スイッチ上で IPv4 ルーティングを最適化します。 • vlan : ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。 • desktop : Catalyst 3750-12S スイッチ上でのみサポートされます。スイッチを、デフォルト、ルーティング、VLAN デスクトップのいずれかのテンプレートに設定します。 <p>スイッチをデフォルト テンプレートに設定するには、<code>no sdm prefer</code> コマンドを使用します。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>reload</code>	OS (オペレーティング システム) をリロードします。

システムの再起動後、`show sdm prefer` 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。`reload` 特権 EXEC コマンドの前に `show sdm prefer` コマンドを入力すると、`show sdm prefer` コマンドによって、現在使用しているテンプレートと、再起動後にアクティブになるテンプレートが表示されます。

次は、テンプレートを変更後にスイッチをリロードしなかった場合の出力表示の一例です。

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

```

number of unicast mac addresses:          3K
number of igmp groups + multicast routes: 1K
number of unicast routes:                11K
  number of directly connected hosts:     3K
  number of indirect routes:              8K
number of qos aces:                       512
number of security aces:                  1K

```

On next reload, template will be "aggregate routing" template.

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

次の例は、スイッチにルーティング テンプレート（デスクトップ スイッチの場合はデスクトップ ルーティング テンプレート、Catalyst 3750-12S の場合はアグリゲータ ルーティング テンプレート）を設定する方法を示しています。

```

Switch(config)# sdm prefer routing
Switch(config)# end
Switch# reload
Proceed with reload?[confirm]

```

次の例は、Catalyst 3750-12S スイッチのデスクトップ ルーティング テンプレートを設定する方法を示しています。

```

Switch(config)# sdm prefer routing desktop
Switch(config)# end
Switch# reload
Proceed with reload?[confirm]

```

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

```

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

```

SDM テンプレートの表示

アクティブ テンプレートを表示するには、パラメータを指定せずに **show sdm prefer** 特権 EXEC コマンドを使用します。

指定のテンプレートがサポートしているリソース数を表示するには、**show sdm prefer [access | default | dual-ipv4-and-ipv6 {default | vlan | routing } vlan [desktop]]** 特権 EXEC コマンドを使用します。



(注)

desktop キーワードは、Catalyst 3750-12S アグリゲータ スイッチでのみ使用できます。

次は、使用中のテンプレートを表示する **show sdm prefer** コマンドの出力例です。

```

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

number of unicast mac addresses:          6K
number of igmp groups + multicast routes: 1K
number of unicast routes:                8K

```

```

    number of directly connected hosts:      6K
    number of indirect routes:              2K
    number of policy based routing aces:     0
    number of qos aces:                    512
    number of security aces:                1K

```

次は、アグリゲータ スイッチに入力された **show sdm prefer routing** コマンドの出力例です。

```

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

number of unicast mac addresses:           6K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 20K
    number of directly connected hosts:    6K
    number of indirect routes:             14K
number of policy based routing aces:      512
number of qos aces:                       512
number of security aces:                   1K

```

次は、デスクトップ スイッチに入力された **show sdm prefer routing** コマンドの出力例です。

```

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

number of unicast mac addresses:           3K
number of igmp groups + multicast routes: 1K
number of unicast routes:                 11K
    number of directly connected hosts:    3K
    number of indirect routes:             8K
number of policy based routing aces:      512
number of qos aces:                       512
number of security aces:                   1K

```

次は、デスクトップ スイッチに入力された **show sdm prefer dual-ipv4-and-ipv6 default** コマンドの出力例です。

```

Switch# show sdm prefer dual-ipv4-and-ipv6 default
"desktop IPv4 and IPv6 default" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:           2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:             3K
    number of directly-connected IPv4 hosts: 2K
    number of indirect IPv4 routes:         1K
number of IPv6 multicast groups:           1K
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:    1K
number of IPv4 policy based routing aces:  0
number of IPv4/MAC qos aces:               512
number of IPv4/MAC security aces:          1K
number of IPv6 policy based routing aces:  0
number of IPv6 qos aces:                   510
number of IPv6 security aces:              510

```




CHAPTER 9

スイッチ ベース認証の設定

この章では、Catalyst 3750 スイッチにスイッチ ベース認証を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

この章で説明する内容は、次のとおりです。

- 「スイッチへの不正アクセスの防止」(P.9-1)
- 「特権 EXEC コマンドへのアクセスの保護」(P.9-2)
- 「TACACS+ によるスイッチ アクセスの制御」(P.9-10)
- 「RADIUS によるスイッチ アクセスの制御」(P.9-18)
- 「Kerberos によるスイッチ アクセスの制御」(P.9-40)
- 「スイッチのローカル認証および許可の設定」(P.9-45)
- 「SSH のためのスイッチの設定」(P.9-46)
- 「SSL HTTP のためのスイッチの設定」(P.9-51)
- 「SCP のためのスイッチの設定」(P.9-57)

スイッチへの不正アクセスの防止

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

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

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。詳細については、「[特権 EXEC コマンドへのアクセスの保護](#)」(P.9-2) を参照してください。
- 追加のセキュリティ レイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。詳細については、「[ユーザ名とパスワードのペアの設定](#)」(P.9-7) を参照してください。

- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティ サーバ上のデータベースに保存できます。これにより、複数のネットワーク デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。詳細については、「TACACS+によるスイッチ アクセスの制御」(P.9-10) を参照してください。
- 失敗したログインおよび成功しなかったログインを記録するログイン拡張機能をイネーブルにすることもできます。この機能を使用すると、ログインの失敗が設定した回数に達した場合、それ以降のログインを防止するようにも設定できます。詳細については、次の URL の『Cisco IOS Login Enhancements』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

特権 EXEC コマンドへのアクセスの保護

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



(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Security Command Reference』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

ここでは、次の設定情報について説明します。

- 「デフォルトのパスワードおよび権限レベル設定」(P.9-3)
- 「スタティック イネーブル パスワードの設定または変更」(P.9-3)
- 「暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護」(P.9-4)
- 「パスワード回復のディセーブル化」(P.9-5)
- 「端末回線に対する Telnet パスワードの設定」(P.9-6)
- 「ユーザ名とパスワードのペアの設定」(P.9-7)
- 「複数の権限レベルの設定」(P.9-8)

デフォルトのパスワードおよび権限レベル設定

表 9-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 9-1 デフォルトのパスワードおよび権限レベル設定

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>enable password password</code>	<p>特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>デフォルトでは、パスワードは定義されません。</p> <p><code>password</code> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符 (?) は、パスワードを作成する場合に、疑問符の前に <code>Ctrl-v</code> を入力すれば使用できます。たとえば、パスワード <code>abc?123</code> を作成するときは、次のようにします。</p> <p><code>abc</code> を入力します。</p> <p><code>Ctrl-v</code> を入力します。</p> <p><code>?123</code> を入力します。</p> <p>システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に <code>Ctrl-v</code> を入力する必要はなく、パスワードのプロンプトにそのまま <code>abc?123</code> と入力できます。</p>
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4 <code>show running-config</code>	設定を確認します。
ステップ 5 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p> <p>イネーブル パスワードは暗号化されず、スイッチのコンフィギュレーション ファイル内では読み取ることができる状態です。</p>

パスワードを削除するには、`no enable password` グローバル コンフィギュレーション コマンドを使用します。

次に、イネーブルパスワードを `11u2c3k4y5` に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password 11u2c3k4y5
```

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

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

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

enable secret コマンドは **enable password** コマンドに優先します。2 つのコマンドが同時に有効になることはありません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	enable password [level level] {password encryption-type encrypted-password} または enable secret [level level] {password encryption-type encrypted-password}	<p>特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>または</p> <p>シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。</p> <ul style="list-style-type: none"> （任意）<i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルトレベルは 15 です（特権 EXEC モード権限）。 <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できませんが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 （任意）<i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。 <p>(注) 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再び特権 EXEC モードを開始できません。暗号化されたパスワードが失われた場合は、どのような方法でも回復できません。</p>

	コマンド	目的
ステップ 3	<code>service password-encryption</code>	(任意) パスワードを定義するとき、または設定を保存するときに、パスワードを暗号化します。 暗号化によって、コンフィギュレーション ファイル内のパスワードが読み取り不能になります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したら、そのレベルでアクセスする必要のあるユーザだけにそのパスワードを渡してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の権限レベルの設定」(P.9-8)を参照してください。

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

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

次に、権限レベル 2 に対して暗号化パスワード `1FaD0$Xyti5Rkls3LoyxzS8` を設定する例を示します。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

パスワード回復のディセーブル化

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

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



(注)

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP (VLAN トランッキング プロトコル) トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」(P.49-3)を参照してください。

パスワードの回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no service password-recovery	パスワードの回復をディセーブルにします。 この設定は、フラッシュ メモリの中で、ブート ロードおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル システムには含まれません。また、ユーザがアクセスすることはできません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show version	コマンド出力の最後の数行をチェックすることによって、設定を確認します。

パスワードの回復を再びイネーブルにする場合は、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。



(注)

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

端末回線に対する Telnet パスワードの設定

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

スイッチを Telnet アクセス用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアを備えた PC またはワークステーションとスイッチのコンソール ポートを接続します。 コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトが表示されるまで、Return キーを何回か押す必要があります。
ステップ 2	enable password <i>password</i>	特権 EXEC モードを開始します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	line vty 0 15	Telnet セッション (回線) の数を設定し、ライン コンフィギュレーション モードを開始します。 コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。

コマンド	目的
ステップ5 <code>password password</code>	1 つまたは複数の回線に対応する Telnet パスワードを入力します。 <code>password</code> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ7 <code>show running-config</code>	設定を確認します。 コマンド <code>line vty 0 15</code> の下にパスワードが表示されます。
ステップ8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

パスワードを削除するには、`no password` グローバル コンフィギュレーション コマンドを使用します。
次に、Telnet パスワードを `let45me67in89` に設定する例を示します。

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

ユーザ名とパスワードのペアの設定

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

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムでは、ログイン ユーザ名とパスワードが要求されます。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>username name [privilege level]</code> <code>{password encryption-type password}</code>	各ユーザのユーザ名、権限レベル、パスワードを入力します。 <ul style="list-style-type: none"> <code>name</code> には、ユーザ ID を 1 ワードで指定します。スペースおよび引用符は使用できません。 (任意) <code>level</code> には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 <code>encryption-type</code> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 <code>password</code> には、ユーザがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<code>username</code> コマンドの最後のオプションとして指定します。
ステップ3 <code>line console 0</code> または <code>line vty 0 15</code>	ライン コンフィギュレーション モードを開始し、コンソール ポート (回線 0) または VTY 回線 (回線 0 ~ 15) を設定します。

	コマンド	目的
ステップ4	login local	ログイン時のローカルパスワードチェックをイネーブルにします。認証は、ステップ2で指定されたユーザ名に基づきます。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show running-config	設定を確認します。
ステップ7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、**no username name** グローバル コンフィギュレーション コマンドを使用します。パスワードチェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアはデフォルトで、2種類のパスワードセキュリティモードを使用します。ユーザ EXEC および特権 EXEC です。モードごとに、コマンドの階層レベルを16まで設定できます。複数のパスワードを設定することにより、さまざまなユーザグループに対して特定のコマンドへのアクセスを許可できます。

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

ここでは、次の設定情報について説明します。

- 「コマンドの権限レベルの設定」(P.9-8)
- 「回線に対するデフォルトの権限レベルの変更」(P.9-9)
- 「権限レベルへのログインおよび終了」(P.9-10)

コマンドの権限レベルの設定

コマンドモードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	privilege mode level level command	コマンドの権限レベルを設定します。 <ul style="list-style-type: none"> • <i>mode</i> には、グローバル コンフィギュレーション モードの場合は configure を、EXEC モードの場合は exec を、インターフェイス コンフィギュレーション モードの場合は interface を、ライン コンフィギュレーション モードの場合は line をそれぞれ入力します。 • <i>level</i> に指定できる範囲は0～15です。レベル1が通常のユーザ EXEC モード権限です。レベル15は、enable パスワードによって許可されるアクセス レベルです。 • <i>command</i> には、アクセスを制限したいコマンドを指定します。

コマンド	目的
ステップ3 <code>enable password level level password</code>	権限レベルに対応するイネーブルパスワードを指定します。 <ul style="list-style-type: none"> <code>level</code> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 <code>password</code> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ5 <code>show running-config</code> または <code>show privilege</code>	設定を確認します。 <code>show running-config</code> コマンドはパスワードとアクセス レベルの設定を表示します。 <code>show privilege</code> コマンドは、権限レベルの設定を表示します。
ステップ6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

`configure` コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして `SecretPswd14` を定義する例を示します。

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

回線に対するデフォルトの権限レベルの変更

回線に対するデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>line vty line</code>	アクセスを制限する仮想端末回線を選択します。
ステップ3 <code>privilege level level</code>	回線のデフォルトの権限レベルを変更します。 <code>level</code> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、 <code>enable</code> パスワードによって許可されるアクセス レベルです。
ステップ4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ5 <code>show running-config</code> または <code>show privilege</code>	設定を確認します。 <code>show running-config</code> コマンドはパスワードとアクセス レベルの設定を表示します。 <code>show privilege</code> コマンドは、権限レベルの設定を表示します。
ステップ6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	enable level	指定した権限レベルにログインします。 <i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ 2	disable level	指定した権限レベルを終了します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

TACACS+ によるスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus (TACACS+) をイネーブルにして設定する方法について説明します。TACACS+ は、詳細なアカウント情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication, Authorization, Accounting (AAA; 認証、許可、アカウント情報) 機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用しなければなりません。



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

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」 (P.9-10)
- 「TACACS+ の動作」 (P.9-12)
- 「TACACS+ の設定」 (P.9-13)
- 「TACACS+ 設定の表示」 (P.9-18)

TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティアプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼動する TACACS+ デモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。



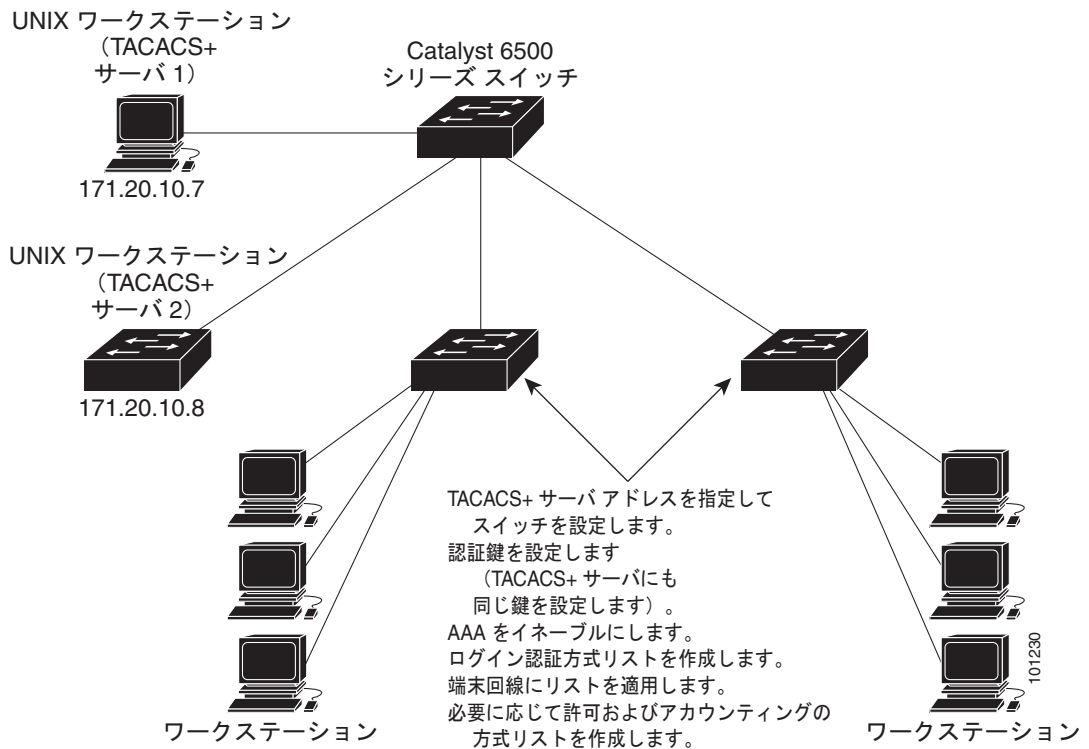
(注)

スイッチ スタックと TACACS+ サーバとの間では冗長接続を確立することを推奨します。これは、接続されているスタック メンバーがスイッチ スタックから削除された場合でも、TACACS+ サーバがアクセス可能なまま維持されるようにする上で役立ちます。

TACACS+ は、個別のモジュール型認証、許可、およびアカウントिंग機能を備えています。TACACS+ では、単一のアクセス制御サーバ (TACACS+ デモン) が各サービス (認証、許可、およびアカウントिंग) を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他のシスコ製ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。ネットワーク アクセス サーバは、個々のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します (図 9-1 を参照)。

図 9-1 一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

認証機能は、ユーザとの対話を実行します (たとえば、ユーザ名とパスワードが入力されたあと、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します)。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセス制御、セッション期間、プロトコル サポートの設定といった、ユーザセッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド (PPP など)、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼動するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。
TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。
2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
 - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
 - REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
 - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
 - CONTINUE：ユーザは、さらに認証情報の入力を求められます。
 認証後、スイッチで許可がイネーブлになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛てのアトリビュートの形式でデータが含まれています。
 - Telnet、Secure Shell (SSH; セキュア シェル)、rlogin、または特権 EXEC サービス
 - 接続パラメータ (ホストまたはクライアントの IP アドレス、アクセスリスト、およびユーザ タイムアウトを含む)

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウントिंगの方式リストを定義することもできます。方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」(P.9-13)
- 「TACACS+ サーバ ホストの特定および認証鍵の設定」(P.9-13)
- 「TACACS+ ログイン認証の設定」(P.9-14)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」(P.9-16)
- 「TACACS+ アカウントिंगの起動」(P.9-17)

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されます。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。



(注) TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定および認証鍵の設定

認証用に 1 つのサーバを使用することも、また、既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバグループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号鍵を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>tacacs-server host hostname [port integer] [timeout integer] [key string]</code>	TACACS+ サーバを維持する IP ホスト (1 つまたは複数) を特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <ul style="list-style-type: none"> <code>hostname</code> には、ホストの名前または IP アドレスを指定します。 (任意) <code>port integer</code> には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ~ 65535 です。 (任意) <code>timeout integer</code> には、スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチはタイムアウトしてエラーを宣言します。デフォルト値は 5 秒です。指定できる範囲は 1 ~ 1000 秒です。 (任意) <code>key string</code> には、スイッチと TACACS+ デーモン間のすべてのトラフィックを暗号化および暗号解除するための暗号鍵を指定します。暗号化が成功するには、TACACS+ デーモンに同じ鍵を設定する必要があります。
ステップ 3	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa group server tacacs+ group-name</code>	(任意) グループ名で AAA サーバグループを定義します。 このコマンドによって、スイッチはサーバグループサブコンフィギュレーションモードになります。
ステップ 5	<code>server ip-address</code>	(任意) 特定の TACACS+ サーバを定義済みサーバグループに対応付けます。AAA サーバグループの各 TACACS+ サーバに対してこのステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show tacacs</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、`no tacacs-server host hostname` グローバル コンフィギュレーション コマンドを使用します。設定リストからサーバグループを削除するには、`no aaa group server tacacs+ group-name` グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、`no server ip-address` サーバグループサブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト (偶然に `default` と名前が付けられている) です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>aaa new-model</code>	AAA をイネーブルにします。
ステップ3 <code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • list-name には、作成するリストの名前として使用する文字列を指定します。 • method1... には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • enable : イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • group tacacs+ : TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの特定および認証鍵の設定」(P.9-13) を参照してください。 • line : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。password password ライン コンフィギュレーション コマンドを使用します。 • local : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。username password グローバル コンフィギュレーション コマンドを使用します。 • local-case : 大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。username name password グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • none : ログインに認証を使用しません。

コマンド	目的
ステップ4 <code>line [console tty vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ5 <code>login authentication {default list-name}</code>	回線または回線セットに対して、認証リストを適用します。 <ul style="list-style-type: none"> <code>default</code> を指定する場合は、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストを使用します。 <code>list-name</code> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ7 <code>show running-config</code>	設定を確認します。
ステップ8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、`no aaa authentication login {default | list-name} method1 [method2...]` グローバル コンフィギュレーション コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするかデフォルト値に戻す場合は、`no login authentication {default | list-name}` ライン コンフィギュレーション コマンドを使用します。



(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、`ip http authentication aaa` グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対するスイッチのセキュリティは確保されません。

`ip http authentication` コマンドの詳細については、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) から、『Cisco IOS Security Command Reference』 Release 12.2 を参照してください。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

`aaa authorization` グローバル コンフィギュレーション コマンドに `tacacs+` キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

`aaa authorization exec tacacs+ local` コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



(注)

許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network tacacs+</code>	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可を、スイッチに設定します。
ステップ 3	<code>aaa authorization exec tacacs+</code>	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ TACACS+ 許可をスイッチに設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードは、アカウンティングのアトリビュート値 (AV) ペアを含み、セキュリティ サーバに保存されます。このデータを解析して、ネットワーク管理、クライアントへの課金、または監査に役立てることができます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop tacacs+</code>	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	<code>aaa accounting exec start-stop tacacs+</code>	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、`no aaa accounting {network | exec} {start-stop} method1...` グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

RADIUS によるスイッチ アクセスの制御

ここでは、RADIUS をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカウント情報収集、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は、AAA を介して実装され、AAA コマンドを使用してだけイネーブルにできます。



(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

ここでは、次の設定情報について説明します。

- 「RADIUS の概要」 (P.9-18)
- 「RADIUS の動作」 (P.9-20)
- 「RADIUS Change of Authorization (CoA)」 (P.9-20)
- 「RADIUS の設定」 (P.9-27)
- 「RADIUS の設定の表示」 (P.9-40)

RADIUS の概要

RADIUS は分散型クライアント/サーバ システムで、不正なアクセスからネットワークを保護します。RADIUS クライアントは、サポート対象のシスコ製ルータおよびスイッチ上で稼動します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。RADIUS ホストは、通常、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft、または他のソフトウェアプロバイダーの RADIUS サーバソフトウェアが稼動しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。



(注)

スイッチ スタックと RADIUS サーバとの間では冗長接続を確立することを推奨します。これは、接続されているスタック メンバーがスイッチ スタックから削除された場合でも、RADIUS サーバがアクセス可能なまま維持されるように保証する上で役立ちます。

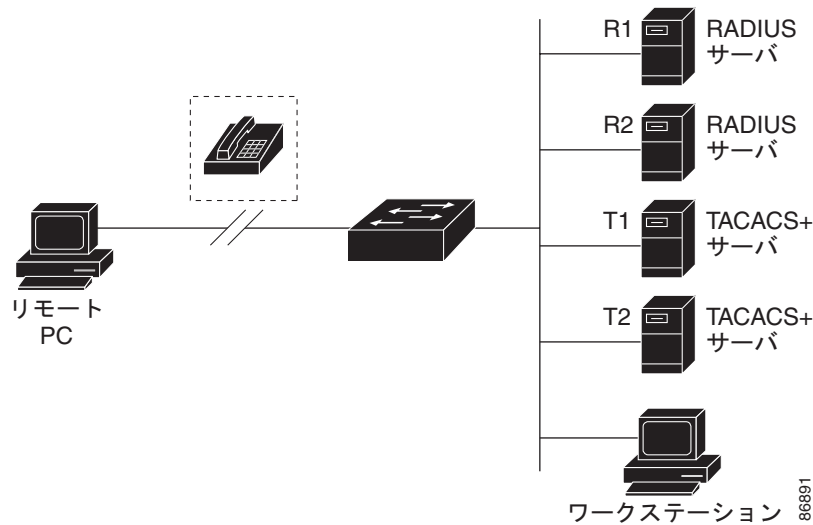
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カードアクセス制御システムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ製スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。図 9-2 (P.9-20) を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1X などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 10 章「IEEE 802.1X ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス制御およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できません。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

図 9-2 RADIUS サービスから TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス制御されるスイッチに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは RADIUS サーバから、次のいずれかの応答を受信します。
 - a. ACCEPT : ユーザが認証されたことを表します。
 - b. REJECT : ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が必要とされるか、またはアクセスが拒否されます。
 - c. CHALLENGE : ユーザに追加データを要求します。
 - d. CHALLENGE PASSWORD : ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります (イネーブルに設定されている場合)。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ (ホストまたはクライアントの IP アドレス、アクセスリスト、およびユーザタイムアウトを含む)

RADIUS Change of Authorization (CoA)

このセクションでは、Change of Authorization (CoA) の間に利用できる基本要素および使用方法など、RADIUS インターフェイスの概要を説明します。

- 「概要」 (P.9-21)
- 「要求に関する Change-of-Authorization」 (P.9-21)

- 「CoA 要求応答コード」 (P.9-23)
- 「CoA 要求コマンド」 (P.9-24)
- 「セッション再認証」 (P.9-24)
- 「セッション終了のスタッキングの注意事項」 (P.9-26)

概要

標準 RADIUS インターフェイスは、一般に、デバイスに接続するネットワークから要求が発生し、クエリーを送信されたサーバから応答が送信されるプル モデルが使用されます。Catalyst スイッチは、RFC 5176 で定義される RADIUS Change of Authorization (CoA) 拡張機能をサポートします。RADIUS Change of Authorization (CoA) は、一般にプッシュ モデルで使用され、外部の authentication, authorization, and accounting (AAA; 認証、認可、アカウントिंग) サーバまたはポリシー サーバから、セッションを動的に再設定できます。

スイッチは Cisco IOS Release 12.2(52)SE から、次のセッションごとの CoA 要求をサポートします。

- セッション再認証
- セッション終了
- ポート シャットダウンによるセッション終了
- ポート バウンスによるセッション終了

Catalyst スイッチ上では、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。しかし、次のアトリビュートには基本設定が必要です。

- Security and Password : 『*Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE*』の「Configuring Switch-Based Authentication」章の「[Preventing Unauthorized Access to Your Switch](#)」セクションを参照してください。
- Accounting : 『*Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE*』の Configuring Switch-Based Authentication」章の「[Starting RADIUS Accounting](#)」セクションを参照してください。

要求に関する Change-of-Authorization

RFC 5176 に記載のとおり、Change of Authorization (CoA) 要求は、セッション識別、ホスト再認証、およびセッション終了を考慮したプッシュ モデルで使用されます。プッシュモデルは、1 つの要求 (CoA-Request) と次の 2 つの応答コードで構成されます。

- CoA Acknowledgement (ACK; 確認応答) (CoA-ACK)
- CoA Non-Acknowledgement (NAK; 否定確認応答) (CoA-NAK)

要求は、CoA クライアント (一般に RADIUS サーバまたはポリシー サーバ) から起動され、リスナーとして機能するスイッチに向けられます。

ここでは、次の内容について説明します。

- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証

RFC 5176 準拠性

セッション終了を求める接続解除メッセージ (Packet of Disconnect (POD; パケット オブ ディスコネクト) と呼ばれる) は、スイッチによってサポートされます。

表 9-2 に、この機能のためにサポートされる IETF アトリビュートを示します。

表 9-2 サポートされる IETF アトリビュート

アトリビュート番号	アトリビュート名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 9-3 に、Error-Cause アトリビュートのとり得る値を示します。

表 9-3 Error-Cause 値

値	説明
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

前提条件

CoA インターフェイスを使用するには、スイッチにすでにセッションが存在している必要があります。CoA はセッションの識別および接続解除要求の実行に使用できます。アップデートは指定されたセッションだけに影響を与えます。

CoA 要求応答コード

CoA 要求応答コードは、スイッチへのコマンドの伝達に使用できます。サポートされるコマンドを表 9-4 (P.9-24) に示します。

セッション識別

特定のセッションを対象とする接続解除要求および CoA 要求の場合、スイッチは次のアトリビュートに基づいてセッションを検索します。

- Calling-Station-Id (IETF アトリビュート #31。ホスト MAC アドレスを含む)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF アトリビュート #44)

CoA メッセージに含まれるすべてのセッション識別アトリビュートがセッションに合致しないかぎり、スイッチは接続解除の NAK か、または CoA-NAK と「Invalid Attribute Value」エラーコードアトリビュートを返します。

特定のセッションを対象とする接続解除要求および CoA 要求の場合、次のセッション ID が使用できます。

- Calling-Station-Id (IETF アトリビュート #31。MAC アドレスを含まなければならない)
- Audit-Session-ID (Cisco ベンダー固有属性)
- Accounting-Session-Id (IETF アトリビュート #44)

2 つ以上のセッション ID アトリビュートがメッセージに含まれている場合、すべてのアトリビュートがセッションに合致する必要があります。そうでない場合は、スイッチは接続解除の否定確認応答 (NAK) か、または CoA-NAK とエラーコード「Invalid Attribute Value」を返します。

RFC 5176 に定義されるように、CoA 要求コードのパケットフォーマットは、Code、Identifier、Length、Authenticator の各フィールド、および複数のアトリビュート (Type:Length:Value (TLV) 形式) で構成されます。

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Code           | Identifier |           Length           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Authenticator                               |
|                                                                           |
|                                                                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Attributes ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

アトリビュート フィールドは、Cisco VSA の伝達に使用されます。

CoA ACK 応答コード

許可ステートが正常に変更される時、肯定確認応答 (ACK) が送信されます。CoA ACK 内で返されるアトリビュートは、CoA 要求によって異なります。また、個々の CoA コマンドで扱われます。

CoA NAK 応答コード

否定確認応答 (NAK) は、許可ステートの変更失敗を示し、失敗の原因を示すアトリビュートを含むことができます。show コマンドを使用して、CoA の成功を確認します。

CoA 要求コマンド

ここでは、次の内容について説明します。

- セッション再認証
- スイッチ スタックにおけるセッション再認証
- セッション終了
- CoA 接続解除要求
- CoA 要求 : ホスト ポートのディセーブル化
- CoA 要求 : バウンス ポート

Cisco IOS Release 12.2(52)SE 以降では、スイッチは表 9-4 に示されるコマンドをサポートします。

表 9-4 スイッチでサポートされる CoA コマンド

コマンド ¹	Cisco VSA
Reauthenticate host	Cisco : Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を必要としない標準の接続解除要求です。
Bounce host port	Cisco : Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco : Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドは、スイッチと CoA クライアントの間のセッション ID を含む必要があります。

セッション再認証

ホストの ID が未知の場合、または、ポスチャがネットワークに参加し、制限付きアクセス許可プロファイルに関連付けられている（ゲスト VLAN など）場合は、AAA サーバは一般にセッション再認証要求を生成します。再認証要求によって、ホストの証明書が既知であればホストは適切な認証グループに配置されます。

セッション認証を開始するために、AAA サーバは、*Cisco:Avpair="subscriber:command=reauthenticate"* 形式の Cisco ベンダー固有属性（VSA）と 1 つ以上のセッション識別アトリビュートを含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージへのスイッチ応答を決定します。IEEE 802.1X によってセッションが現在認証される場合、スイッチは、EAPoL¹-RequestId メッセージ（下の脚注 1 を参照）をサーバに送信することで応答します。

MAC authentication bypass（MAB; MAC 認証バイパス）によってセッションが現在認証される場合、スイッチはアクセス要求をサーバに送信し、初期の正常認証に使用されたものと同一の識別アトリビュートを渡します。

スイッチがコマンドを受信したときにセッション認証が進行中であれば、スイッチはプロセスを終了し、最初に試みるように設定された方式から認証シーケンスを再開します。

セッションがまだ認証されていない場合、ゲスト VLAN、またはクリティカルな VLAN、または同様のポリシーで認証された場合、再認証メッセージは、最初に試みるように設定された方式からアクセスコントロール方式を開始します。現在のセッションの認証は、再認証が異なる認証結果になるまで維持されます。

1. Extensible Authentication Protocol over LAN

スイッチ スタックにおけるセッション再認証

スイッチ スタックがセッション再認証メッセージを受信したときは、次を実行します。

- 確認応答 (ACK) を返す前に、再認証の必要性をチェックポイントします。
- 該当するセッションの再認証を開始します。
- 成功または失敗のいずれかの状態の認証終了後、再認証を起動した信号がスタック メンバーから削除されます。
- 認証終了の前にスタック マスターに障害が発生した場合、オリジナルのコマンドに基づくスタック マスターの切り替え後に再認証が開始されます (オリジナルのコマンドは後で削除されます)。
- ACK を送信する前にスタック マスターに障害が発生した場合は、新しいスタック マスターが再送信されたコマンドを新しいコマンドとして処理します。

セッション終了

セッション終了を発生させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディセーブル化することなくセッションを終了させます。このコマンドによって指定されたホストのオーセンティケータ ステート マシンの再初期化が実行されますが、ホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、CoA 要求と

Cisco:Avpair="subscriber:command=disable-host-port" の VSA を使用します。このコマンドは、あるホストがネットワーク上で問題を起こしていることが既知であり、ホストのネットワーク アクセスをただちにブロックする必要がある場合に有効です。ポート上のネットワーク アクセスを回復するときは、非 RADIUS メカニズムを使用して再度イネーブルにします。

プリンタなどのサブリカントのない装置が、新しい IP アドレス (VLAN 変更の後など) を取得する必要がある場合、ポート バウンス (一時的にポートをディセーブルにして、再度イネーブルにする) を使用してホスト ポートのセッションを終了します。

CoA 接続解除要求

このコマンドは、標準の接続解除要求です。このコマンドはセッション指向であるため、「[セッション識別](#)」(P.9-23) に記述されている 1 つ以上のセッション識別アトリビュートを伴う必要があります。セッションが見つからない場合、スイッチは接続解除 NAK メッセージと「Session Context Not Found」エラー コードアトリビュートを返します。セッションが見つかった場合は、スイッチはセッションを終了します。セッションが完全に削除されると、スイッチは接続解除 ACK を返します。

クライアントに接続解除 ACK を返す前にスイッチがスタンバイ スイッチにフェールオーバーした場合、要求がクライアントから再送されたときに、新しいアクティブ スイッチでプロセスが繰り返されます。再送の後でセッションが見つからない場合は、接続解除 ACK と「Session Context Not Found」エラー コードアトリビュートが送信されます。

CoA 要求 : ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA のある標準の CoA 要求メッセージで搬送されます。

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

このコマンドはセッション指向であるため、「[セッション識別](#)」(P.9-23) に記述されている 1 つ以上のセッション識別アトリビュートを伴う必要があります。セッションが見つからない場合、スイッチは CoA NAK メッセージと「Session Context Not Found」エラー コードアトリビュートを返します。セッションが見つかった場合は、スイッチはホスティング ポートをディセーブルにし、CoA ACK メッセージを返します。

クライアントに CoA ACK を返す前にスイッチに障害が発生した場合は、要求がクライアントから再送されたときに、新しいアクティブ スイッチでプロセスが繰り返されます。クライアントに CoA ACK メッセージを返した後、動作が完了する前にスイッチに障害が発生した場合は、新しいアクティブ スイッチで動作が再スタートされます。



(注)

コマンド再送の後の接続解除要求の失敗によって、切り替え前にセッションが正常に終了する（接続解除 ACK が送信されなかった場合）か、または、オリジナルのコマンドが発行されてスタンバイ スイッチがアクティブになる前に発生した別の理由（リンク障害など）でセッションが終了するかのいずれかです。

CoA 要求 : バウンス ポート

このコマンドは、次の新しい VSA のある標準の CoA 要求メッセージで搬送されます。

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

このコマンドはセッション指向であるため、「セッション識別」(P.9-23) に記述されている 1 つ以上のセッション識別アトリビュートを伴う必要があります。セッションが見つからない場合、スイッチは CoA NAK メッセージと「Session Context Not Found」エラー コードアトリビュートを返します。セッションが見つかった場合、スイッチはホスティング ポートを 10 秒間ディセーブルに、再度、イネーブルにして（ポート バウンス）し、CoA ACK を返します。

クライアントに CoA ACK を返す前にスイッチに障害が発生した場合は、要求がクライアントから再送されたときに、新しいアクティブ スイッチでプロセスが繰り返されます。クライアントに CoA ACK メッセージを返した後、動作が完了する前にスイッチに障害が発生した場合は、新しいアクティブ スイッチで動作が再スタートされます。

セッション終了のスタッキングの注意事項

スイッチ スタックでは、CoA 接続解除要求メッセージに特別な取扱いは必要ありません。

CoA 要求バウンス ポートのスタッキングの注意事項

bounce-port コマンドは、ポートではなく、セッションで起動されるため、セッションが見つからない場合、コマンドは実行できません。

スタック マスターの Auth Manager コマンドハンドラが有効な **bounce-port** コマンドを受信した場合、CoA ACK メッセージを返す前に次の情報をチェックポイントします。

- ポート バウンスの必要性
- ポート ID（ローカルセッション コンテキストで判明する）

スイッチはポート バウンス（ポートを 10 秒間ディセーブルにし、再度、イネーブルする）を開始します。

ポート バウンスが成功した場合、ポート バウンスを起動した信号がスタンバイ スタック マスターから削除されます。

ポート バウンス終了の前にスタック マスターに障害が発生した場合、オリジナルのコマンドに基づくスタック マスターの切り替え後にポート バウンスが開始されます（オリジナルのコマンドは後で削除されます）。

CoA ACK メッセージを送信する前にスタック マスターに障害が発生した場合は、新しいスタック マスターが再送信されたコマンドを新しいコマンドとして処理します。

CoA 要求ディセーブル ポートのスタッキングの注意事項

disable-port コマンドは、ポートではなく、セッションで起動されるため、セッションが見つからない場合、コマンドは実行できません。

スタック マスターの **Auth Manager** コマンドハンドラが有効な **disable-port** コマンドを受信した場合、CoA ACK メッセージを返す前に次の情報を確認します。

- ポート ディセーブルの必要性
- ポート ID (ローカルセッション コンテキストで判明する)

スイッチはポートのディセーブル化を試みます。

ポート ディセーブル操作が成功した場合、ポート ディセーブルを起動した信号がスタンバイ スタック マスターから削除されます。

ポート ディセーブル操作終了の前にスタック マスターに障害が発生した場合、オリジナルのコマンドに基づくスタック マスターの切り替え後にポートがディセーブルにされます (オリジナルのコマンドは後で削除されます)。

CoA ACK メッセージを送信する前にスタック マスターに障害が発生した場合は、新しいスタック マスターが再送信されたコマンドを新しいコマンドとして処理します。

RADIUS の設定

ここでは、スイッチが RADIUS をサポートするように設定する方法について説明します。最低限、RADIUS サーバ ソフトウェアが稼動するホスト (1 つまたは複数) を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウントिंगの方式リストを定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコル (TACACS+、ローカル ユーザ名検索など) を 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用して、ユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。

- 「RADIUS のデフォルト設定」 (P.9-28)
- 「RADIUS サーバ ホストの識別」 (P.9-28) (必須)
- 「RADIUS ログイン認証の設定」 (P.9-30) (必須)
- 「AAA サーバ グループの定義」 (P.9-32) (任意)
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」 (P.9-34) (任意)
- 「RADIUS アカウントिंगの起動」 (P.9-35) (任意)
- 「すべての RADIUS サーバの設定」 (P.9-36) (任意)
- 「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」 (P.9-36) (任意)
- 「ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定」 (P.9-38) (任意)
- 「スイッチ上での CoA 設定」 (P.9-39)
- 「CoA 機能のモニタリングとトラブルシューティング」 (P.9-40)

- 「RADIUS サーバ ロード バランシングの設定」(P.9-40) (任意)

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホストの識別

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー ストリング
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス (たとえばアカウンティング) を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示して、そのあと同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます (RADIUS ホスト エントリは、設定した順序に従って試行されます)。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デモンが稼動するホストと、そのホストがスイッチと共有するシークレット テキスト (キー) ストリングを指定しなければなりません。

タイムアウト、再送信回数、および暗号鍵の値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。スイッチと通信するすべての RADIUS サーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。



(注)

スイッチ上にグローバルな機能とサーバ単位での機能 (タイムアウト、再送信回数、およびキー コマンド) を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、および鍵に関するコマンドは、グローバルに設定したタイムアウト、再送信回数、および鍵に関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、「すべての RADIUS サーバの設定」(P.9-36) を参照してください。

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。詳細については、「AAA サーバ グループの定義」(P.9-32)を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> • (任意) auth-port port-number には、認証要求の UDP 宛先ポートを指定します。 • (任意) acct-port port-number には、アカウント要求の UDP 宛先ポートを指定します。 • (任意) timeout seconds には、スイッチが RADIUS サーバの応答を待機して再送信するまでのタイム インターバルを指定します。指定できる範囲は 1 ~ 1000 です。この設定は、radius-server timeout グローバル コンフィギュレーション コマンドによる設定を上書きします。radius-server host コマンドでタイムアウトを設定しない場合は、radius-server timeout コマンドの設定が使用されます。 • (任意) retransmit retries には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。radius-server host コマンドで再送信回数を指定しない場合、radius-server retransmit グローバル コンフィギュレーション コマンドの設定が使用されます。 • (任意) key string には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。 <p>(注) 鍵はテキスト ストリングで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。鍵は常に radius-server host コマンドの最後のアイテムとして設定してください。先行スペースは無視されますが、鍵の中間および末尾にあるスペースは有効です。鍵にスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないでください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号鍵をそれぞれ設定してください。</p>
ステップ3 end	特権 EXEC モードに戻ります。
ステップ4 show running-config	設定を確認します。
ステップ5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host hostname | ip-address** グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウントリング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウントリングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```



(注) RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー スtring があります。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ3 <code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • list-name には、作成するリストの名前として使用する文字列を指定します。 • method1... には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 <ul style="list-style-type: none"> – enable : イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 – group radius : RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別 (P.9-28)」を参照してください。 – line : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。password password ライン コンフィギュレーション コマンドを使用します。 – local : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。username name password グローバル コンフィギュレーション コマンドを使用します。 – local-case : 大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。username password グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 – none : ログインに認証を使用しません。
ステップ4 <code>line [console tty vty] line-number [ending-line-number]</code>	<p>ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。</p>
ステップ5 <code>login authentication {default list-name}</code>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • list-name には、aaa authentication login コマンドで作成したリストを指定します。
ステップ6 <code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ7 <code>show running-config</code>	<p>設定を確認します。</p>
ステップ8 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login {default | list-name} method1 [method2...]** グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication {default | list-name}** ライン コンフィギュレーション コマンドを使用します。



(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対するスイッチのセキュリティは確保されません。

ip http authentication コマンドの詳細については、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) から、『Cisco IOS Security Command Reference』 Release 12.2 を参照してください。

AAA サーバグループの定義

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID (IP アドレスと UDP ポート番号の組み合わせ) を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス (たとえばアカウントिंग) を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバグループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> （任意）<code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。 （任意）<code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。 （任意）<code>timeout seconds</code> には、スイッチが RADIUS サーバの応答を待機して再送信するまでのタイム インターバルを指定します。指定できる範囲は 1 ～ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。 （任意）<code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。 （任意）<code>key string</code> には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。 <p>(注) 鍵はテキスト ストリングで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。鍵は常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先行スペースは無視されますが、鍵の中間および末尾にあるスペースは有効です。鍵にスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まなくてください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号鍵をそれぞれ設定してください。</p>
ステップ3 <code>aaa new-model</code>	AAA をイネーブルにします。
ステップ4 <code>aaa group server radius group-name</code>	<p>AAA サーバグループを、特定のグループ名で定義します。</p> <p>このコマンドを使用すると、スイッチはサーバグループ コンフィギュレーション モードになります。</p>
ステップ5 <code>server ip-address</code>	<p>特定の RADIUS サーバを定義済みのサーバグループに対応付けます。AAA サーバグループの RADIUS サーバごとに、このステップを繰り返します。</p> <p>グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。</p>
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ7	<code>show running-config</code>	設定を確認します。
ステップ8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。
ステップ9		RADIUS ログイン認証をイネーブルにします。「 RADIUS ログイン認証の設定 」(P.9-30) を参照してください。

特定の RADIUS サーバを削除するには、`no radius-server host hostname | ip-address` グローバル コンフィギュレーション コマンドを使用します。サーバグループをコンフィギュレーション リストから削除するには、`no aaa group server radius group-name` グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、`no server ip-address` サーバグループ コンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ (*group1* および *group2*) を認識するようにスイッチを設定しています。*group1* では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは (ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する) ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定するには、`aaa authorization` グローバル コンフィギュレーション コマンドとともに `radius` キーワードを使用します。

`aaa authorization exec radius local` コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注)

許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、スイッチに設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可を、スイッチに設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードは、アカウンティングのアトリビュート値 (AV) ペアを含み、セキュリティ サーバに保存されます。このデータを解析して、ネットワーク管理、クライアントへの課金、または監査に役立てることができます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop radius</code>	ネットワーク関連のすべてのサービス要求について、RADIUS アカウンティングをイネーブルにします。
ステップ 3	<code>aaa accounting exec start-stop radius</code>	RADIUS アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止アカウンティング通知を送信するように設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、`no aaa accounting {network | exec} {start-stop} method1...` グローバル コンフィギュレーション コマンドを使用します。

すべての RADIUS サーバの設定

スイッチとすべての RADIUS サーバ間でグローバルに通信を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server key string</code>	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト スtring を指定します。 (注) 鍵はテキスト スtring で、RADIUS サーバで使用されている暗号鍵と一致する必要があります。先行スペースは無視されますが、鍵の中間および末尾にあるスペースは有効です。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
ステップ 3	<code>radius-server retransmit retries</code>	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 4	<code>radius-server timeout seconds</code>	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間 (秒) を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 です。
ステップ 5	<code>radius-server deadtime minutes</code>	認証要求に応答しない RADIUS サーバをスキップする時間 (分) を指定し、要求がタイムアウトするまで待機することなく、次に設定されているサーバを試行できるようにします。デフォルトは 0 です。指定できる範囲は 1 ~ 1440 分です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定値を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数、タイムアウト、および待機時間の設定をデフォルトに戻すには、これらのコマンドの **no** 形式を使用します。

ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定

Internet Engineering Task Force (IETF) ドラフト規格に、ベンダー固有のアトリビュート (アトリビュート 26) を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、一般的な用途には適さない独自の拡張アトリビュートをサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダー タイプ 1 (名前は *cisco-avpair*) です。この値は、次のフォーマットの String です。

```
protocol : attribute sep value *
```

protocol は、特定の許可タイプに使用するシスコのプロトコルアトリビュートの値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切なアトリビュート値 (AV) ペアです。*sep* は、必須のアトリビュートの場合は =、任意指定のアトリビュートの場合は * です。TACACS+ 許可で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアを指定すると、IP 許可時 (PPP の IPCP アドレスの割り当て時) に、シスコの複数の名前付き IP アドレス プール機能が有効になります。

```
cisco-avpair= "ip:addr-pool=first"
```

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバ データベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type (#64)=VLAN (13)"
cisco-avpair= "tunnel-medium-type (#65)=802 media (6)"
cisco-avpair= "tunnel-private-group-ID (#81)=vlanid"
```

次に、この接続中に ASCII 形式の入力 ACL (アクセス コントロール リスト) をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any deernet-iv"
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138 「Remote Authentication Dial-In User Service (RADIUS)」を参照してください。

スイッチが VSA を認識して使用するよう設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server vsa send [accounting authentication]</code>	<p>スイッチが VSA (RADIUS IETF アトリビュート 26 で定義) を認識して使用できるようにします。</p> <ul style="list-style-type: none"> (任意) 認識されるベンダー固有アトリビュートの集合をアカウントングアトリビュートだけに限定するには、accounting キーワードを使用します。 (任意) 認識されるベンダー固有アトリビュートの集合を認証アトリビュートだけに限定するには、authentication キーワードを使用します。 <p>キーワードを指定せずにこのコマンドを入力すると、アカウントングおよび認証のベンダー固有アトリビュートの両方が使用されます。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定値を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

RADIUS アトリビュートの全リストまたはベンダー固有属性 26 の詳細については、『Cisco IOS Security Configuration Guide』Release 12.2 の付録「RADIUS Attributes」を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS アトリビュート セットを独自に機能拡張しているベンダーもあります。CiscoIOS ソフトウェアは、ベンダー独自仕様の RADIUS アトリビュートのサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバデーモン稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト スtringを指定しなければなりません。RADIUS ホストおよびシークレット テキスト スtringを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト スtringを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host {hostname ip-address} non-standard	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、そのホストが、ベンダーが独自に実装した RADIUS を使用していることを指定します。
ステップ 3	radius-server key string	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト スtringを指定します。スイッチおよび RADIUS サーバは、このテキスト スtringを使用して、パスワードの暗号化および応答の交換を行います。 (注) 鍵はテキスト スtringで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。先行スペースは無視されますが、鍵の中間および末尾にあるスペースは有効です。鍵にスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないでください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定値を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、**no radius-server host {hostname | ip-address} non-standard** グローバル コンフィギュレーション コマンドを使用します。鍵をディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次に、ベンダー独自仕様の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* という秘密鍵を使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

スイッチ上での CoA 設定

スイッチ上で CoA を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa server radius dynamic-author</code>	外部ポリシー サーバとの相互作用を容易にするために、認証、認可、アカウントिंग (AAA) サーバとしてスイッチを設定します。
ステップ 4	<code>client {ip-address name} [vrf vrfname] [server-key string]</code>	ダイナミック 認可ローカルサーバ設定モードを開始し、装置が受け入れる CoA 要求と接続解除要求の送信元である RADIUS クライアントを指定します。
ステップ 5	<code>server-key [0 7] string</code>	装置と RADIUS クライアントの間で共有される RADIUS 鍵を設定します。
ステップ 6	<code>port port-number</code>	設定された RADIUS クライアントからの RADIUS 要求をリスニングする装置のポートを指定します。
ステップ 7	<code>auth-type {any all session-key}</code>	スイッチが RADIUS クライアントに使用する認可の種類を指定します。クライアントが、認可に設定されたアトリビュートのすべてが一致する必要があります。
ステップ 8	<code>ignore session-key</code>	(任意) セッション鍵を無視するようにスイッチを設定します。 ignore コマンドの詳細については、Cisco.com にある『 Cisco IOS Intelligent Services Gateway Command Reference 』を参照してください。
ステップ 9	<code>ignore server-key</code>	(任意) サーバ鍵を無視するようにスイッチを設定します。 ignore コマンドの詳細については、Cisco.com にある『 Cisco IOS Intelligent Services Gateway Command Reference 』を参照してください。
ステップ 10	<code>authentication command bounce-port ignore</code>	(任意) CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。ポートの一時的なディセーブル化の目的は、VLAN 変更が発生し、エンドポイントに変更を検知するサブリカントがない場合に、ホストから DHCP 再ネゴシエーションを起動することです。
ステップ 11	<code>authentication command disable-port ignore</code>	(任意) セッションをホスティングするポートの管理上のシャットダウンを要求する非標準コマンドを無視するようにスイッチを設定します。ポートのシャットダウンによって、セッションが終了します。 標準の CLI コマンドまたは Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) コマンドを使用してポートを再度、イネーブルにします。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show running-config</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。スイッチ上で AAA サーバ機能をディセーブルにするには、`no aaa server radius dynamic authorization` グローバル コンフィギュレーション コマンドを使用します。

CoA 機能のモニタリングとトラブルシューティング

次の Cisco IOS コマンドは、スイッチ上の CoA 機能のモニタリングおよびトラブルシューティングに使用できます。

- `debug radius`
- `debug aaa coa`
- `debug aaa pod`
- `debug aaa subsys`
- `debug cmdhd [detail | error | events]`
- `show aaa attributes protocol radius`

RADIUS サーバ ロード バランシングの設定

この機能を使用して、アクセスおよび認証要求をサーバグループ内のすべての RADIUS サーバに均等に分散することができます。詳細については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「RADIUS Server Load Balancing」の章を参照してください。

http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrlddbl.html

RADIUS の設定の表示

RADIUS の設定を表示するには、`show running-config` 特権 EXEC コマンドを使用します。

Kerberos によるスイッチ アクセスの制御

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。この機能を使用するには、スイッチにスイッチ ソフトウェアの暗号化バージョンをインストールする必要があります。

この機能を使用し、暗号化ソフトウェア ファイルを Cisco.com からダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「Kerberos の概要」(P.9-41)
- 「Kerberos の動作」(P.9-43)
- 「Kerberos の設定」(P.9-44)

Kerberos の設定例については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Kerberos Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html

ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Security Command Reference』 Release 12.2 の「Security Server Protocols」の章の「Kerberos Commands」のセクションを参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html



(注)

Kerberos の設定例および『Cisco IOS Security Command Reference』Release 12.2 では、信頼のおけるサードパーティとして Catalyst 3750 スイッチを使用しています。このスイッチは Kerberos に対応し、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用したユーザ認証ができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密鍵によるネットワーク認証プロトコルです。Data Encryption Standard (DES; データ暗号化規格) という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティを *Key Distribution Center* (KDC; 鍵発行局) と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC (つまり信頼できる Kerberos サーバ) がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ証明書のキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。



(注)

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる Catalyst 3750 スイッチを使用できます。

Kerberos の証明書発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを1回認証すると、ユーザ証明書が有効な間は (他のパスワードの暗号化を行わずに) セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、(UNIX サーバや PC などの) 他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

このソフトウェア リリースでは、Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh (リモート シェル プロトコル)

表 9-5 に、一般的な Kerberos 関連用語とその定義を示します。

表 9-5 Kerberos の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段

表 9-5 Kerberos の用語 (続き)

用語	定義
証明書	認証チケット (TGT ¹ やサービス証明書など) を表す総称。Kerberos 証明書で、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの許可レベル ラベル。ほとんどの Kerberos プリンシパルは、[user@REALM] という形式です (たとえば、smith@EXAMPLE.COM)。Kerberos インスタンスのある Kerberos プリンシパルは、[user/instance@REALM] という形式です (たとえば、smith/admin@EXAMPLE.COM)。Kerberos インスタンスは、認証が成功した場合のユーザの許可レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 (注) Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 (注) Kerberos レルム名はすべて大文字でなければなりません。
KDC ²	ネットワーク ホストで稼動する Kerberos サーバおよびデータベース プログラムで構成される鍵発行局
Kerberos 対応	Kerberos 証明書のインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 (注) Kerberos レルム名はすべて大文字でなければなりません。
Kerberos サーバ	ネットワーク ホストで稼動しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB ³	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス証明書を暗号解除して認証します。KEYTAB は Kerberos 5 よりも前のバージョンでは、SRVTAB ⁴ と呼ばれています。
プリンシパル	Kerberos ID と呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 (注) Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス証明書	ネットワーク サービスの証明書。KDC から証明書が発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT とともにパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザに発行する証明書。TGT を受け取ったユーザは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

1. TGT = Ticket Granting Ticket (身分証明書)
2. KDC = Key Distribution Center (鍵発行局)
3. KEYTAB = key table (キー テーブル)
4. SRVTAB = server table (サーバテーブル)

Kerberos の動作

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してリモート ユーザを認証できる Catalyst 3750 スイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

Kerberos サーバとして Catalyst 3750 スイッチを使用して、ネットワーク サービスに対して認証を得る手順は、次のとおりです。

1. 「境界スイッチに対する認証の取得」(P.9-43)
2. 「KDC からの TGT の取得」(P.9-43)
3. 「ネットワーク サービスに対する認証の取得」(P.9-44)

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
 - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
 - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力 (Caps Lock または Num Lock のオン/オフに注意) するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番目のセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番目のセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Authenticating to Network Services」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。



(注)

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる Catalyst 3750 スイッチを使用できます。

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

設定については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Kerberos Configuration Task List」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

スイッチのローカル認証および許可の設定

ローカルモードでAAAを実装するようにスイッチを設定すると、サーバがなくても動作するようにAAAを設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウント機能は使用できません。

スイッチをローカルAAA用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ3	<code>aaa authentication login default local</code>	ローカルのユーザ名データベースを使用するようにログイン認証を設定します。 default キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ4	<code>aaa authorization exec local</code>	ユーザの AAA 許可を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ5	<code>aaa authorization network local</code>	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 許可を設定します。
ステップ6	<code>username name [privilege level] {password encryption-type password}</code>	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 <ul style="list-style-type: none"> name には、ユーザ ID を 1 ワードで指定します。スペースおよび引用符は使用できません。 (任意) level には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 encryption-type には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 password には、ユーザがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ8	<code>show running-config</code>	設定を確認します。
ステップ9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。



(注) AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『Cisco IOS Security Command Reference』Release 12.2 を参照してください。

SSH のためのスイッチの設定

ここでは、SSH 機能を設定する方法について説明します。この機能を使用するには、暗号（暗号化）ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「SSH の概要」(P.9-46)
- 「SSH の設定」(P.9-48)
- 「SSH の設定およびステータスの表示」(P.9-50)

SSH の設定例については、『Cisco IOS Security Configuration Guide』Release 12.2 の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html



(注) ここで使用するコマンドの構文および使用方法の詳細については、次の URL にあるこのリリースに対応するコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

SSH の概要

SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1 (SSHv1) および SSH バージョン 2 (SSHv2) をサポートしています。

ここでは、次の内容について説明します。

- 「SSH サーバ、統合クライアント、およびサポートされているバージョン」(P.9-47)
- 「制限事項」(P.9-47)



(注)

IP ベース イメージ (以前の Standard Multilayer Image (SMI; 標準マルチレイヤ イメージ)) ソフトウェアまたは IP サービス イメージ (以前の Enhanced Multilayer Image (EMI; 拡張マルチレイヤ イメージ)) ソフトウェアの暗号化バージョンを実行するスタック マスターで障害が発生し、ソフトウェアの非暗号化バージョンを実行するスイッチに置き換わった場合、スイッチ スタックへの SSH 接続は失われることがあります。IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの暗号化バージョンを実行するスイッチをスタック マスターにすることを推奨します。スタック マスターが IP ベース イメージ ソフトウェアまたは IP サービス イメージ ソフトウェアの非暗号化バージョンを実行している場合、暗号化機能は使用できません。

SSH サーバ、統合クライアント、およびサポートされているバージョン

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるアプリケーションです。SSH クライアントを使用すると、SSH サーバが稼動するスイッチに接続できます。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。また、SSH クライアントは、このリリースでサポートされている SSH サーバおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートしています。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、DES 暗号化アルゴリズム、Triple DES (3DES) 暗号化アルゴリズム、およびパスワードベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+ (詳細については、「[TACACS+ によるスイッチ アクセスの制御](#)」(P.9-10) を参照してください)
- RADIUS (詳細については、「[RADIUS によるスイッチ アクセスの制御](#)」(P.9-18) を参照してください)
- ローカル認証および許可 (詳細については、「[スイッチのローカル認証および許可の設定](#)」(P.9-45) を参照してください)



(注)

このソフトウェア リリースは、IP Security (IPSec) をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman (RSA) 認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES (56 ビット) および 3DES (168 ビット) データ暗号化ソフトウェアに限りサポートされます。
- スイッチは、Advanced Encryption Standard (AES) 対称暗号化アルゴリズムをサポートしません。

SSH の設定

ここでは、次の設定情報について説明します。

- 「[設定時の注意事項](#)」 (P.9-48)
- 「[スイッチで SSH を実行するためのセットアップ](#)」 (P.9-48) (必須)
- 「[SSH サーバの設定](#)」 (P.9-49) (スイッチを SSH サーバとして設定する場合に限り必須)

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA 鍵のペアを使用できません (逆の場合も同様です)。
- SSH サーバがスタック マスター上で稼動中に、スタック マスターに障害が生じた場合、新しいスタック マスターは直前のスタック マスターによって生成された RSA 鍵を使用します。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力したあと、CLI エラー メッセージが表示される場合、RSA 鍵ペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、「[スイッチで SSH を実行するためのセットアップ](#)」 (P.9-48) を参照してください。
- RSA 鍵のペアを生成する場合に、メッセージ [No host name specified] が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA 鍵のペアを生成する場合に、メッセージ [No domain specified] が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

スイッチで SSH を実行するためのセットアップ

SSH を実行するようにスイッチをセットアップするには、次の手順を実行してください。

1. 暗号化ソフトウェア イメージを Cisco.com からダウンロードします。この手順は必須です。詳細については、このリリースのリリース ノートを参照してください。
2. スイッチのホスト名および IP ドメイン名を設定します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
3. スイッチが SSH を自動的にイネーブルにするための RSA 鍵のペアを生成します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
4. ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、「[スイッチのローカル認証および許可の設定](#)」 (P.9-45) を参照してください。

ホスト名と IP ドメイン名を設定し、RSA 鍵のペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合です。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>hostname hostname</code>	スイッチのホスト名を設定します。
ステップ3 <code>ip domain-name domain_name</code>	スイッチのホスト ドメインを設定します。
ステップ4 <code>crypto key generate rsa</code>	スイッチ上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA 鍵のペアを生成します。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA 鍵のペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。
ステップ5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ6 <code>show ip ssh</code> または <code>show ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。
ステップ7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RSA 鍵のペアを削除するには、`crypto key zeroize rsa` グローバル コンフィギュレーション コマンドを使用します。RSA 鍵のペアを削除すると、SSH サーバは自動的にディセーブルになります。

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 <code>ip ssh version [1 2]</code>	(任意) SSHv1 または SSHv2 を実行するようにスイッチを設定します。 <ul style="list-style-type: none"> 1: SSHv1 を実行するようにスイッチを設定します。 2: SSHv2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートしている場合、SSH サーバは SSHv2 を選択します。

コマンド	目的
ステップ3 <code>ip ssh {timeout seconds authentication-retries number}</code>	SSH 制御パラメータを設定します。 <ul style="list-style-type: none"> タイムアウト値は秒単位で指定します (デフォルト値は 120 秒)。指定できる範囲は 0 ~ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション (セッション 0 ~ 4) に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ~ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ4 <code>line vty line_number [ending_line_number]</code> <code>transport input ssh</code>	(任意) 仮想端末回線設定を設定します。 <ul style="list-style-type: none"> ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。 <code>line_number</code> および <code>ending_line_number</code> に対して、1 回線ペアを指定します。指定できる範囲は 0 ~ 15 です。 スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ6 <code>show ip ssh</code> または <code>show ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバの接続ステータスを表示します。
ステップ7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの SSH 制御パラメータに戻すには、`no ip ssh {timeout | authentication-retries}` グローバル コンフィギュレーション コマンドを使用します。

SSH の設定およびステータスの表示

SSH サーバの設定およびステータスを表示するには、表 9-6 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 9-6 SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
<code>show ip ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。
<code>show ssh</code>	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』 Release 12.2 の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cd.html

SSL HTTP のためのスイッチの設定

ここでは、HTTP 1.1 のサーバおよびクライアントに対応した Secure Socket Layer (SSL) バージョン 3.0 を設定する方法について説明します。SSL は、セキュア HTTP 通信を実現するために、HTTP クライアント認証だけでなく、サーバ認証、暗号化、およびメッセージの完全性も提供します。SSL を使用するには、暗号化ソフトウェア イメージがスイッチにインストールされている必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。暗号化イメージの詳細については、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「セキュア HTTP サーバおよびクライアントの概要」(P.9-51)
- 「セキュア HTTP サーバおよびクライアントの設定」(P.9-53)
- 「セキュア HTTP サーバおよびクライアントのステータスの表示」(P.9-57)

ここで使用する設定例やコマンドの構文および使用方法の詳細については、次の URL にある Cisco IOS Release 12.2(15)T の「HTTPS - HTTP Server and Client with SSL 3.0」の機能説明を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015a4c6.html

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよびセキュア HTTP クライアントでは、アプリケーション レイヤの暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます (セキュアな接続の場合、URL が http:// の代わりに https:// で始まります)。

セキュア HTTP サーバ (スイッチ) の主な役割は、指定のポート (デフォルトの HTTPS ポートは 443) で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答 (呼び出す) します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント (Web ブラウザ) の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を (そのアプリケーションに) 返すことです。

CA の信頼点

Certificate Authority (CA; 認証局) は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集約的なセキュリティ キーおよび証明書の管理を提供します。特定の CA サーバは *信頼点* と呼ばれます。

接続が実行されると、HTTPS サーバは、信頼点となる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント (通常、Web ブラウザ) は、その証明書の認証に必要な公開鍵を保有しています。

セキュア HTTP 接続には、CA の信頼点を設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA の信頼点が設定されていないと、サーバは自身を認証して必要な RSA の鍵のペアを生成します。自身で認証した（自己署名）証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択（確立または拒否）をさせる必要があります。この選択肢は内部ネットワーク トポロジ（テスト用など）に役立ちます。

CA の信頼点を設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ（またはクライアント）に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されていない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書（一時的に）が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。



(注)

CA および信頼点は、デバイスごとに設定する必要があります。他のデバイスからこれらをコピーしても、スイッチでは無効です。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力（show running-config コマンド）を例として一部示します。

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

<output truncated>

```
crypto pki trustpoint TP-self-signed-3080755072
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3080755072
  revocation-check none
  rsakeypair TP-self-signed-3080755072
```

```
!
```

```
crypto ca certificate chain TP-self-signed-3080755072
  certificate self-signed 01
    3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
```

<output truncated>

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。



(注)

TP self-signed の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド (**ip http secure-client-auth**) を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Configuring Authority Interoperability」の章を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ (RSA 公開鍵暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC) をサポートします。

最適な暗号化には、128 ビット暗号化をサポートするクライアントブラウザ (Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など) が必要です。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷 (速さ) による CipherSuite のランク (速い順) を定義します。

1. SSL_RSA_WITH_DES_CBC_SHA : メッセージの暗号化に DES-CBC、およびメッセージ ダイジェストに SHA を使用した RSA の鍵交換 (RSA 公開鍵暗号化)
2. SSL_RSA_WITH_RC4_128_MD5 : RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA の鍵交換
3. SSL_RSA_WITH_RC4_128_SHA : RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA の鍵交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA : メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージ ダイジェストに SHA を使用した RSA の鍵交換 (RSA 公開鍵暗号化)

(暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた) RSA は、SSL 接続において鍵の生成および認証の両方に使用されます。これは、CA の信頼点が設定されているかどうかにかかわらず。

セキュア HTTP サーバおよびクライアントの設定

ここでは、次の設定情報について説明します。

- 「SSL のデフォルト設定」 (P.9-53)
- 「SSL の設定時の注意事項」 (P.9-54)
- 「CA の信頼点の設定」 (P.9-54)
- 「セキュア HTTP サーバの設定」 (P.9-55)
- 「セキュア HTTP クライアントの設定」 (P.9-56)

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA の信頼点は設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンドで終了します。クラスタ メンバーのスイッチは標準の HTTP で動作させる必要があります。

CA の信頼点を設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチ スタックでは、SSL セッションはスタック マスターで終了します。

CA の信頼点の設定

セキュア HTTP 接続には、CA の信頼点を正式に設定することを推奨します。CA の信頼点は、自己署名証明書より高いセキュリティがあります。

CA の信頼点を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	hostname hostname	スイッチのホスト名を指定します (以前ホスト名を設定していない場合に限り必須)。ホスト名はセキュリティ鍵と証明書に必要です。
ステップ 3	ip domain-name domain-name	スイッチの IP ドメイン名を指定します (以前 IP ドメイン名を設定していない場合に限り必須)。IP ドメイン名はセキュリティ鍵と証明書に必要です。
ステップ 4	crypto key generate rsa	(任意) RSA 鍵のペアを生成します。RSA 鍵のペアは、スイッチの証明書を手に入れる前に必要です。RSA 鍵のペアは自動的に生成されます。必要であれば、このコマンドを使用して鍵を再生成できます。
ステップ 5	crypto ca trustpoint name	CA の信頼点にローカルの設定名を指定して、CA 信頼点コンフィギュレーション モードを開始します。
ステップ 6	enrollment url url	証明書の要求の送信先スイッチの URL を指定します。
ステップ 7	enrollment http-proxy host-name port-number	(任意) HTTP プロキシサーバを経由して CA から証明書を手に入れるようにスイッチを設定します。
ステップ 8	crl query url	ピアの証明書が取り消されていないかを確認するために、Certificate Revocation List (CRL; 証明書失効リスト) を要求するようにスイッチを設定します。
ステップ 9	primary	(任意) 信頼点が CA 要求に対してプライマリ (デフォルト) 信頼点として使用されるように指定します。
ステップ 10	exit	CA 信頼点コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	crypto ca authentication name	CA の公開鍵を取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	crypto ca enroll name	指定の CA の信頼点から証明書を取得します。このコマンドは、各 RSA 鍵のペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	end	特権 EXEC モードに戻ります。
ステップ 14	show crypto ca trustpoints	設定を確認します。
ステップ 15	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

`no crypto ca trustpoint name` グローバル コンフィギュレーション コマンドを使用して、CA に関連するすべての ID 情報および証明書を削除できます。

セキュア HTTP サーバの設定

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA 信頼点を設定してから、HTTP サーバを有効にする必要があります。CA の信頼点を設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定したあと、標準およびセキュア HTTP サーバ両方に適用するオプション（パス、適用するアクセスリスト、最大接続数、またはタイムアウトポリシー）を設定できます。

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>show ip http server status</code>	(任意) HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。 HTTP secure server capability: Present or HTTP secure server capability: Not present
ステップ2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>ip http secure-server</code>	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。
ステップ4	<code>ip http secure-port port-number</code>	(任意) HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ~ 65535 の範囲で指定できます。
ステップ5	<code>ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</code>	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴリズム) を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これがデフォルトです。
ステップ6	<code>ip http secure-client-auth</code>	(任意) HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ7	<code>ip http secure-trustpoint name</code>	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA の信頼点を指定します。 (注) このコマンドの使用は、前の手順に従って CA の信頼点をすでに設定しているという前提を踏まえて説明しています。
ステップ8	<code>ip http path path-name</code>	(任意) HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します (通常、システムのフラッシュ メモリを指定します)。
ステップ9	<code>ip http access-class access-list-number</code>	(任意) HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ10	<code>ip http max-connections value</code>	(任意) HTTP サーバへの同時最大接続数を指定します。指定できる範囲は 1 ~ 16 です。デフォルトは 5 です。

	コマンド	目的
ステップ 11	<code>ip http timeout-policy idle seconds life seconds requests value</code>	(任意) 指定の状況下における、HTTP サーバへの接続最大時間を指定します。 <ul style="list-style-type: none"> • idle : データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ~ 600 秒です。デフォルト値は 180 秒 (3 分) です。 • life : 接続を確立している最大時間。指定できる範囲は 1 ~ 86400 秒です (24 時間)。デフォルト値は 180 秒です。 • requests : 永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルト値は 1 です。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip http server secure status</code>	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

標準の HTTP サーバをディセーブルにするには、**no ip http server** グローバル コンフィギュレーション コマンドを使用します。セキュア HTTP サーバをディセーブルにするには、**no ip http secure-server** グローバル コンフィギュレーション コマンドを使用します。デフォルトの設定に戻すには、**no ip http secure-port** および **no ip http secure-ciphersuite** グローバル コンフィギュレーション コマンドを使用します。クライアント認証の要件を削除するには、**no ip http secure-client-auth** グローバル コンフィギュレーション コマンドを使用します。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、`https://URL` を入力します (URL は IP アドレス、またはサーバスイッチのホスト名)。デフォルト ポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

セキュア HTTP クライアントの設定

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA の信頼点をスイッチに設定していることを前提としています。CA の信頼点が設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip http client secure-trustpoint name</code>	(任意) リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA の信頼点を指定します。このコマンドの使用は、前の手順を使用して CA の信頼点をすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリ の信頼点がすでに設定されている場合は、このコマンドは任意です。

コマンド	目的
ステップ3 <code>ip http client secure-ciphersuite</code> {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴリズム) を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これがデフォルトです。
ステップ4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ5 <code>show ip http client secure status</code>	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

クライアントの信頼点の設定を削除するには、`no ip http client secure-trustpoint name` コマンドを使用します。クライアントにすでに設定されている CipherSuite 仕様を削除するには、`no ip http client secure-ciphersuite` コマンドを使用します。

セキュア HTTP サーバおよびクライアントのステータスの表示

SSL セキュア サーバおよびクライアントのステータスを表示するには、表 9-7 に記載された特権 EXEC コマンドを使用します。

表 9-7 SSL セキュア サーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
<code>show ip http client secure status</code>	セキュア HTTP クライアントの設定を表示します。
<code>show ip http server secure status</code>	セキュア HTTP サーバの設定を表示します。
<code>show running-config</code>	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

SCP のためのスイッチの設定

Secure Copy Protocol (SCP) 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供します。SCP には SSH が必要です (Berkeley の r-tools に代わるセキュリティの高いアプリケーションおよびプロトコルです)。

SSH を動作させるには、スイッチに RSA の公開鍵と秘密鍵のペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらの鍵のペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、および許可を適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA 鍵のペアが必要です。



(注)

SCP を使用する場合、コピー コマンドにパスワードを入力できません。プロンプトが表示されたときに、入力する必要があります。

Secure Copy に関する情報

Secure Copy 機能を設定するには、次の概念を理解する必要があります。

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol (RCP) と類似しています。また、SCP の設定には AAA の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。

適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System (IFS) のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

SCP の設定および検証方法の詳細は、次の URL にアクセスして、Cisco IOS Release 12.2 の『Cisco IOS New Features』から「Secure Copy Protocol」の章を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html



CHAPTER 10

IEEE 802.1X ポートベース認証の設定

IEEE 802.1x ポートベース認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

コマンドの構文と使用方法の詳細については、Catalyst 3750 のスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 の「RADIUS Commands」のセクションを参照してください。

- [「IEEE 802.1X ポートベース認証の概要」 \(P.10-1\)](#)
- [「802.1X 認証の設定」 \(P.10-33\)](#)
- [「802.1X の統計情報およびステータスの表示」 \(P.10-66\)](#)

IEEE 802.1X ポートベース認証の概要

標準では、一般の人がアクセス可能なポートから無許可のクライアントが LAN に接続しないように規制する、クライアント/サーバ型のアクセス制御および認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN のサービスを利用できるようにします。

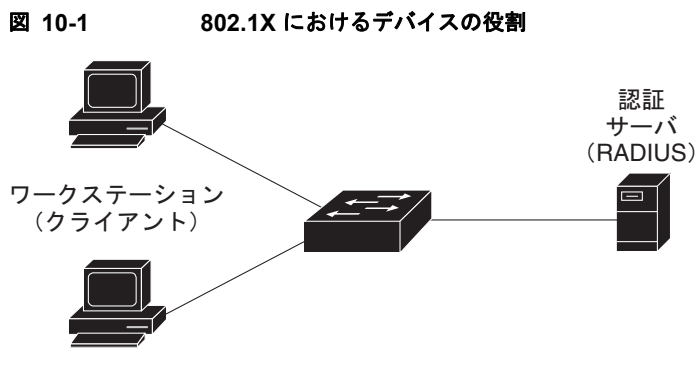
IEEE 802.1X アクセス制御では、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL)、Cisco Discovery Protocol (CDP)、および Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) トラフィックしか許可されません。認証後、通常のトラフィックをポート経由で送受信します。

- [「デバイスの役割」 \(P.10-2\)](#)
- [「認証プロセス」 \(P.10-3\)](#)
- [「認証の開始およびメッセージ交換」 \(P.10-5\)](#)
- [「認証マネージャ」 \(P.10-7\)](#)
- [「許可ステートおよび無許可ステートのポート」 \(P.10-10\)](#)
- [「802.1X 認証とスイッチ スタック」 \(P.10-11\)](#)
- [「802.1X のホスト モード」 \(P.10-12\)](#)
- [「マルチドメイン認証」 \(P.10-12\)](#)
- [「802.1X マルチ認証モード」 \(P.10-14\)](#)
- [「MAC 移動」 \(P.10-14\)](#)

- 「802.1X アカウンティング」 (P.10-15)
- 「802.1X アカウンティングアトリビュート値 (AV) ペア」 (P.10-15)
- 「802.1X 準備チェック」 (P.10-16)
- 「VLAN 割り当てを使用した 802.1X 認証」 (P.10-16)
- 「ユーザ単位 ACL を使用した 802.1X 認証の利用」 (P.10-18)
- 「ゲスト VLAN を使用した 802.1X 認証」 (P.10-21)
- 「制限付き VLAN による 802.1X 認証」 (P.10-22)
- 「アクセス不能認証バイパスによる 802.1X 認証」 (P.10-23)
- 「音声 VLAN ポートを使用した 802.1X 認証」 (P.10-24)
- 「ポートセキュリティを使用した 802.1X 認証」 (P.10-25)
- 「Wake-on-LAN (WoL) 機能を使用した 802.1X 認証」 (P.10-26)
- 「MAC 認証バイパスを使用した 802.1X 認証」 (P.10-26)
- 「802.1X ユーザ分散」 (P.10-28)
- 「NAC レイヤ 2 802.1X 検証」 (P.10-28)
- 「柔軟な認証の順序」 (P.10-29)
- 「OpenIx 認証」 (P.10-29)
- 「音声認識 802.1X セキュリティの使用」 (P.10-30)
- 「Network Edge Access Topology (NEAT) を使用した 802.1X サプリカントスイッチおよびオーセンティケータスイッチ」 (P.10-30)
- 「ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証」 (P.10-19)
- 「ACL および RADIUS Filter-Id アトリビュートによる IEEE 802.1X 認証の使用」 (P.10-31)
- 「共通セッション ID」 (P.10-32)

デバイスの役割

802.1X ポートベース認証を使用するデバイスの役割



- クライアント: LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス (ワークステーション)。ワークステーションでは、Microsoft Windows XP OS (オペレーティング システム) に付属しているような 802.1X 準拠のクライアント ソフトウェアを実行する必要があります (クライアントは、802.1X 標準ではサブリクアントといえます)。



(注) Windows XP のネットワーク接続および 802.1X 認証については、次の URL にある「Microsoft Knowledge Base」を参照してください。
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- 認証サーバ: クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol (EAP) 拡張機能を備えた Remote Authentication Dial-In User Service (RADIUS) セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- スイッチ (エッジ スイッチまたはワイヤレス アクセス ポイント): クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス (プロキシ) として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています (スイッチは、802.1X 標準ではオーセンティケータと呼ばれます)。

スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われなため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

仲介デバイスとして動作できるものには、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940、またはワイヤレス アクセス ポイントがあります。これらのデバイスでは、RADIUS クライアントおよび 802.1X 認証をサポートするソフトウェアが稼動している必要があります。

認証プロセス

802.1X ポートベース認証がイネーブルであり、クライアントが 802.1X 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1X 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。

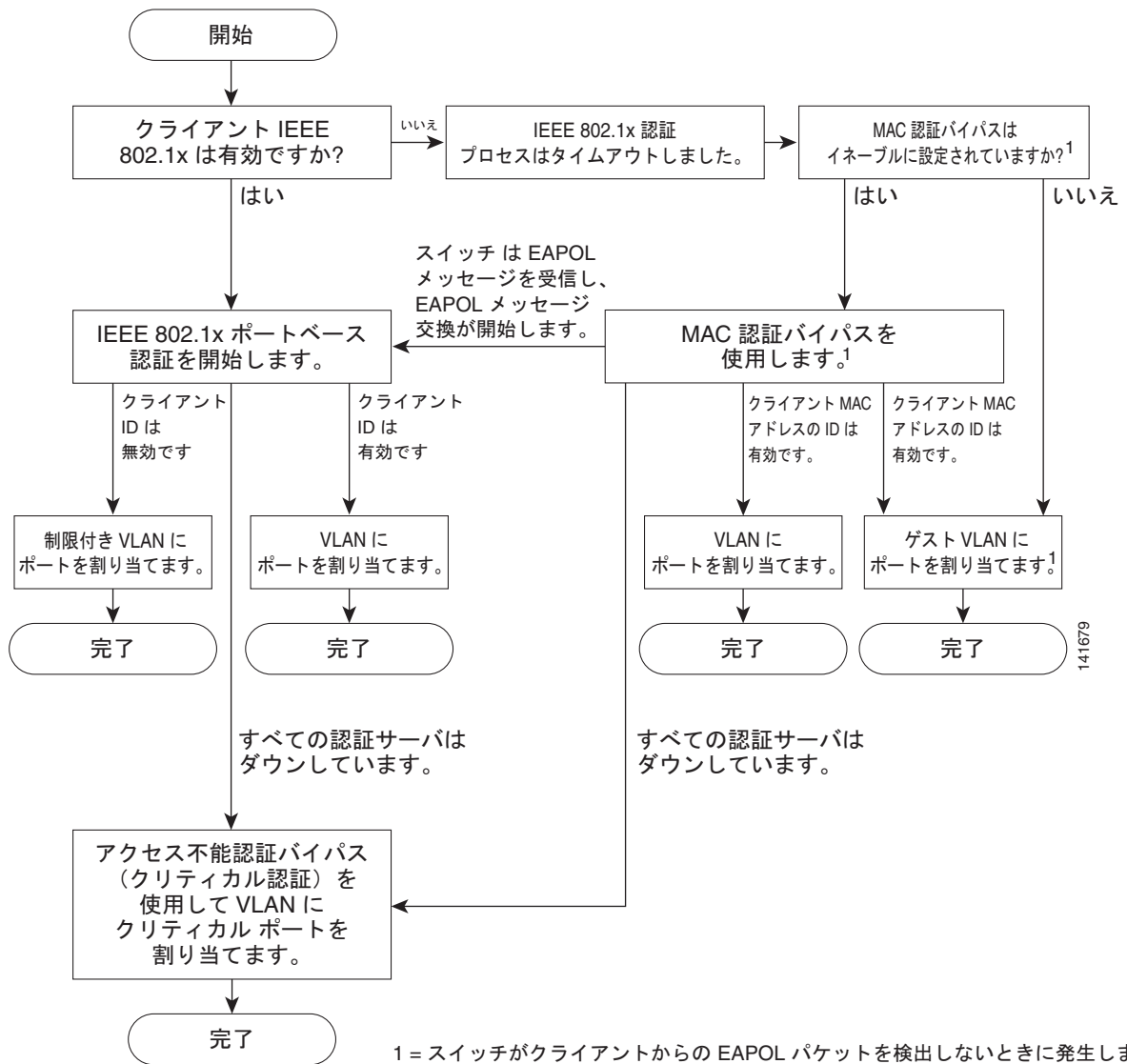
- スイッチが 802.1X 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証状態にして、クライアントにネットワークのアクセスを許可します。



(注) アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) 失敗ポリシーとも呼ばれます。

図 10-2 に、認証プロセスを示します。

図 10-2 認証フローチャート



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

RADIUS サーバを使用する 802.1X 認証を設定したあと、スイッチは、Session-Timeout RADIUS アトリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリビュート [29]) に基づいてタイマーを使用します。

Session-Timeout RADIUS アトリビュート (アトリビュート [27]) は、再認証が発生するまでの時間を指定します。

Termination-Action RADIUS アトリビュート (アトリビュート [29]) は、再認証中に行うアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。*Initialize* アクションが設定されていると (アトリビュートの値は *DEFAULT*)、802.1X セッションが終了し、再認証中に接続が切断されます。*ReAuthenticate* アクションが設定されていると (アトリビュートの値は RADIUS-Request)、再認証中にセッションは影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface interface-id** 特権 EXEC コマンドを入力します。

Multidomain Authentication (MDA; マルチドメイン認証) がポートでイネーブルの場合、音声認証に適用可能ないくつかの例外とともにこのフローを使用することができます。MDA の詳細については、「[マルチドメイン認証](#)」(P.10-12) を参照してください。

認証の開始およびメッセージ交換

802.1X 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** または **dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにした場合、スイッチはポートのリンク ステータスがダウンからアップに変更した時点で、またはポートが認証されてないままアップの状態であるかぎり定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。



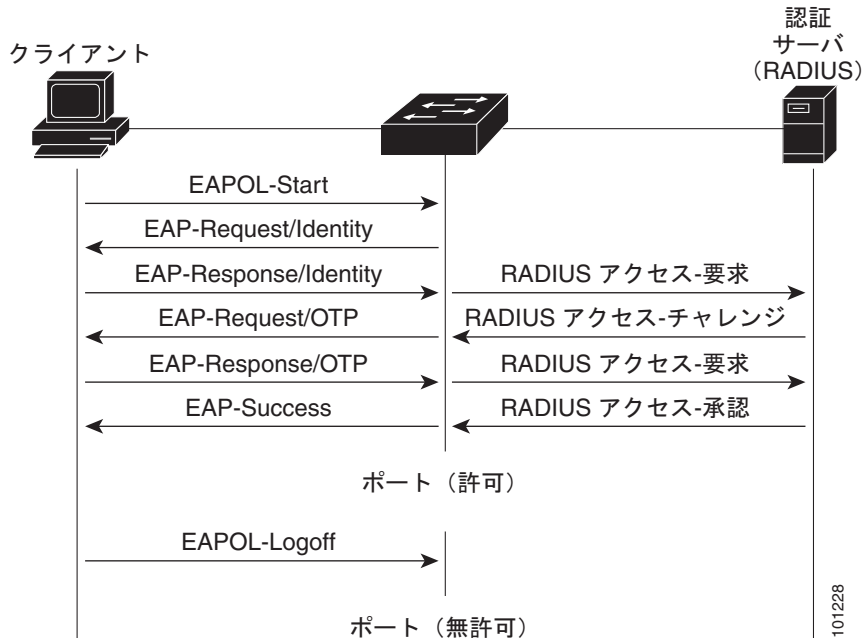
(注)

ネットワーク アクセス デバイスで 802.1X 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステータスであるものとしてフレームを送信します。ポートが許可ステータスであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「[許可ステータスおよび無許可ステータスのポート](#)」(P.10-10) を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステータスになります。認証に失敗した場合、認証が再実行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「[許可ステータスおよび無許可ステータスのポート](#)」(P.10-10) を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 10-3 に、クライアントが RADIUS サーバとの間で One-Time-Password (OTP; ワンタイム パスワード) 認証方式を使用する際に行われるメッセージ交換を示します。

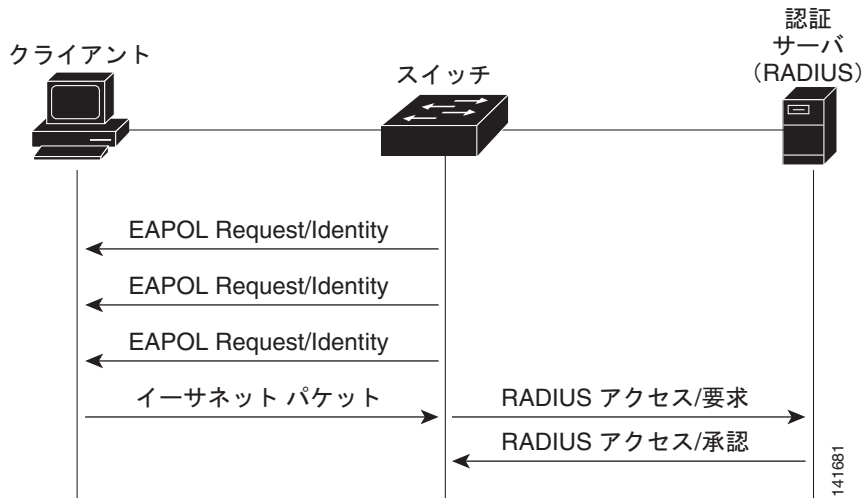
図 10-3 メッセージ交換



EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS アクセス/要求フレームにこの情報を保存します。サーバがスイッチに RADIUS アクセス/承認フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1X 認証を停止します。

図 10-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 10-4 MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、このスイッチ上で、および Catalyst 6000 などのその他のネットワーク デバイス上でも、CLI コマンドとメッセージを含め、同じ認証方式を使用できませんでした。個別の認証設定を使用する必要がありました。Cisco IOS Release 12.2(50)SE 以降では、ネットワーク内のすべての Catalyst スイッチ上で、同じ認証方式をサポートしています。

- 「ポートベース認証」 (P.10-7)
- 「ユーザ単位 ACL と Filter-Id」 (P.10-8)
- 「認証マネージャの CLI コマンド」 (P.10-9)

ポートベース認証

表 10-1 に、これらのホスト モードでサポートされる認証方式を示します。

- シングル ホスト：1 つのポートで 1 つのデータ ホストだけまたは音声ホスト（クライアント）だけが認証されることができます。
- マルチ ホスト：同一のポートで複数のデータホストが認証されることができます（ポートがマルチ ホスト モードで無許可になると、スイッチはすべての接続されたクライアントへのネットワーク アクセスを拒否します）。
- マルチドメイン認証（MDA）：データ装置と音声装置の両方が、同一のスイッチ ポートで認証されることができます。ポートは、データ ドメインと音声ドメインに分けられます。
- マルチ認証：複数のホストがデータ VLAN 上で認証を行えます。このモードでは、音声 VLAN が設定されている場合は、VLAN に 1 つのクライアントも可能です。

表 10-1 802.1X の機能

認証方式	モード			
	シングル ホスト	マルチ ホスト	MDA ¹	マルチ認証 ²
802.1X	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL ⁴ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID アトリビュート ³ ダウンロード可能な ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-ID アトリビュート ³ ダウンロード可能な ACL ³ リダイレクト URL ³
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード可能な ACL ³ リダイレクト URL ³	VLAN 割り当て ユーザ単位 ACL ³ Filter-ID アトリビュート ³ ダウンロード可能な ACL ³ リダイレクト URL ³	ユーザ単位 ACL ³ Filter-ID アトリビュート ³ ダウンロード可能な ACL ³ リダイレクト URL ³
スタンドアロン Web 認証 ⁴	プロキシ ACL、Filter-ID アトリビュート、ダウンロード可能な ACL ²			
NAC レイヤ 2 IP 検証	Filter-ID アトリビュート ³ ダウンロード可能な ACL リダイレクト URL	Filter-ID アトリビュート ³ ダウンロード可能な ACL リダイレクト URL	Filter-ID アトリビュート ³ ダウンロード可能な ACL リダイレクト URL	Filter-ID アトリビュート ³ ダウンロード可能な ACL ³ リダイレクト URL ³
フォールバック メソッドとしての Web 認証 ⁵	プロキシ ACL Filter-ID アトリビュート ³ ダウンロード可能な ACL ³	プロキシ ACL Filter-ID アトリビュート ³ ダウンロード可能な ACL ³	プロキシ ACL Filter-ID アトリビュート ³ ダウンロード可能な ACL ³	プロキシ ACL ³ Filter-ID アトリビュート ³ ダウンロード可能な ACL ³

1. MDA = マルチドメイン認証。

2. *multiauth* とも呼ばれます。

3. Cisco IOS Release 12.2(50)SE 以降でサポートされます。

4. Cisco IOS Release 12.2(50)SE 以降でサポートされます。

5. 802.1X 認証をサポートしないクライアント用です。

ユーザ単位 ACL と Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id は、シングル ホストモードでだけサポートされました。Cisco IOS Release 12.2(50) では、MDA およびマルチ認証がイネーブルであるポートのサポートが追加されました。12.2(52)SE 以降では、マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチ上で設定された Access Control List (ACL; アクセス コントロール リスト) は、Catalyst 6000 スイッチなどの Cisco IOS ソフトウェアを実行している別のデバイスで設定された ACL との互換性がありません。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行している他のデバイスと互換性があります。



(注) ACL では **any** だけをソースとして設定できます。



(注) マルチ ホスト モードに対して設定された ACL では、ステートメントのソース部分は、**any** でなければなりません (たとえば、**permit icmp any host 10.10.1.1**)。

定義された ACL のソース部分に **any** を指定する必要があります。そうしなければ、ACL は適用できず、認証は失敗します。シングル ホストだけが下位互換性サポートから除外されます。

MDA がイネーブルのポートおよびマルチ認証のポートで、2 つ以上のホストを認証できます。1 つのホストに適用された ACL ポリシーは別のホストのトラフィックに影響を与えません。

マルチホストのポートで 1 つのホストだけが認証され、他のホストは認証なしでネットワーク アクセスを取得した場合、ソース アドレスに **any** を指定することで 1 番めのホストに対する ACL ポリシーを他の接続されたホストにも適用できます。

認証マネージャの CLI コマンド

認証マネージャのインターフェイス コンフィギュレーション コマンドは 802.1X、MAC 認証バイパス、Web 認証などのすべての認証方式を制御します。認証マネージャのコマンドは、接続されたホストに適用される認証方式のプライオリティと順序を決定します。

認証マネージャのコマンドは、ホスト モード、違反モード、認証タイマーなどの汎用認証機能を制御します。汎用認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** インターフェイス コンフィギュレーション コマンドが含まれます。

802.1X 固有のコマンドは **dot1x** キーワードで開始します。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイス上での認証をイネーブルにします。ただし、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは、グローバルにのみ 802.1X 認証をイネーブルまたはディセーブルにします。



(注) 802.1X 認証がグローバルにディセーブルになっている場合は、そのポートでは Web 認証などの他の認証方式はまだイネーブルになっています。

authentication manager コマンドは、以前の 802.1X コマンドと同じ機能を提供します。

表 10-2 認証マネージャのコマンドおよび以前の 802.1X コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1X コマンド	説明
<code>authentication control-direction {both in}</code>	<code>dot1x control-direction {both in}</code>	wake-on-LAN (WoL) 機能を使用して認証をイネーブルにし、ポート コントロールを双方向または単方向に設定します。
<code>authentication event</code>	<code>dot1x auth-fail vlan</code> <code>dot1x critical (interface configuration)</code> <code>dot1x guest-vlan6</code>	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能をイネーブルにします。 アクティブ VLAN をゲスト VLAN として指定します。
<code>authentication fallback fallback-profile</code>	<code>dot1x fallback fallback-profile</code>	認証をサポートしないクライアントのフォールバック メソッドとして Web 認証を使用するようにポートを設定します。
<code>authentication host-mode [multi-auth multi-domain multi-host single-host]</code>	<code>dot1x host-mode {single-host multi-host multi-domain}</code>	認証済みポート上で単一のホスト (クライアント) または複数のホストを許可します。
<code>authentication order</code>	<code>dot1x mac-auth-bypass</code>	使用される認証方式の順序の定義に柔軟性を与えます。
<code>authentication periodic</code>	<code>dot1x reauthentication</code>	クライアントの定期的な再認証をイネーブルにします。
<code>authentication port-control {auto force-authorized force-unauthorized}</code>	<code>dot1x port-control {auto force-authorized force-unauthorized}</code>	ポートの許可ステータスの手動での制御をイネーブルにします。
<code>authentication timer</code>	<code>dot1x timeout</code>	タイマーを設定します。
<code>authentication violation {protect restrict shutdown}</code>	<code>dot1x violation-mode {shutdown restrict protect}</code>	ポートに新しいデバイスが接続されたとき、またはあるポートに最大数のデバイスが接続された後にそのポートに新しいデバイスが接続されたときに発生する違反モードを設定します。

詳細については、このリリースのコマンド リファレンスを参照してください。

許可ステートおよび無許可ステートのポート

802.1X 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN (仮想 LAN) ポートとして設定されていないポートは 802.1X 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは *許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN として設定されている場合、VoIP トラフィックおよび 802.1X プロトコル パケットが許可されたあとクライアントが正常に認証されます。

802.1X をサポートしていないクライアントが、無許可ステートの 802.1X ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1X 対応のクライアントが、802.1X 標準が稼動していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。また、応答がない場合は、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control または **dot1x port-control** インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御します。

- **force-authorized** : 802.1X 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- **force-unauthorized** : クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、ポートを介してクライアントに認証サービスを提供できません。
- **auto** : 802.1X 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC (メディア アクセス制御) アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると (認証サーバから **Accept** フレームを受信すると)、ポートが許可ステートに変わり、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可されます。認証に失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1X 認証とスイッチ スタック

スイッチがスイッチ スタックで追加または削除されても、RADIUS サーバとスタック間の IP 接続が保たれているかぎり、802.1X 認証に影響はありません。このことは、スタック マスターがスイッチ スタックから削除された場合にも当てはまります。スタック マスターに障害が生じると、スタック メンバーが [第 5 章「スイッチ スタックの管理」](#)に記載されている選択プロセスを使用して新たなスタック マスターとなり、802.1X 認証プロセスは通常どおり継続されることに注意してください。

サーバに接続されていたスイッチが削除されたり、またはそのスイッチに障害が発生したりといった理由で RADIUS サーバへの IP 接続が切断された場合には、次のイベントが発生します。

- すでに認証済みで定期的な再認証がイネーブル化されていないポートは、認証ステートのままです。RADIUS サーバとの通信は必要ありません。
- すでに認証済みで、定期的な再認証がイネーブル化されているポートは (**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用して)、再認証時に認証プロセスに失敗します。ポートは、再認証プロセスで未認証ステートに戻ります。RADIUS サーバとの通信が必要です。

進行中の認証は、サーバ接続がないため即座に失敗します。

障害の発生したスイッチが再びアップし、スイッチ スタックに参加した場合は、起動時間と、認証が試行されるまでに RADIUS サーバへの接続が再確立されたかどうかによって、認証は失敗することもあります。

RADIUS サーバ接続の切断を回避するには、冗長接続を確立しておく必要があります。たとえば、スタック マスターへの冗長接続とスタック メンバーへの別の冗長接続を確立しておけば、スタック マスターに障害が発生しても、スイッチ スタックは RADIUS サーバへの接続を維持できます。

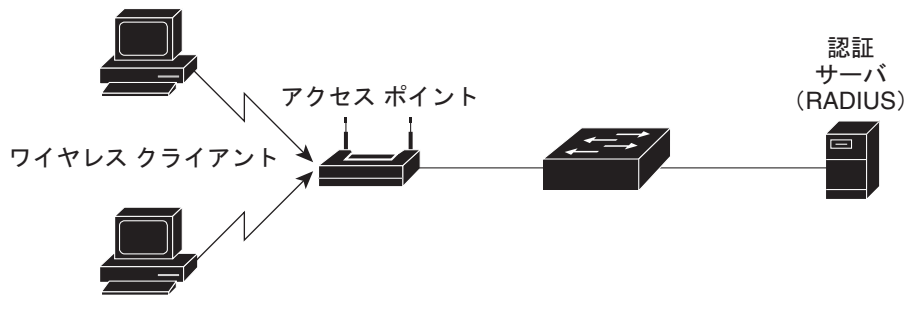
802.1X のホスト モード

IEEE 802.1X ポートは、シングルホスト モードまたはマルチホスト モードで設定できます。シングルホスト モード (図 10-1 (P.10-2) を参照) では、802.1X 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステータスがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステータスをダウンに変更し、ポートは無許可ステータスに戻ります。

マルチホスト モードでは、複数のホストを単一の 802.1X 対応ポートに接続できます。図 10-5 (P.10-12) に、ワイヤレス LAN における 802.1X ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステータスになると (再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合)、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチホスト モードがイネーブルの場合、802.1X 認証を使用してポートおよびポート セキュリティを認証し、クライアントを含むすべての MAC アドレスのネットワーク アクセスを管理できます。

図 10-5 マルチホスト モードの例



このスイッチは、マルチドメイン認証 (MDA) をサポートしています。これにより、データ デバイスと (シスコまたはシスコ以外の) IP 電話のような音声デバイスの両方が、同一のスイッチ ポートに接続できます。詳細については、「マルチドメイン認証」(P.10-12) を参照してください。

マルチドメイン認証

このスイッチは、MDA をサポートしています。これにより、データ デバイスと (シスコまたはシスコ以外の) IP 電話のような音声デバイスの両方が、同一のスイッチ ポートを認証することができます。ポートは、データ ドメインと音声ドメインに分けられます。

MDA は、デバイス認証の順序を強制しません。しかし、最良の結果を出すには、MDA 対応ポートでは音声デバイスをデータ デバイスの前に認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA 用にスイッチ ポートを設定するには、「ホスト モードの設定」(P.10-43) を参照してください。

- ホスト モードがマルチドメインに設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 14 章「VLAN の設定」を参照してください。
- Cisco IOS Release 12.2(40)SE 以降のリリースでは、MDA 対応ポートでの音声 VLAN 割り当てをサポートしています。



(注) ダイナミック VLAN を使用して音声 VLAN を Cisco IOS Release 12.2(37)SE の動作する MDA 対応スイッチ ポートに割り当てると、音声デバイスで許可が失敗します。

- 音声デバイスを許可するには、`device-traffic-class=voice` という値を持ったシスコ Attribute-Value (AV; アトリビュート値) ペア アトリビュートを送信するように、AAA サーバを設定する必要があります。この値がない場合、スイッチは音声デバイスをデータ デバイスとして扱います。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応レポートのデータ デバイスだけに適用されます。スイッチは、許可に失敗した音声デバイスをデータ デバイスとして扱います。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、`errdisable` になります。
- デバイスが許可されるまで、ポートでトラフィックが廃棄されます。シスコ製以外の IP 電話や音声デバイスがデータおよび音声 VLAN で許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得できます。音声デバイスが音声 VLAN で送信を開始したあと、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック メカニズムとして MAC 認証バイパスを使用して、802.1X 認証をサポートしていないデバイスにスイッチポートを接続することができます。詳細については、「MAC 認証バイパス」(P.10-36) を参照してください。
- データまたは音声デバイスがポートで検出されると、許可に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが無許可である間に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは `errdisable` になります。
- ポートのホスト モードがシングルホストまたはマルチホストからマルチドメイン モードに変更される際に、許可済みのデータ デバイスはポートで許可済みのままになります。ただし、ポート音声 VLAN 上の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。
- ポートがシングルホストまたはマルチホスト モードからマルチドメイン モードに変更されたあとに、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック メカニズムは設定されたままになります。
- マルチドメイン モードからシングルホストまたはマルチホスト モードにポートを切り替えると、ポートからすべての許可済みデバイスが削除されます。
- データ ドメインがまず許可されてゲスト VLAN に配置された場合、802.1X 非対応音声デバイスは認証をトリガするために音声 VLAN 上のパケットにタグを付ける必要があります。電話はタグ付きトラフィックを送信する必要はありません (802.1X 対応電話も同様です)。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを有する許可済みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。ポート上の 1 つのデバイスだけを使用してユーザ単位 ACL を実行することができます。

詳細については、「ホスト モードの設定」(P.10-43) を参照してください。

802.1X マルチ認証モード

マルチ認証 (multiauth) モードは、音声 VLAN 上のデータ VLAN 上の複数の認証済みクライアントを許可します。各ホストは別々に認証されます。音声 VLAN が設定されている場合、このモードでは VLAN 上に 1 つのクライアントが可能です (ポートがその他の音声クライアントを検知すると、その音声クライアントはポートから破棄されますが、違反エラーは発生しません)。

ハブまたはアクセスポイントが 802.1X 対応ポートに接続されている場合、接続されているクライアントは認証される必要があります。

802.1X 非対応デバイスでは、個別のホスト認証が単一のポート上でさまざまな方式によってホスト単位で認証するためのフォールバック メソッドとして MAC 認証バイパスまたは Web 認証を使用できます。

マルチ認証ポート上で認証されるデータ ホストの数に制限はありません。しかし、音声デバイスが設定されている場合は、1 つのデバイスだけが許可されます。違反がトリガーされることを定義されたホストの制限がないため、別の音声デバイスが見つかったときは、何も通知せずに破棄され違反はトリガーされません。

音声 VLAN の MDA 機能の場合、マルチ認証モードは、認証サーバから受信した VSA に応じて認証済みデバイスをデータまたは音声 VLAN のいずれかに割り当てます。



(注)

ポートがマルチ認証モードの場合、RADIUS サーバにより提供される VLAN 割り当て、ゲスト VLAN、および認証失敗 VLAN がアクティブにされることはありません。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「[アクセス不能認証バイパスによる 802.1X 認証](#)」(P.10-23) を参照してください。

ポートのマルチ認証モードの詳細については、「[ホスト モードの設定](#)」(P.10-43) を参照してください。

MAC 移動

あるスイッチで MAC アドレスが認証されている場合、そのアドレスはスイッチの別の 802.1X ポート上では許可されません。スイッチが別の 802.1X ポートに同一の MAC アドレスを検知すると、そのアドレスは許可されません。

MAC アドレスをあるポートから同一スイッチの別のポートに移動する必要がある場合があります。たとえば、認証されたホストとスイッチポートの間にもう一つのデバイス (ハブや IP 電話など) がある場合、ホストをデバイスから接続解除し、同一スイッチの別のポートに直接接続する場合があります。

デバイスが新しいポートで再認証されるように MAC 移動をグローバルにイネーブルにできます。別のポートにホストが移動した場合、1 番めのポート上のセッションは削除され、新しいポート上でホストが再認証されます。

MAC 移動はすべてのホストモードでサポートされます (認証されたホストは、そのポートでイネーブルにされているホストモードにかかわらず、スイッチの任意のポートに移動できます)。



(注)

MAC 移動は、ポート セキュリティ対応 802.1X ポートではサポートされません。スイッチ上で MAC 移動がグローバルに設定され、ポート セキュリティ対応ホストが 802.1X 対応ポートに移動すると違反エラーが発生します。

詳細については、「[MAC 移動のイネーブル化](#)」(P.10-49) を参照してください。

802.1X アカウンティング

802.1X 標準では、ユーザのネットワーク アクセスに対するユーザの許可および認証方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1X アカウンティングは、デフォルトでディセーブルです。802.1X アカウンティングをイネーブルにすると、次のアクティビティを 802.1X 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログオフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1X アカウンティング情報を記録しません。その代わりに、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1X アカウンティング アトリビュート値 (AV) ペア

RADIUS サーバに送信された情報は、アトリビュート値 (AV) ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます (たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets アトリビュートの情報が必要です)。

AV ペアは、802.1X アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START : 新規ユーザセッションが始まると送信されます。
- INTERIM : 既存のセッションが更新されると送信されます。
- STOP : セッションが終了すると送信されます。

次の表 10-3 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 10-3 アカウンティング AV ペア

アトリビュート番号	AV ペア名	START	INTERIM	STOP
アトリビュート [1]	User-Name	常時送信	常時送信	常時送信
アトリビュート [4]	NAS-IP-Address	常時送信	常時送信	常時送信
アトリビュート [5]	NAS-Port	常時送信	常時送信	常時送信
アトリビュート [8]	Framed-IP-Address	非送信	条件に応じて送信 ¹	条件に応じて送信 ¹
アトリビュート [25]	Class	常時送信	常時送信	常時送信
アトリビュート [30]	Called-Station-ID	常時送信	常時送信	常時送信
アトリビュート [31]	Calling-Station-ID	常時送信	常時送信	常時送信
アトリビュート [40]	Acct-Status-Type	常時送信	常時送信	常時送信
アトリビュート [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
アトリビュート [42]	Acct-Input-Octets	非送信	常時送信	常時送信
アトリビュート [43]	Acct-Output-Octets	非送信	常時送信	常時送信

表 10-3 アカウンティング AV ペア (続き)

アトリビュート番号	AV ペア名	START	INTERIM	STOP
アトリビュート [44]	Acct-Session-ID	常時送信	常時送信	常時送信
アトリビュート [45]	Acct-Authentic	常時送信	常時送信	常時送信
アトリビュート [46]	Acct-Session-Time	非送信	常時送信	常時送信
アトリビュート [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
アトリビュート [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol (DHCP) バインディングが DHCP スーピング バインディング テーブルに存在している場合に限り、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、次の URL で『Cisco IOS Debug Command Reference』 Release 12.2 を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

AV ペアの詳細については、RFC 3580 『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1X 準備チェック

802.1X 準備チェックは、すべてのスイッチ ポート上で 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続されたデバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。802.1X 機能をサポートしていないデバイスについては、MAC 認証バイパスまたは Web 認証などの認証を変更できます。

この機能は、クライアントのサブリカントが NOTIFY EAP 通知パケットのクエリーをサポートしている場合に限り有効です。クライアントは 802.1X タイムアウト値内に応答する必要があります。

802.1X 準備チェックに関するスイッチ設定の詳細は、「[802.1X 準備チェックの設定](#)」(P.10-37) を参照してください。

VLAN 割り当てを使用した 802.1X 認証

RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ データベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されて RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証 (MDA) 対応ポート上でデータ VLAN 割り当てと同じように動作します。詳細については、「[マルチドメイン認証](#)」(P.10-12) を参照してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1X 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1X 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN はアクセス ポートに割り当てられた VLAN であることを思い出してください。このポートで送受信されるすべてのパケットはこの VLAN に所属します。
- 802.1X 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッドポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッドポート）の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホストポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。

- 802.1X 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1X ポートでマルチホストモードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポートセキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1X 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1X ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
 - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホストモードがディセーブルになります。
 - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホストモードがディセーブルになります。

ポートが、強制許可 (force-authorized) ステート、強制無許可 (force-unauthorized) ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

トランクポート、ダイナミックポート、または VLAN Membership Policy Server (VMPS; VLAN メンバシップポリシーサーバ) によるダイナミックアクセスポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします。(アクセスポートで 802.1X 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネルアトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに返す必要があります。
 - [64] Tunnel-Type = VLAN

- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID、または VLAN グループ
- [83] Tunnel-Preference

アトリビュート [64] は、値 *VLAN* (タイプ 13) でなければなりません。アトリビュート [65] は、値 *802* (タイプ 6) でなければなりません。アトリビュート [81] は、802.1X 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

トンネルアトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」(P.9-36) を参照してください。

ユーザ単位 ACL を使用した 802.1X 認証の利用

ユーザ単位の Access Control List (ACL; アクセスコントロールリスト) をイネーブルにして、802.1X 認証ユーザに対して異なるレベルのネットワーク アクセスおよびサービスを提供します。RADIUS サーバが 802.1X ポートに接続されたユーザを認証すると、ユーザ ID に基づいて ACL アトリビュートを取得してスイッチに送信します。スイッチは、ユーザセッションの期間中、そのアトリビュートを 802.1X ポートに適用します。セッションが終了した場合、認証が失敗した場合、またはリンクダウン状態になった場合には、スイッチはユーザ単位の ACL を削除します。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションに保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL の設定およびポート ACL の入力を行うことができます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力済みのルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。発信するルーテッドパケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を避けるために、RADIUS サーバに格納するユーザプロファイルを慎重に計画します。

RADIUS は、ベンダー固有のアトリビュートなどのユーザ単位アトリビュートをサポートします。これらのベンダー固有のアトリビュート (VSA) は、オクテットストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。スイッチは、入力方向に限り VSA をサポートします。このスイッチでは、レイヤ 2 ポートで出力方向のポート ACL はサポートされません。詳細は、第 35 章「ACL によるネットワークセキュリティの設定」を参照してください。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位の設定を定義します。RADIUS サーバから定義が渡されると、拡張命名規則を使用して作成されます。ただし、Filter-Id アトリビュートを使用する場合、標準 ACL を示すことができます。

Filter-Id アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す `.in` または `.out` が含まれています。RADIUS サーバが `.in` または `.out` 構文を許可しない場合、アクセスリストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセスリストに関するサポートが制限されているため、Filter-ID アトリビュートは 1 ~ 199 および 1300 ~ 2699 の IP ACL (IP 標準 ACL および IP 拡張 ACL) に対してのみサポートされます。

ユーザ単位 ACL の最大サイズは 4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズによって制限されます。

ベンダー固有のアトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」(P.9-36) を参照してください。ACL の設定の詳細については、第 35 章「ACL によるネットワークセキュリティの設定」を参照してください。



(注) ユーザ単位 ACL は、シングル ホスト モードでだけサポートされます。

ユーザ単位の ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- シングルホスト モードの 802.1X ポートを設定します。

設定の詳細については、「[認証マネージャ](#)」(P.10-7) を参照してください。

ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証

ホストの 802.1X 認証または MAC 認証バイパスの間に、RADIUS サーバから ACL とリダイレクト URL をスイッチにダウンロードできます。Web 認証の間にも ACL をダウンロードすることもできます。



(注) ダウンロード可能な ACL は *dACL* とも呼ばれます。

ホスト モードがシングルホスト、MDA、またはマルチ認証である場合は、スイッチによって ACL のソースアドレスがホスト IP アドレスになるように変更されます。

ACL とリダイレクト URL は 802.1X 対応ポートに接続されているすべてのデバイスに適用できます。

802.1X 認証の間に ACL がダウンロードされない場合、スイッチはポート上のスタティック デフォルト ACL をホストに適用します。音声 VLAN ポート上では、スイッチは ACL を電話機だけに適用します。



(注) ダウンロード可能な ACL またはリダイレクト URL が認証サーバ上のクライアントに対して設定されている場合、接続されているクライアント スイッチ ポート上のデフォルト ポート ACL も設定されている必要があります。

リダイレクト URL に対する Cisco Secure ACS とアトリビュート値 (AV) ペア

スイッチは次の *cisco-av-pair* VSA を使用します。

- *url-redirect* は HTTP から HTTPS への URL です。
- *url-redirect-acl* はスイッチ ACL の名前または番号です。

スイッチは、CiscoSecure-Defined-ACL AV ペアを使用してエンドポイント デバイスからの HTTP または HTTPS 要求を代行受信します。その後、スイッチはクライアント Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure ACS 上の *url-redirect* AV ペアには、Web ブラウザのリダイレクト先である URL が含まれます。*url-redirect-acl* AV ペアには、リダイレクトする HTTP または HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL 内の許可 ACE に一致するトラフィックがリダイレクトされます。



(注) スイッチ上の URL リダイレクト ACL とデフォルト ポート ACL を定義します。

認証サーバ上のクライアントに対してリダイレクト URL が設定されている場合、接続されているクライアント スイッチ ポート上のデフォルト ポート ACL も設定されている必要があります。

ダウンロード可能な ACL に対する Cisco Secure ACS と AV ペア

RADIUS cisco-av-pair ベンダー固有のアトリビュート (VSA) を使用して Cisco Secure ACS 上の CiscoSecure-Defined-ACL AV ペアを設定できます。このペアは、#ACL#-IP-name-number アトリビュートを使用して Cisco Secure ACS 上でダウンロード可能な ACL を指定します。

- *name* は ACL 名です。
- *number* はバージョン番号 (たとえば、3f783768) です。

ダウンロード可能な ACL が認証サーバ上のクライアントに対して設定されている場合、接続されたクライアント スイッチ ポート上のデフォルト ポート ACL も設定されている必要があります。

デフォルト ACL がスイッチ上で設定されており、Cisco Secure ACS が host-access-policy をスイッチに送信している場合、スイッチ ポートに接続されているホストからトラフィックにそのポリシーが適用されます。このポリシーが適用されない場合、スイッチはデフォルト ACL を適用します。Cisco Secure ACS がスイッチにダウンロード可能な ACL を送信した場合、この ACL は、スイッチ ポート上で設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信していても、デフォルト ACL が設定されていない場合、許可の失敗が宣言されます。

設定の詳細については、「[認証マネージャ](#)」(P.10-7) および「[ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定](#)」(P.10-61) を参照してください。

VLAN ID ベースの MAC 認証

ダウンロード可能な VLAN の代わりに、スタティックな VLAN ID に基づいてホストを認証する場合、VLAN ID ベースの MAC 認証を使用できます。スイッチに設定されたスタティック VLAN ポリシーがある場合、認証のために各ホストの MAC アドレスと VLAN 情報が Internet Authentication Service (IAS) (Microsoft) RADIUS サーバに送信されます。接続されたポートに設定された VLAN ID が MAC 認証に使用されます。IAS サーバによる VLAN ID ベースの MAC 認証を使用することで、ネットワーク内に定まった個数の VLAN を所有できます。

この機能は、STP によってモニタされ、処理される VLAN の個数を制限します。ネットワークは固定された VLAN として管理されます。



(注) この機能は Cisco ACS サーバではサポートされません (ACS サーバは、送信された新しいホストの VLAN-ID を無視し、MAC アドレスだけに基いて認証します)。

設定手順については、「[VLAN ID ベースの MAC 認証の設定](#)」(P.10-63) を参照してください。その他の設定は、「[MAC 認証バイパスの設定](#)」(P.10-56) で説明される MAC 認証バイパスと同様です。

ゲスト VLAN を使用した 802.1X 認証

スイッチ上の各 802.1X ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます (802.1X クライアントのダウンロードなど)。これらのクライアントは 802.1X 認証用にシステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は 802.1X 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1X ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1X 対応の音声デバイスを許可するときに AAA が使用できない場合、認証は失敗しますが EAPOL パケットの検出は EAPOL 履歴に保存されます。その後 AAA サーバが使用できるようになれば、スイッチはその音声デバイスを認証します。ただし、スイッチは他のデバイスがゲスト VLAN へアクセスすることを許可しなくなります。この状態を回避するには、次のコマンドのいずれかを使用してください。

- **dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドに続けて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力し、ポートを再起動します。



(注)

インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1X 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1X 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1X 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、802.1X ポート上でシングルホスト モードまたはマルチホスト モードでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッド ポート) またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

スイッチは、MAC 認証バイパスをサポートします。MAC 認証バイパスが 802.1X ポートでイネーブルの場合、スイッチは、802.1X 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス/要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗した場合、ゲスト VLAN が指定されていれば、スイッチはポートをゲスト VLAN に割り当てます。詳細については、「[MAC 認証バイパスを使用した 802.1X 認証](#)」(P.10-26) を参照してください。

詳細については、「[ゲスト VLAN の設定](#)」(P.10-50) を参照してください。

制限付き VLAN による 802.1X 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 802.1X ポートに対して制限付き VLAN（*認証失敗 VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1X 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効な証明書を持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。



(注)

両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパンニング ツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることができます。再認証をディセーブルにすると、*link down* または *EAP logoff* イベントを受信しないかぎり、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の擬似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼動しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1X ポート上でシングルホスト モードの場合のみサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポート セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、*errdisable* ステートに移行します。

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査、DHCP スヌーピング、および IP 送信元ガードのような他のポート セキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「[制限付き VLAN の設定](#)」(P.10-51) を参照してください。

アクセス不能認証バイパスによる 802.1X 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストが認証されない場合、アクセス不能な認証バイパス機能（クリティカル認証または AAA 失敗ポリシーともいう）を使用します。これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカルポートへの接続を試みる時は、そのホストはユーザ定義アクセス VLAN クリティカル VLAN に移動されます。管理者は制限された認証をホストに与えます。

スイッチがクリティカルポートに接続されたホストの認証を行う際に、スイッチは設定された RADIUS サーバのステータスを確認します。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワークアクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

マルチ認証ポートに関するサポート

マルチ認証（multiauth）ポートでアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan *vlan-id*** を使用します。新しいホストがクリティカルポートに接続する場合、そのポートは再初期化され、接続されているホストはすべてユーザ指定のアクセス VLAN に移動されます。

authentication event server dead action reinitialize vlan *vlan-id* インターフェイス コンフィギュレーション コマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイムアウトとなり、スイッチは次の認証試行の間にクリティカルポートをクリティカル認証ステートとします。

RADIUS サーバが改めて利用可能であれば、クリティカルポートを設定してホストを再初期化し、ホストをクリティカル VLAN の外へ移動できます。これが設定される場合、クリティカル認証ステートのすべてのクリティカルポートは、自動的に再認証されます。詳細については、このリリースのコマンドリファレンスおよび「[アクセス不能認証バイパス機能の設定](#)」(P.10-53) を参照してください。

相互作用機能

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN : アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 802.1X ポートでイネーブルの場合、この機能は次のように相互に作用します。
 - スwitch が EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。

- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
- すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN : ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1X アカウンティング : RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN : プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異ならなければなりません。
- Remote Switched Port Analyzer (RSPAN) : アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックでは次のとおりです。

- スタック マスターがキープアライブ パケットを送信して RADIUS サーバのステータスを確認します。
RADIUS サーバのステータスが変化すると、スタック マスターはその情報をスタック メンバーに送信します。これにより、スタック メンバーはクリティカル ポートの再認証の際に RADIUS サーバのステータスを確認できます。
- 新しいスタック マスターが選ばれると、スイッチ スタックと RADIUS サーバ間のリンクが変更することがあり、新しいスタック マスターは RADIUS サーバのステータスを更新するために、即座にキープアライブ パケットを送信します。
サーバのステータスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。
- スタックにメンバーが追加されると、スタック マスターはそのメンバーにサーバ ステータスを送信します。

音声 VLAN ポートを使用した 802.1X 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は 802.1X 認証とは独立して動作できます。

シングルホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチホスト モードでは、サブリカントが PVID で認証されたあと、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチホスト モードがイネーブルの場合、サブリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで 802.1X 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットを廃棄します。

802.1X 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。



(注) 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで 802.1X 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、第 16 章「音声 VLAN の設定」を参照してください。

ポート セキュリティを使用した 802.1X 認証

シングルホスト モードまたはマルチホスト モードのどちらでもポート セキュリティを備えた 802.1X ポートを設定できます (`switchport port-security` インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定する必要があります)。ポートでポート セキュリティおよび 802.1X 認証をイネーブルに設定すると、802.1X 認証はそのポートを認証し、ポート セキュリティはそのクライアントを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、802.1X ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

次に、スイッチ上での 802.1X 認証とポート セキュリティ間における相互関係の例を示します。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

クライアントが認証されて、ポート セキュリティが手動で設定された場合、セキュア ホスト テーブル内のエントリは保証されます (ポート セキュリティのスタティック エージングがイネーブルになっていない場合)。

クライアントが認証されてもポート セキュリティ テーブルがいっぱいの場合、セキュリティ違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内でのエントリは他のホストに取って代わられます。

最初に認証されたホストが原因でセキュリティ違反が発生すると、ポートは `errdisable` ステートになり、ただちにシャットダウンします。

セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「[セキュリティ違反](#)」(P.26-10) を参照してください。

- `no switchport port-security mac-address mac-address` インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから 802.1X クライアント アドレスを手動で削除する場合、`dot1x re-authenticate interface interface-id` 特権 EXEC コマンドを使用して、802.1X クライアントを再認証する必要があります。

- 802.1X クライアントがログオフすると、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュア ホスト テーブル内のダイナミック エントリがすべてクリアされます。ここで通常の認証が実行されます。
- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- シングルホスト モードまたはマルチホスト モードのいずれの場合でも、802.1X ポート上でポートセキュリティと音声 VLAN を同時に設定できます。ポートセキュリティは、Voice VLAN Identifier (VVID) および Port VLAN Identifier (PVID) の両方に適用されます。
- 新しいデバイスが 802.1X 対応ポートに接続されている場合、または許可されているデバイスの最大数が認証された場合に、ポートがシャットダウン、Syslog エラーの生成、または新しいデバイスからのパケットの廃棄を実行するように **authentication violation** または **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定できます。詳細については、「[ポートごとに許可できるデバイスの最大数](#)」(P.10-37) およびこのリリースのコマンド リファレンスを参照してください。

スイッチ上でポートセキュリティをイネーブルにする手順については、「[ポートセキュリティの設定](#)」(P.26-9) を参照してください。

Wake-on-LAN (WoL) 機能を使用した 802.1X 認証

802.1X 認証の Wake-on-LAN (WoL) 機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1X ポートを通じて接続され、ホストの電源がオフになると、802.1X ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1X 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1X ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。



(注) PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in または **dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパンニング ツリー フォワーディング ステートに変わります。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。

authentication control-direction both または **dot1x control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した 802.1X 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス (図 10-2 (P.10-4) を参照) に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 802.1X ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス/要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクの存続時間中にインターフェイスで EAPOL パケットが検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応サブリカントであると判断し、インターフェイスを許可するために (MAC 認証バイパスではなく) 802.1X 認証を使用します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1X サブリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS アトリビュート値が DEFAULT であるために前のセッションが終了した場合、スイッチは優先再認証プロセスとして 802.1X 認証を使用します。

MAC 認証バイパスを使用して許可されたクライアントを再認証できます。再認証プロセスは、802.1X を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS アトリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリビュート [29]) に基づいており、Termination-Action RADIUS アトリビュート (アトリビュート [29]) のアクションが *Initialize* (初期化) される場合 (アトリビュート値が *DEFAULT*)、MAC 認証バイパスセッションが終了して、再認証中に接続が切断されます。MAC 認証バイパス機能が 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。AV ペアの詳細については、RFC 3580 『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1X 認証 : 802.1X 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN : クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN : 802.1X ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ : 「ポート セキュリティを使用した 802.1X 認証」(P.10-25) を参照してください。
- 音声 VLAN : 「音声 VLAN ポートを使用した 802.1X 認証」(P.10-24) を参照してください。
- VLAN Membership Policy Server (VMPS) : 802.1X および VMPS は相互に排他的です。
- プライベート VLAN : クライアントをプライベート VLAN に割り当てられます。
- Network Admission Control (NAC; ネットワーク アドミッション コントロール) レイヤ 2 IP 検証 : この機能は、802.1X ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。

設定の詳細については、「認証マネージャ」(P.10-7) を参照してください。

802.1X ユーザ分散

802.1X ユーザ分散を設定して、同一のグループ名を持つユーザを複数の異なる VLAN 間でロード バランスできます。

VLAN は、RADIUS サーバによって提供されるか、または、VLAN グループ名に属するスイッチ CLI によって設定されます。

- ユーザ用の 2 つ以上の VLAN 名を送信するように RADIUS サーバを設定します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1X ユーザ分散は、特定の VLAN のすべてのユーザを追跡し、認証されたユーザを最もユーザ数の少ない VLAN に移動することで、ロード バランシングを達成します。
- ユーザ用の 1 つの VLAN グループ名を送信するように RADIUS サーバを設定します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用することで設定した VLAN グループ名から、選択された VLAN グループ名を検索できます。VLAN グループ名が見つかった場合、最もユーザ数の少ない VLAN を探すために、この VLAN グループ名に属する、対応する VLAN が検索されます。対応する認証されたユーザを該当する VLAN に移動することで、ロード バランシングが達成されます。



(注) RADIUS サーバは、VLAN ID、VLAN 名、VLAN グループの任意の組み合わせで、VLAN 情報を送信します。

802.1X ユーザ分散設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。
- 2 つ以上の VLAN を VLAN グループにマップできます。
- VLAN を追加または削除することで VLAN グループを変更できます。
- 既存の VLAN を VLAN グループからクリアした場合、VLAN 内の認証されたポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブな VLAN が VLAN グループにマッピングされているときでも、VLAN グループをクリアできます。VLAN グループをクリアした場合、グループ内の VLAN の認証状態であるポートまたはユーザはクリアされませんが、VLAN グループへのマッピングはクリアされます。

詳細については、「[802.1X ユーザ分散の設定](#)」(P.10-57) を参照してください。

NAC レイヤ 2 802.1X 検証

スイッチは NAC レイヤ 2 802.1X 検証をサポートします。これは、デバイス ネットワーク アクセスを許可する前に、エンドポイント システムやクライアントのウイルス対策の状態やポスチャをチェックします。NAC レイヤ 2 802.1X 検証を使用すると、次の作業を実行できます。

- Session-Timeout RADIUS アトリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリビュート [29]) を認証サーバからダウンロードします。
- Session-Timeout RADIUS アトリビュート (アトリビュート [27]) の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS アトリビュート (アトリビュート [29]) を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。

- VLAN 番号または名前、または VLAN グループ名のリストを Tunnel Group Private ID (アトリビュート [81]) の値として設定し、VLAN 番号または名前、または VLAN グループ名のプレフィックスを Tunnel Preference (アトリビュート [83]) の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID (アトリビュート [81]) アトリビュートがリストから選択されます。
- **show authentication** または **show dot1x** 特権 EXEC コマンドを使用して、クライアントのポストチャを表示する NAC ポストチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1X 検証の設定は、RADIUS サーバにポストチャ トークンを設定する必要があることを除いて、802.1X ポートベース認証と似ています。NAC レイヤ 2 802.1X 検証の設定に関する詳細については、「[NAC レイヤ 2 802.1X 検証の設定](#)」(P.10-58) および「[定期的な再認証の設定](#)」(P.10-44) を参照してください。

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

設定の詳細については、「[認証マネージャ](#)」(P.10-7) を参照してください。

柔軟な認証の順序

ポートが新しいホストを認証するために使用する方式の順序を設定する場合に、柔軟な認証の順序を使用できます。MAC 認証バイパスおよび 802.1X はプライマリまたはセカンダリの認証方式にすることができ、Web 認証はこれらのどちらかまたは両方の認証が失敗した場合にフォールバック メソッドにすることができます。詳細については、「[認証の順序を柔軟に設定](#)」(P.10-64) を参照してください。

Open1x 認証

Open1x 認証は、デバイスが認証される前にそのデバイスがポートへアクセスすることを許可します。Open 認証が設定されると、ポート上の新しいホストはスイッチにトラフィックだけを送信できます。ホストが認証された後に、RADIUS サーバ上で設定されたポリシーがそのホストに適用されます。

次のシナリオで Open 認証を設定できます。

- Open 認証を使用したシングルホスト モード：認証の前と後で 1 人のユーザのみがネットワークへのアクセスを許可されます。
- Open 認証を使用した MDA モード：音声ドメイン内の 1 人のユーザのみ、およびデータ ドメイン内で 1 人のユーザのみが許可されます。
- Open 認証を使用したマルチホスト モード：任意のホストがネットワークにアクセスできます。
- Open 認証を使用したマルチ認証モード：MDA と同様に、複数のホスト以外を認証できます。

詳細については、「[ホスト モードの設定](#)」(P.10-43) を参照してください。

音声認識 802.1X セキュリティの使用

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN に関わらず、セキュリティ違反が発生した VLAN のみをスイッチの設定でディセーブルにできます。以前のリリースでは、セキュリティ違反を犯したデータ クライアントを認証しようとする、ポート全体がシャットダウンし、その結果、接続が完全に切られました。

この機能は、PC が IP Phone に接続されている環境で使用できます。データ VLAN でセキュリティ違反が検出されると、そのデータ VLAN のみがシャットダウンされます。音声 VLAN のトラフィックは中断せずに続行します。

音声認識 802.1X セキュリティの設定については、「[音声認識 802.1X セキュリティの設定](#)」(P.10-38)を参照してください。

Network Edge Access Topology (NEAT) を使用した 802.1X サプリカント スイッチおよびオーセンティケータ スイッチ

Network Edge Access Topology (NEAT) 機能は、(会議室などの) ワイヤリング クローゼットの外側の領域に ID を拡張します。これによって、任意の種類のデバイスがポート上で認証できます。

- 802.1X スイッチ サプリカント : 802.1X サプリカント機能を使用することによって、別のスイッチに対するサプリカントとして動作するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼットの外側にあり、トランク ポートを通してアップストリームスイッチに接続されるシナリオで役立ちます。802.1X スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチを使用して認証します。

サプリカント スイッチがポートを正常に認証した後、モードがアクセスからトランクに変更されます。

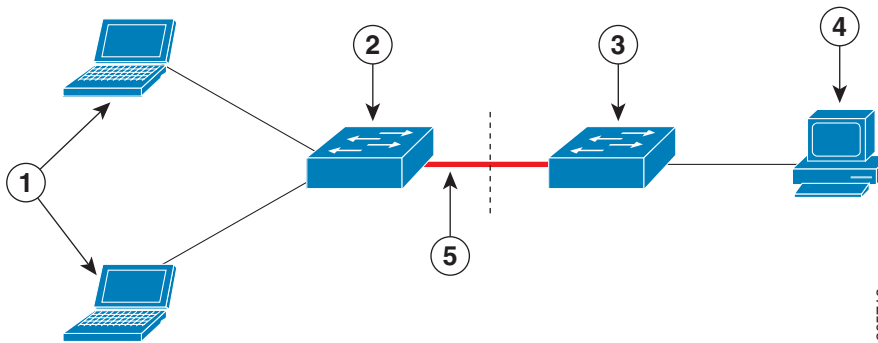
- オーセンティケータ スイッチにアクセス VLAN が設定された場合、認証の正常終了後にトランクポートのネイティブ VLAN になります。

もう 1 つのサプリカント スイッチに接続しているオーセンティケータ スイッチのインターフェイス上で MDA またはマルチ認証モードをイネーブルにできます。マルチホスト モードは、オーセンティケータ スイッチのインターフェイスではサポートされません。

サプリカント スイッチで **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを使用して、Network Edge Access Topology (NEAT) をすべてのホストモードで動作させます。

- ホスト許可 : 確実にネットワーク上で (サプリカントを使用してスイッチに接続している) 許可済みのホストからのトラフィックだけが許可されるようにします。スイッチは、Client Information Signalling Protocol (CISP) を使用して、[図 10-6](#) に示すように、サプリカント スイッチにつながる MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル : オーセンティケータ スイッチ上のトランク設定を自動的にイネーブルにし、サプリカント スイッチからの複数の VLAN のユーザ トラフィックを許可します。ACS で `cisco-av-pair` を `device-traffic-class=switch` として設定します (これは `group` または `user` 設定によって設定できます)。

図 10-6 CISP を使用したオーセンティケータおよびサブリカントスイッチ



1	ワークステーション (クライアント)	2	サブリカントスイッチ (ワイヤリングローゼットの外側)
3	オーセンティケータ スイッチ	4	Access Control Server (ACS)
5	トランク ポート		

注意事項

- 他の認証ポートと同一の設定を使用して NEAT ポートを設定できます。サブリカントスイッチが認証する場合、スイッチのベンダー固有のアトリビュート (VSA) に基づいてモードがアクセスからトランクに変更されます (`device-traffic-class=switch`)。
- ネイティブ トランク VLAN に変換される場合は、VSA は、オーセンティケータ スイッチ ポートモードをアクセスからトランクに変更し、802.1X トランク カプセル化およびアクセス VLAN をイネーブルにします。VSA はサブリカントのポート設定を変更しません。
- ホストモードを変更し、かつ、標準ポート設定をオーセンティケータ スイッチ ポートに適用するには、スイッチ VSA の代わりに Auto Smartport ユーザ定義マクロも使用できます。これによって、オーセンティケータ スイッチ ポート上のサポートされない設定を削除でき、ポートモードをアクセスからトランクに変更できます。詳細については、第 13 章「Auto Smartport マクロの設定」を参照してください。

詳細については、「NEAT を使用したオーセンティケータおよびサブリカントスイッチの設定」(P.10-59) を参照してください。

ACL および RADIUS Filter-Id アトリビュートによる IEEE 802.1X 認証の使用

スイッチは、入力ポートに適用される IP 標準および IP 拡張ポート アクセス コントロール リスト (ACL) をサポートします。

- 管理者が設定した ACL
- Access Control Server (ACS) から入手した ACL

シングル ホスト モードの IEEE 802.1X ポートは、ACS から入手した ACL を使用して、異なるレベルのサービスを IEEE 802.1X 認証済みユーザに提供します。RADIUS サーバは、この種類のユーザとポートを認証し、ユーザ ID に基づいて ACL アトリビュートをスイッチに送信します。スイッチは、

ユーザセッションの期間中、そのアトリビュートをポートに適用します。セッションが終了する、認証が失敗する、または、リンクが失敗すると、ポートは無許可になり、スイッチはポートから ACL を削除します。

ACS から取得した IP 標準 ACL および IP 拡張ポート ACL だけが、Filter-Id アトリビュートをサポートします。Filter-Id アトリビュートは、ACL の名前または番号を指定します。また、Filter-Id アトリビュートは、方向（インバウンドまたはアウトバウンド）およびユーザまたはユーザが所属するグループを指定します。

- ユーザの Filter-Id アトリビュートは、グループの Filter-Id アトリビュートよりも優先されます。
- ACS から入手した Filter-Id アトリビュートが、設定済みの ACL を指定する場合、ユーザ設定の ACL よりも優先されます。
- RADIUS サーバが 2 つ以上の Filter-Id アトリビュートを送信した場合、最後のアトリビュートが適用されます。

Filter-Id アトリビュートがスイッチで定義されていない場合、認証は失敗し、ポートは無許可ステートに戻ります。

共通セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。この ID は、show コマンドや management information base (MIB; 管理情報ベース) など、すべてのレポーティング用途に使用されます。セッション ID はセッション単位の syslog message のすべてと共に表示されます。

セッション ID には次が含まれています。

- Network Access Device (NAD) の IP アドレス
- 単調増加する、一意の 32 ビット整数
- セッション開始タイム スタンプ (32 ビット整数)

次に、show authentication コマンドの出力にセッション ID が表示される例を示します。次の例のセッション ID は 160000050000000B288508E5 です。

```
Switch# show authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Fa4/0/4	0000.0000.0203	mab	DATA	Authz Success	160000050000000B288508E5

次に、syslog 出力にセッション ID が表示される例を示します。次の例のセッション ID も 160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は NAD、AAA サーバ、およびその他のレポート分析アプリケーションによってクライアントの特定に使用されます。ID は自動的に表示されます。設定は必要ありません。

802.1X 認証の設定

ここでは、次の設定情報について説明します。

- 「802.1X 認証のデフォルト設定」 (P.10-34)
- 「802.1X 認証設定時の注意事項」 (P.10-35)
- 「802.1X 準備チェックの設定」 (P.10-37) (任意)
- 「音声認識 802.1X セキュリティの設定」 (P.10-38) (任意)
- 「802.1X 違反モードの設定」 (P.10-39) (任意)
- 「スイッチおよび RADIUS サーバ間の通信の設定」 (P.10-42) (必須)
- 「ホスト モードの設定」 (P.10-43) (任意)
- 「定期的な再認証の設定」 (P.10-44) (任意)
- 「ポートに接続するクライアントの手動での再認証」 (P.10-45) (任意)
- 「待機時間の変更」 (P.10-46) (任意)
- 「スイッチからクライアントへの再送信時間の変更」 (P.10-46) (任意)
- 「スイッチからクライアントへのフレーム再送信回数設定」 (P.10-47) (任意)
- 「再認証回数設定」 (P.10-48) (任意)
- 「802.1X アカウンティングの設定」 (P.10-49) (任意)
- 「MAC 移動のイネーブル化」 (P.10-49) (任意)
- 「ゲスト VLAN の設定」 (P.10-50) (任意)
- 「制限付き VLAN の設定」 (P.10-51) (任意)
- 「アクセス不能認証バイパス機能の設定」 (P.10-53) (任意)
- 「WoL を使用した 802.1X 認証の設定」 (P.10-55) (任意)
- 「MAC 認証バイパスの設定」 (P.10-56) (任意)
- 「NAC レイヤ 2 802.1X 検証の設定」 (P.10-58) (任意)
- 「NEAT を使用したオーセンティケータおよびサブリカント スwitch の設定」 (P.10-59)
- 「ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定」 (P.10-61)
- 「認証の順序を柔軟に設定」 (P.10-64)
- 「ポート上での 802.1X 認証のディセーブル化」 (P.10-65) (任意)
- 「802.1X 認証設定のデフォルト値へのリセット」 (P.10-66) (任意)

802.1X 認証のデフォルト設定

表 10-4 に、802.1X 認証のデフォルト設定を示します。

表 10-4 802.1X 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1X イネーブル ステート	ディセーブル。
ポート単位の 802.1X イネーブル ステート	ディセーブル (force-authorized)。 ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
Authentication、Authorization、Accounting (AAA)	ディセーブル。
RADIUS サーバ	
<ul style="list-style-type: none"> IP アドレス UDP 認証ポート 鍵 	<ul style="list-style-type: none"> 指定なし。 1812。 指定なし。
ホスト モード	シングルホスト モード。
制御方向	双方向制御。
定期的な再認証	ディセーブル。
再認証の間隔 (秒)	3600 秒。
再認証回数	2 回 (ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数)。
待機時間	60 秒 (スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数)。
再送信時間	30 秒 (スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数)。
最大再送信回数	2 回 (スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数)。
クライアント タイムアウト時間	30 秒 (認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間)。
認証サーバ タイムアウト時間	30 秒 (クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間)。 タイムアウト期間は、 authentication timer server または dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用して変更できます。
無活動タイムアウト	ディセーブル。
ゲスト VLAN	指定なし。
アクセス不能認証バイパス	ディセーブル。
制限付き VLAN	指定なし。
オーセンティケータ (スイッチ) モード	指定なし。
MAC 認証バイパス	ディセーブル。
音声認識セキュリティ	ディセーブル。

802.1X 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1X 認証」 (P.10-35)
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」 (P.10-36)
- 「MAC 認証バイパス」 (P.10-36)
- 「ポートごとに許可できるデバイスの最大数」 (P.10-37)

802.1X 認証

- 802.1X 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1X 対応ポートを（たとえばアクセスからトランクに）変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当てられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

802.1X ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除されたあと、ポートは無許可になります。

- 802.1X プロトコルは、レイヤ 2 スタティック アクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポートタイプではサポートされません。
 - トランク ポート：トランク ポート上で 802.1X 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートをトランクに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
 - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートをダイナミックに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
 - ダイナミック アクセス ポート：ダイナミック アクセス (VLAN Query Protocol (VQP)) ポートで 802.1X 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。
 - EtherChannel ポート：EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにするポートを 802.1X ポートとして設定しないでください。EtherChannel ポートで 802.1X 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1X 認証はイネーブルになりません。
 - Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN; リモート SPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポート上で 802.1X 認証をイネーブルにできます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1X 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは、802.1X 認証をイネーブルにできます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1X 認証をグローバルにイネーブルにする前に、802.1X 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1X 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。
- 802.1X 認証をプライベート VLAN ポートに設定できますが、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた 802.1X 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッド ポート) またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。
- Dynamic Host Configuration Protocol (DHCP) クライアントが接続する 802.1X ポートにゲスト VLAN を設定したあとは、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の 802.1X 認証プロセスを再開するための設定を変更することもできます。802.1X 認証プロセスの設定を減らしてください (**authentication timer inactivity** または **dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンド、および **authentication timer reauthentication** または **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド)。設定を減らす量は、接続している 802.1X クライアント タイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
 - この機能はシングルホスト モードおよびマルチホスト モードの 802.1X ポートでサポートされます。
 - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステータスの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
 - Windows XP クライアントに DHCP が設定されていて、DHCP サーバからの IP アドレスを持つ場合、クリティカル ポート上で EAP 成功メッセージを受信すると、DHCP 設定プロセスが再始動しない場合があります。
 - 802.1X ポート上では、アクセス不能認証バイパス機能および制限付き VLAN を設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステータスをクリティカル認証ステータスに変更し、制限付き VLAN に残ります。
 - 同じスイッチ ポート上にアクセス不能バイパス機能とポート セキュリティを設定できます。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN (ルーテッド ポート) またはトランク ポートではサポートされていません。アクセス ポート上に限りサポートされます。

MAC 認証バイパス

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1X 認証のものと同じです。詳細については、「[802.1X 認証](#)」(P.10-35) を参照してください。
- ポートが MAC アドレスで許可されたあとに、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステータスに影響はありません。
- ポートが無許可状態でクライアント MAC アドレスが認証サーバ データベースにない場合、ポートは無許可状態のままになります。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再認証できます。

- ポートが許可状態である場合、再認証が発生するまでポートの状態は変わりません。
- MAC 認証バイパスに接続されているものの非アクティブのホストのタイムアウト期間を設定することができます。範囲は 1 ～ 65535 秒です。タイムアウト値を設定する前にポートセキュリティをイネーブルにする必要があります。詳細については、「[ポートセキュリティの設定](#)」(P.26-9)を参照してください。

ポートごとに許可できるデバイスの最大数

802.1X 対応ポートで許可できるデバイスの最大数は、次のとおりです。

- シングルホスト モードでは、1 つのデバイスだけがアクセス VLAN で許可されます。ポートも音声 VLAN で設定されていた場合、音声 VLAN で送受信される Cisco IP Phone は無制限です。
- MultiDomain Authentication (MDA) モードでは、1 つのデバイスだけがアクセス VLAN に許可されます。また、1 つの IP Phone が音声 VLAN に許可されます。
- マルチホスト モードでは、1 つの 802.1X サプリカントだけがポートで許可されます。ただし、非 802.1X ホストはアクセス VLAN で無制限に許可されます。また、デバイスも音声 VLAN で無制限に許可されます。

802.1X 準備チェックの設定

802.1X 準備チェックは、すべてのスイッチ ポート上で 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続されたデバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。

802.1X 準備チェックは、802.1X を設定できるすべてのポートに許可されています。**dot1x force-unauthorized** として設定されているポートでは使用できません。

スイッチで準備チェックをイネーブルにするには、次の事項に注意してください。

- 通常、準備チェックは 802.1X がスイッチでイネーブルになる前に使用します。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用している場合、スイッチ スタックのすべてのポートがテストされます。
- 802.1X 対応のポートに **dot1x test eapol-capable** コマンドを設定してリンクをアップした場合、ポートは 802.1X 機能に関して接続クライアントにクエリーを送信します。クライアントが通知パケットに回答した場合、802.1X に対応していることとなります。クライアントがタイムアウト期間内に回答した場合、Syslog メッセージが生成されます。クライアントがクエリーに回答しなかった場合、そのクライアントは 802.1X に対応していません。そのため、Syslog メッセージも生成されません。
- 準備チェックは、複数のホストを扱うポートにも送信できます (例 : IP Phone に接続した PC)。準備チェックに対してタイムアウト期間内に回答したクライアントごとに Syslog メッセージが生成されます。

スイッチ上で 802.1X 準備チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>dot1x test eapol-capable [interface interface-id]</code>	スイッチ上で 802.1X 準備チェックをイネーブルにします。 (任意) <i>interface-id</i> には、802.1X 準備チェックを行うポートを指定します。 (注) interface キーワードを省略した場合、スイッチ上のすべてのインターフェイスがテストされます。
ステップ 1	<code>configure terminal</code>	(任意) グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot1x test timeout timeout</code>	(任意) EAPOL 応答を待機するタイムアウト時間を設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルト値は 10 秒です。
ステップ 3	<code>end</code>	(任意) 特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	(任意) 変更したタイムアウト値を確認します。

次に、ポートにクエリーを実行するスイッチ上で準備チェックをイネーブルにする方法を示します。また、クエリーを送信したポートから受信した応答も示します。これにより、接続したデバイスが 802.1X に対応しているかどうか確認できます。

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

音声認識 802.1X セキュリティの設定

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN に関わらず、セキュリティ違反が発生した VLAN だけをスイッチでディセーブルにできます。この機能は、PC が IP Phone に接続されている IP Phone 環境に役立ちます。データ VLAN でセキュリティ違反が検出されてもシャットダウン対象はそのデータ VLAN だけです。音声 VLAN のトラフィックは中断せずにスイッチを通過できます。

スイッチに音声認識 802.1X セキュリティを設定する場合、次の注意事項に従ってください。

- 音声認識 802.1X セキュリティは、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力してイネーブルにします。音声認識 802.1X セキュリティをディセーブルにする場合は、このコマンドの **no** バージョンを使用します。このコマンドはスイッチで 802.1X を設定したすべてのポートに適用されます。



(注)

shutdown vlan キーワードを指定しない場合、**errdisable** ステートになった際にポート全体がシャットダウンします。

- errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して **errdisabled** 回復を設定した場合、ポートは自動的に再度イネーブルになります。**errdisable** 回復がポートに設定されていない場合、**shutdown** および **no-shutdown** インターフェイス コンフィギュレーション コマンドを使用して、もう一度イネーブルにします。
- clear errdisable interface interface-id vlan [vlan-list]** 特権 EXEC コマンドを使用すれば、VLAN ごとに再度イネーブルにできます。範囲を指定しない場合、ポート上のすべての VLAN がイネーブルになります。

音声認識 802.1X セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>errdisable detect cause security-violation shutdown vlan</code>	セキュリティ違反が発生したすべての VLAN をシャットダウンします。 (注) <code>shutdown vlan</code> キーワードを指定しない場合、ポート全体が <code>errdisable</code> ステートになり、シャットダウンします。
ステップ 3	<code>errdisable recovery cause security-violation</code>	(任意) VLAN ごとの自動エラー回復をイネーブルにします。
ステップ 4	<code>clear errdisable interface interface-id vlan [vlan-list]</code>	(任意) <code>errdisable</code> ステートの個々の VLAN を再度イネーブルにします。 <ul style="list-style-type: none"> <code>interface-id</code> には、再度イネーブルにする各 VLAN ポートを指定します。 (任意) <code>vlan-list</code> には、再度イネーブルにする VLAN のリストを指定します。<code>vlan-list</code> が指定されていない場合、すべての VLAN が再度イネーブルになります。
ステップ 5	<code>shutdown no-shutdown</code>	(任意) <code>errdisable</code> ステートの VLAN を再度イネーブルにし、すべての <code>errdisable</code> 状態を回復します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show errdisable detect</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、セキュリティ違反が発生したすべての VLAN をシャットダウンするようにスイッチを設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート Gigabit Ethernet 4/0/2 で `errdisable` ステートだったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2 vlan
```

設定を確認するには、`show errdisable detect` 特権 EXEC コマンドを入力します。

802.1X 違反モードの設定

802.1X ポートを設定することで、シャットダウン、Syslog エラーの生成、または新規デバイスからのパケットの廃棄を実行できます。実行するための条件は次のとおりです。

- デバイスが 802.1X 対応ポートへ接続されている
- 許可するデバイスの最大数がポートで認証された

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ 3 <code>aaa authentication dot1x {default} method1</code>	802.1X 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用方法になっている方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 method1 には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4 <code>interface interface-id</code>	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5 <code>switchport mode access</code>	ポートをアクセス モードにします。
ステップ 6 <code>authentication violation shutdown restrict protect}</code> または <code>dot1x violation-mode {shutdown restrict protect}</code>	違反モードを設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • shutdown : ポートを <code>errdisable</code> ステートにします。 • restrict : Syslog エラーを生成します。 • protect : そのポートへトラフィックを送信する新規デバイスからのパケットを廃棄します。
ステップ 7 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 8 <code>show authentication</code> または <code>show dot1x</code>	設定を確認します。
ステップ 9 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1X 認証の設定

802.1X ポートベース認証を設定するには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリ送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1X の AAA プロセスを示します。

- ステップ 1 ユーザがスイッチのポートに接続します。
- ステップ 2 認証が実行されます。
- ステップ 3 RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
- ステップ 4 スイッチが開始メッセージをアカウントिंग サーバに送信します。
- ステップ 5 必要に応じて、再認証が実行されます。
- ステップ 6 スイッチが仮のアカウントング アップデートを、再認証結果に基づいたアカウントング サーバに送信します。
- ステップ 7 ユーザがポートから切断します。

ステップ 8 スイッチが停止メッセージをアカウントिंग サーバに送信します。

802.1X ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 aaa new-model	AAA をイネーブルにします。
ステップ 3 aaa authentication dot1x {default} method1	802.1X 認証方式リストを作成します。 authentication コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用するになっている方法に続いて default キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 <i>method1</i> には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) group radius キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4 dot1x system-auth-control	スイッチ上で 802.1X 認証をグローバルにイネーブルにします。
ステップ 5 aaa authorization network {default} group radius	(任意) ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定がデフォルトです。
ステップ 6 radius-server host ip-address	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7 radius-server key string	(任意) RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
ステップ 8 interface interface-id	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9 switchport mode access	(任意) ステップ 6 および 7 で RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 10 authentication port-control auto または dot1x port-control auto	ポート上で 802.1X 認証をイネーブルにします。 機能の相互作用については、「 802.1X 認証設定時の注意事項 」(P.10-35)を参照してください。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show authentication または show dot1x	設定を確認します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host { <i>hostname</i> <i>ip-address</i> } auth-port <i>port-number</i> key <i>string</i>	<p>RADIUS サーバ パラメータを設定します。</p> <p><i>hostname</i> <i>ip-address</i> には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。</p> <p>auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。デフォルト値は 1812 です。指定できる範囲は 0 ~ 65536 です。</p> <p>key <i>string</i> には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵はテキスト ストリングで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。</p> <p>(注) 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず radius-server host コマンド構文の最後の項目として設定してください。鍵でスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用される暗号鍵と一致する必要があります。</p> <p>複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバをクリアするには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号鍵を RADIUS サーバ上の鍵と同じ *rad123* に設定する例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」(P.9-36) を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー スtring があります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

802.1X 認証済みポート上でシングル ホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。**multi-domain** キーワードを使用して MDA を設定して、ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を、同一スイッチ ポートで認証することができます。

この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 radius-server vsa send authentication	VSA（Vendor-Specific Attribute; ベンダー固有属性）を認識し使用するために、ネットワーク アクセス サーバを設定します。
ステップ 3 interface interface-id	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 authentication host-mode [multi-auth multi-domain multi-host single-host] または dot1x host-mode {single-host multi-host multi-domain}	<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> multi-auth : 音声 VLAN 上では 1 つのクライアントを、データ VLAN 上では複数の認証されたクライアントを許可します。各ホストは別々に認証されます。 <p>(注) multi-auth のキーワードを使用できるのは、authentication host-mode コマンドの場合だけです。</p> <ul style="list-style-type: none"> multi-host : シングル ホストの認証後に 802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 multidomain : ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を 1 つの 802.1X 認証済みポートで認証することができます。 <p>(注) ホスト モードが multi-domain に設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 16 章「音声 VLAN の設定」を参照してください。</p> <ul style="list-style-type: none"> single-host : 802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 <p>指定するインターフェイスで、authentication port-control または dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。</p>
ステップ 5 switchport voice vlan vlan-id	(任意) 音声 VLAN を設定します。
ステップ 6 end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<code>show authentication interface interface-id</code> または <code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上で複数のホストをディセーブルにするには、**no authentication host-mode** または **no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1X 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにしてポート上でホストと音声デバイスを許可する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

定期的な再認証の設定

802.1X クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔 (秒) を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>authentication periodic</code> または <code>dot1x reauthentication</code>	クライアントの定期的な再認証 (デフォルトではディセーブル) をイネーブルにします。

コマンド	目的
ステップ 4 authentication timer {[[inactivity reauthenticate] [server am]} { restart value }} または dot1x timeout reauth-period { seconds server }	再認証の間隔 (秒) を指定します。 authentication timer のキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • inactivity : クライアントからアクティビティがない場合、そのクライアントが無許可になるまでの間隔 (秒) • reauthenticate : 自動再認証の試行が開始されるまでの時間 (秒) • server am : 無許可ポートを認証する試行が実行されるまでの間隔 (秒) • restart value : 無許可ポートを認証する試行が実行されるまでの間隔 (秒) dot1x timeout reauth-period のキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • seconds : 秒数を 1 ~ 65535 の範囲で設定します。デフォルトは 3600 秒です。 • server : Session-Timeout RADIUS アトリビュート (アトリビュート [27]) および Terminate-Action RADIUS アトリビュート (アトリビュート [29]) の値に基づいて秒数を指定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show authentication interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

定期的な再認証をディセーブルにするには、**no authentication periodic** または **no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。再認証の間隔をデフォルトの秒数に戻すには、**no authentication timer** または **no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface interface-id 特権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「[定期的な再認証の設定](#)」(P.10-44) を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet2/0/1
```

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、そのあと再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。クライアントが無効なパスワードを提示した場合、クライアントの認証に失敗する場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	dot1x timeout quiet-period seconds	スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

待機時間をデフォルトに戻すには、**no dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、そのあとフレームを再送信します。



(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を α 更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	dot1x timeout tx-period seconds	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 5 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信時間をデフォルトに戻すには、**no dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

スイッチからクライアントへのフレーム再送信回数の設定

(クライアントから応答が得られなかった場合に) スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。



(注) このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	dot1x max-reauth-req count	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は 1 ~ 10 です。デフォルトは 2 です。
ステップ 4	end	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 5 show authentication interface <i>interface-id</i> または show dot1x interface <i>interface-id</i>	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数をデフォルトに戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 5 に設定する例を示します。

```
Switch(config-if)# dot1x max-req 5
```

再認証回数の設定

ポートが無許可ステートになる前に、スイッチが認証プロセスを再開する回数を変更することもできます。



(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 dot1x max-reauth-req <i>count</i>	ポートが無許可ステートになる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォルトは 2 です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show authentication interface <i>interface-id</i> または show dot1x interface <i>interface-id</i>	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再認証回数をデフォルトに戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが無許可ステートになる前に、スイッチが認証プロセスを再開する回数として 4 を設定する例を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

MAC 移動のイネーブル化

MAC 移動はスイッチ上のあるポートから別のポートへの認証されたホストの移動を許可します。スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
<code>authentication mac-move permit</code>	イネーブル
<code>end</code>	特権 EXEC モードに戻ります。
<code>show run</code>	設定を確認します。
<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチで MAC 移動をグローバルにイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

802.1X アカウンティングの設定

802.1X アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1X セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```



(注)

ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになったあと、802.1X アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

	コマンド	目的
ステップ 3	<code>aaa accounting dot1x default start-stop group radius</code>	すべての RADIUS サーバのリストを使用して、802.1X アカウンティングをイネーブルにします。
ステップ 4	<code>aaa accounting system default start-stop group radius</code>	(任意) システム アカウンティングをイネーブルにし (すべての RADIUS サーバのリストを使用)、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** 特権 EXEC コマンドを使用します。

次に、802.1X アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1X 対応でないクライアントはゲスト VLAN に配置されます。802.1X 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングルホストモードまたはマルチホストモードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1X 認証設定時の注意事項 」(P.10-35) を参照してください。
ステップ 3	<code>switchport mode access</code> または <code>switchport mode private-vlan host</code>	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホストポートとして設定します。
ステップ 4	<code>authentication port-control auto</code> または <code>dot1x port-control auto</code>	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5	<code>dot1x guest-vlan vlan-id</code>	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 7 <code>show authentication interface-id</code> または <code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ゲスト VLAN をディセーブルにして削除するには、`no dot1x guest-vlan` インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間 (秒) を 15 に設定し、802.1X ポートの DHCP クライアント接続時に、VLAN 2 を 802.1X ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定すると、認証サーバが有効なユーザ名またはパスワードを受信できない場合、802.1X に準拠したクライアントは制限付き VLAN に移されません。スイッチは、シングルホスト モードに限り制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1X 認証設定時の注意事項 」(P.10-35) を参照してください。
ステップ 3 <code>switchport mode access</code> または <code>switchport mode private-vlan host</code>	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4 <code>authentication port-control auto</code> または <code>dot1x port-control auto</code>	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5 <code>authentication event fail action authorize vlan-id</code>	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッド ポート)、RSPAN VLAN、プライマリプライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 7 show authentication interface-id または show dot1x interface interface-id	(任意) 設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

制限付き VLAN をディセーブルにして削除するには、**no dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を 802.1X 制限付き VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# dot1x auth-fail vlan 2
```

ユーザに制限付き VLAN を割り当てる前に、**dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ~ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」(P.10-35) を参照してください。
ステップ 3 switchport mode access または switchport mode private-vlan host	ポートをアクセス モードにします。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4 authentication port-control auto または dot1x port-control auto	ポート上で 802.1X 認証をイネーブルにします。
ステップ 5 dot1x auth-fail vlan vlan-id	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッド ポート)、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1X 制限付き VLAN として設定できます。
ステップ 6 dot1x auth-fail max-attempts max attempts	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ~ 3 です。デフォルトは 3 です。
ステップ 7 end	特権 EXEC モードに戻ります。
ステップ 8 show authentication interface-id または show dot1x interface interface-id	(任意) 設定を確認します。
ステップ 9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定数をデフォルトに戻すには、**no dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートを制限付き VLAN にするために、認証試行回数を 2 に設定する方法を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）を設定できます。

ポートをクリティカルポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server dead-criteria time time tries tries</code>	(任意) RADIUS サーバが使用できない、または <i>dead</i> と見なされることを判別するのに使われる条件を設定します。 指定できる <i>time</i> の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの <i>seconds</i> 値を 10 ～ 60 秒の間で動的に決定します。 指定できる <i>tries</i> の範囲は 1 ～ 100 です。スイッチは、デフォルトの <i>tries</i> パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 3	<code>radius-server deadtime minutes</code>	(任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分 (24 時間) です。デフォルト値は 0 分です。

コマンド	目的
ステップ 4 radius-server host <i>ip-address</i> [acct-port <i>udp-port</i>] [auth-port <i>udp-port</i>] [test username <i>name</i> [idle-time <i>time</i>] [ignore-acct-port [ignore-auth-port]] [key string]	<p>(任意) 次のキーワードを使用して RADIUS サーバパラメータを設定します。</p> <ul style="list-style-type: none"> • acct-port <i>udp-port</i> : RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ~ 65536 です。デフォルト値は 1646 です。 • auth-port <i>udp-port</i> : RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ~ 65536 です。デフォルト値は 1645 です。 <p>(注) RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。</p> <ul style="list-style-type: none"> • test username <i>name</i> : RADIUS サーバステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。 • idle-time <i>time</i> : スイッチがテストパケットをサーバに送信したあとの間隔を分数で設定します。指定できる範囲は 1 ~ 35791 分です。デフォルトは 60 分 (1 時間) です。 • ignore-acct-port : RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • ignore-auth-port : RADIUS サーバ認証ポートのテストをディセーブルにします。 • key string : スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号鍵を指定します。 <p>(注) 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず radius-server host コマンド構文の最後の項目として設定してください。鍵でスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないとください。鍵は RADIUS デーモンで使用する暗号鍵と一致している必要があります。</p> <p>radius-server key {<i>0 string</i> <i>7 string</i> <i>string</i>} グローバル コンフィギュレーション コマンドを使用しても認証および暗号鍵を設定できます。</p>
ステップ 5 dot1x critical { <i>eapol</i> <i>recovery</i> delay <i>milliseconds</i> }	<p>(任意) アクセス不能認証バイパスのパラメータを設定します。</p> <p>eapol : スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。</p> <p>recovery delay <i>milliseconds</i> : 使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ~ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です (ポートは毎秒再初期化できます)。</p>
ステップ 6 interface <i>interface-id</i>	<p>設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」(P.10-35) を参照してください。</p>
ステップ 7 authentication event server dead action [<i>authorize</i> <i>reinitialize</i>] vlan <i>vlan-id</i>	<p>RADIUS サーバが到達不能である場合、これらのキーワードを使用してポート上のホストを移動します。</p> <ul style="list-style-type: none"> • authorize : 認証を試みる新しいホストをユーザ指定のクリティカル VLAN に移動します。 • reinitialize : ポートのすべての認証済みホストをユーザ指定のクリティカル VLAN に移動します。

コマンド	目的
ステップ 8 dot1x critical [recovery action reinitialize vlan vlan-id]	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。 <ul style="list-style-type: none"> recovery action reinitialize : 回復機能をイネーブルにして、認証サーバが使用可能なとき、回復動作中にポートを認証するように指定します。 vlan vlan-id : スイッチがクリティカル ポートに割り当てるアクセス VLAN を指定します。指定できる範囲は 1 ~ 4094 です。
ステップ 9 end	特権 EXEC モードに戻ります。
ステップ 10 show authentication interface interface-id または show dot1x interface interface-id	(任意) 設定を確認します。
ステップ 11 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical {eapol | recovery delay}** グローバル コンフィギュレーション コマンドを使用します。アクセス不能認証バイパスをディセーブルにするには、**no dot1x critical** インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet1/0/2
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1X 認証の設定

WoL を使用した 802.1X 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、「 802.1X 認証設定時の注意事項 」(P.10-35) を参照してください。

コマンド	目的
ステップ 3 authentication control-direction {both in} または dot1x control-direction {both in}	ポートで WoL を使用して 802.1X 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 <ul style="list-style-type: none"> • both : ポートを双方向に設定します。ポートは、ホストとの間でパケットを送受信できません。デフォルトでは、ポートは双方向です。 • in : ポートを単方向に設定します。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show authentication interface interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

WoL を使用して 802.1X 認証をディセーブルにするには、**no authentication control-direction** または **no dot1x control-direction** インターフェイス コンフィギュレーション コマンドを使用します。

次に、WoL を使用した 802.1X 認証をイネーブルにして、ポートを双方向に設定する例を示します。

```
Switch(config-if)# authentication control-direction both
```

または

```
Switch(config-if)# dot1x control-direction both
```

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされるポートのタイプについては、 「802.1X 認証設定時の注意事項」(P.10-35) を参照してください。
ステップ 3 authentication port-control auto または dot1x port-control auto	ポート上で 802.1X 認証をイネーブルにします。

コマンド	目的
ステップ 4 dot1x mac-auth-bypass [eap timeout activity {value}]	MAC 認証バイパスをイネーブルにします。 (任意) eap キーワードを使用して認証用の EAP を使用するようにスイッチを設定します。 (任意) timeout activity キーワードを使用して、未認証ステートに移行する前に接続されているホストを非アクティブにすることができる秒数を設定します。指定できる範囲は 1 ~ 65535 です。 タイムアウト値を設定する前にポートセキュリティをイネーブルにする必要があります。詳細については、「 ポートセキュリティの設定 」(P.26-9) を参照してください。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show authentication interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MAC 認証バイパスをディセーブルにするには、**no dot1x mac-auth-bypass** インターフェイス コンフィギュレーション コマンドを使用します。

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Switch(config-if)# dot1x mac-auth-bypass
```

802.1X ユーザ分散の設定

VLAN グループを設定し、VLAN を VLAN グループにマッピングするには特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 vlan group vlan-group-name vlan-list vlan-list	VLAN グループを設定し、単一の VLAN または VLAN 範囲を VLAN グループにマッピングします。
ステップ 2 show vlan group all vlan-group-name	設定を確認します。
ステップ 3 no vlan group vlan-group-name vlan-list vlan-list	VLAN グループ設定、または VLAN グループ設定の要素をクリアします。

次の例では、VLAN グループを設定し、VLAN をグループにマッピングし、VLAN グループ設定および指定された VLAN へのマッピングを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 10
```

```
switch(config)# show vlan group group-name eng-dept
Group Name          Vlans Mapped
-----
eng-dept            10
switch# show dot1x vlan-group all
Group Name          Vlans Mapped
-----
eng-dept            10
hr-dept             20
```

次の例では、VLAN を既存のグループに追加し、VLAN が追加されたことを確認する方法を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                Vlans Mapped
-----
eng-dept                  10,30
```

次の例では、VLAN グループから VLAN を削除する方法を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループから削除され、VLAN グループがクリアされる例を示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
```

```
switch(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

NAC レイヤ 2 802.1X 検証の設定

NAC レイヤ 2 802.1X 検証を設定できます。これは、RADIUS サーバを使用した 802.1X 認証とも呼ばれます。

NAC レイヤ 2 802.1X 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	dot1x guest-vlan vlan-id	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッド ポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 4	authentication periodic または dot1x reauthentication	クライアントの定期的な再認証 (デフォルトではディセーブル) をイネーブルにします。

コマンド	目的
ステップ 5 dot1x timeout reauth-period {seconds server}	再認証の間隔 (秒) を指定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> seconds : 1 ~ 65535 の秒数を設定します。デフォルトは 3600 秒です。 server : Session-Timeout RADIUS アトリビュート (アトリビュート [27]) および Terminate-Action RADIUS アトリビュート (アトリビュート [29]) の値に基づいて秒数を指定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show authentication interface interface-id または show dot1x interface interface-id	802.1X 認証の設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、NAC レイヤ 2 802.1X 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

NEAT を使用したオーセンティケータおよびサブリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチがサブリカントとして設定され、オーセンティケータ スイッチに接続している必要があります。

概要については、「[Network Edge Access Topology \(NEAT\) を使用した 802.1X サブリカント スイッチおよびオーセンティケータ スイッチ](#)」(P.10-30) を参照してください。



(注) *cisco-av-pairs* は、ACS 上で *device-traffic-class=switch* として設定する必要があります。これにより、インターフェイスは、サブリカントの認証が成功したあとにトランクとして設定されます。

スイッチをオーセンティケータとして設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 cisp enable	CISP をイネーブルにします。
ステップ 3 interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 switchport mode access	ポートをアクセス モードにします。
ステップ 5 authentication port-control auto	port-authentication モードを auto に設定します。

	コマンド	目的
ステップ 6	dot1x pae authenticator	Port Access Entity (PAE; ポート アクセス エンティティ) オーセンティケータとしてインターフェイスを設定します。
ステップ 7	spanning-tree portfast	単一ワークステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show running-config interface interface-id	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、スイッチを 802.1X オーセンティケータとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサブリカントとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cisp enable	CISP をイネーブルにします。
ステップ 3	dot1x credentials profile	Create 802.1X 証明書プロファイルを作成します。これは、サブリカントとして設定されるポートに適用する必要があります。
ステップ 4	username suppswitch	ユーザ名を作成します。
ステップ 5	password password	新しいユーザ名用のパスワードを作成します。
ステップ 6	dot1x supplicant force-multicast	強制的に、スイッチがユニキャスト パケットまたはマルチキャスト パケットのいずれかを受信したときにマルチキャスト EAPOL パケットだけを送信するように設定します。 これによって、NEAT はサブリカント スイッチ上ですべてのホストモードで動作できます。
ステップ 7	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	switchport trunk encapsulation dot1q	ポートをトランク モードにします。
ステップ 9	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	dot1x pae supplicant	Port Access Entity (PAE; ポート アクセス エンティティ) サブリカントとしてインターフェイスを設定します。
ステップ 11	dot1x credentials profile-name	802.1X 証明書プロファイルをインターフェイスに適用します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show running-config interface interface-id	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、スイッチをサブリカントとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Auto Smartport (ASP) による NEAT の設定

スイッチ VSA の代わりに Auto Smartport ユーザ定義マクロを使用してオーセンティケータ スイッチを設定することもできます。詳細については、第 13 章「Auto Smartport マクロの設定」を参照してください。

ダウンロード可能な ACL とリダイレクト URL を使用した 802.1X 認証の設定

スイッチ上で 802.1X 認証を設定するほかに、ACS を設定する必要があります。詳細については、『Cisco Secure ACS configuration guides』を参照してください。



(注)

ACS をスイッチにダウンロードする前に、ダウンロード可能な ACL をスイッチ上で設定する必要があります。

ポート上での認証のあと、**show ip access-list** 特権 EXEC コマンドを使用して、ダウンロードされた ACL をポート上で表示できます。

ダウンロード可能な ACL の設定

クライアント認証が終了して、IP デバイス トラッキング テーブルにクライアント IP アドレスが追加されると、ポリシーが有効になります。そしてスイッチはダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip device tracking	IP デバイス トラッキング テーブルを設定します。
ステップ 3	aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa authorization network default group radius	認証方法を local に設定します。認証方法を削除するには、 no aaa authorization network default group radius コマンドを使用します。
ステップ 5	radius-server vsa send authentication	radius vsa send authentication を設定します。

	コマンド	目的
ステップ 6	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<code>ip access-group acl-id in</code>	ポート上でデフォルトの ACL を入力方向に設定します。 (注) <code>acl-id</code> は、アクセス リスト名または番号です。
ステップ 8	<code>show running-config interface interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダウンロード ポリシーの設定

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number deny source source-wildcard log</code>	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 access-list-number は、1 ~ 99 または 1300 ~ 1999 の 10 進数です。 deny または permit を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 <ul style="list-style-type: none"> ドット付き 10 進表記で 32 ビットの値。 0.0.0.0 255.255.255.255 という source および source-wildcard 値の省略形を表すキーワード any。source-wildcard 値の入力は不要です。 source 0.0.0.0 という source および source-wildcard の省略形を表すキーワード host。 (任意) source-wildcard によって、ワイルドカード ビットが source に適用されます。 (任意) log を指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>ip access-group acl-id in</code>	ポート上でデフォルトの ACL を入力方向に設定します。 (注) <code>acl-id</code> は、アクセス リスト名または番号です。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 7	<code>aaa authorization network default group radius</code>	認証方法を local に設定します。認証方法を削除するには、 no aaa authorization network default group radius コマンドを使用します。
ステップ 8	<code>ip device tracking</code>	IP デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング テーブルをディセーブルにするには、 no ip device tracking グローバル コンフィギュレーション コマンドを使用します。

コマンド	目的
ステップ9 ip device tracking probe count count	(任意) IP デバイス トラッキング テーブルを設定します。 <ul style="list-style-type: none"> count count : スイッチが ARP プロブを送信する回数を設定します。指定できる範囲は 1 ~ 5 です。デフォルト値は 3 です。 interval interval : スイッチが ARP プロブを再送信する前に応答を待機する秒数を設定します。指定できる範囲は 30 ~ 300 秒です。デフォルト値は 30 秒です。
ステップ10 radius-server vsa send authentication	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。 (注) ダウンロード可能な ACL は動作している必要があります。
ステップ11 end	特権 EXEC モードに戻ります。
ステップ12 show ip device tracking all	IP デバイス トラッキング テーブルのエントリについての情報を表示します。
ステップ13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ダウンロード ポリシー用のスイッチ設定の例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベースの MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 mab request format attribute 32 vlan access-vlan	VLAN ID ベースの MAC 認証をイネーブルにします。
ステップ3 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN ID ベースの MAC 認証の状態を確認する show コマンドはありません。 **debug radius accounting** 特権 EXEC コマンドを使用して RADIUS アトリビュート 32 を確認してください。このコマンドの詳細については、次の URL で『Cisco IOS Debug Command Reference』 Release 12.2 を参照してください。

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次の例では、スイッチで VLAN ID ベースの MAC 認証をグローバルにイネーブルにする方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

認証の順序を柔軟に設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	authentication order [dot1x mab] {webauth}	(任意) ポートで使用する認証方式の順番を設定します。
ステップ 4	authentication priority [dot1x mab] {webauth}	(任意) port-priority リストに認証方式を追加します。
ステップ 5	show authentication	(任意) 設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ポートが最初に 802.1X 認証を試行し、次にフォールバック メソッドとして Web 認証を試行する設定方法の例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config)# authentication order dot1x webauth
```

Open1x の設定

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	authentication control-direction {both in}	(任意) ポート コントロールを単方向または双方向に設定します。
ステップ 4	authentication fallback name	(任意) 802.1X 認証をサポートしていないクライアント用に、ポートが Web 認証をフォールバック メソッドとして使用するよう設定します。
ステップ 5	authentication host-mode [multi-auth multi-domain multi-host single-host]	(任意) ポート上で認証マネージャ モードを設定します。
ステップ 6	authentication open	(任意) ポート上でオープン アクセスをイネーブルまたはディセーブルにします。

	コマンド	目的
ステップ 7	authentication order [dot1x mab] {webauth}	(任意) ポートで使用する認証方式の順番を設定します。
ステップ 8	authentication periodic	(任意) ポート上で再認証をイネーブ爾またはディセーブルにします。
ステップ 9	authentication port-control {auto force-authorized force-un authorized}	(任意) ポートの許可ステートの手動制御をイネーブ爾にします。
ステップ 10	show authentication	(任意) 設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ポート上で open 1X を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config)# authentication control-direction both
Switch(config)# authentication fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポート上での 802.1X 認証のディセーブル化

802.1X 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1X 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no dot1x pae	ポート上で 802.1X 認証をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1X Port Access Entity (PAE; ポート アクセス エンティティ) オーセンティケーターとしてポートを設定するには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで 802.1X がイネーブ爾になりますが、ポートに接続されたクライアントは許可されません。

次に、802.1X 認証をポートでディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no dot1x pae authenticator
```

802.1X 認証設定のデフォルト値へのリセット

802.1X 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	dot1x default	802.1X パラメータをデフォルト値に戻します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id または show dot1x interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1X の統計情報およびステータスの表示

すべてのポートに関する 802.1X 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。特定のポートに関する 802.1X 統計情報を表示するには、**show dot1x statistics interface interface-id** 特権 EXEC コマンドを使用します。

スイッチに関する 802.1X 管理および動作ステータスを表示するには、**show dot1x all [details | statistics | summary]** 特権 EXEC コマンドを使用します。特定のポートに関する 802.1X 管理および動作ステータスを表示するには、**show dot1x interface interface-id** 特権 EXEC コマンドを使用します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER 11

Web ベース認証の設定

この章では、Web ベース認証を設定する手順について説明します。内容は次のとおりです。

- 「Web ベース認証の概要」(P.11-1)
- 「Web ベース認証の設定」(P.11-9)
- 「Web ベース認証ステータスの表示」(P.11-18)



(注)

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

Web ベース認証の概要

Web ベース認証機能 (*Web 認証* プロキシとも呼ばれます) を使用して、IEEE 802.1X サブリカントを実行していないホスト システムでエンド ユーザを認証します。



(注)

Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上で設定できます。

Web ベース認証では、ユーザが HTTP セッションを開始すると、ホストからの入力 HTTP パケットが代行受信され、ユーザに HTML ログイン ページが送信されます。ユーザが認定証を入力すると、その情報は、認証のために Authentication, Authorization, Accounting (AAA; 認証、認可、アカウントینگ) サーバに送信されます。

認証に成功すると、ログイン成功 HTML ページがホストに送信され、AAA サーバによって返されたアクセス ポリシーが適用されます。

認証に失敗すると、ログイン失敗 HTML ページがユーザに転送され、ユーザはログインを再実行するように求められます。ユーザが試行の最大数を超過すると、ログイン期限切れ HTML ページがホストに転送され、そのユーザは一定の待機時間、ウォッチ リストに配置されます。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

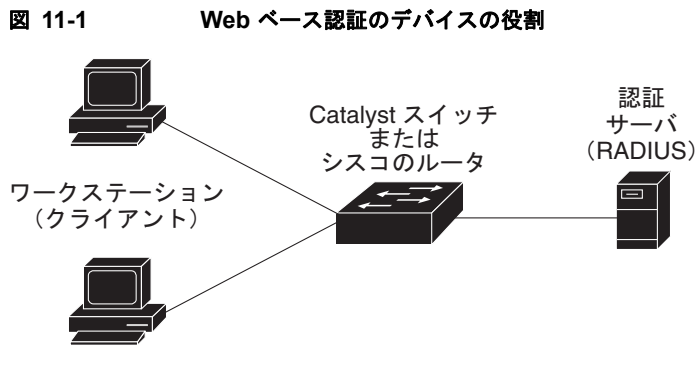
- 「デバイスの役割」(P.11-2)
- 「ホスト検出」(P.11-2)
- 「セッションの作成」(P.11-3)
- 「認証プロセス」(P.11-3)
- 「Web 認証のカスタマイズ可能な Web ページ」(P.11-6)
- 「Web ベース認証とその他の機能の相互作用」(P.11-7)

デバイスの役割

Web ベース認証では、ネットワーク上のデバイスには次のような特定の役割があります。

- **クライアント**：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションは、Java スクリプト対応の HTML ブラウザを実行している必要があります。
- **認証サーバ**：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントに対して LAN およびスイッチ サービスへのアクセスを許可するのか、そのクライアントを拒否するのかをスイッチに通知します。
- **スイッチ**：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの間の仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 11-1 に、ネットワーク上でのこれらのデバイスの役割を示します。



ホスト検出

スイッチは、検出されたホストに関する情報を保存するための IP デバイス トラッキング テーブルを維持しています。



(注)

デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルです。Web ベース認証を使用するには、IP デバイス トラッキング機能をイネーブルにする必要があります。

レイヤ 2 インターフェイスの場合、Web ベース認証では次のメカニズムを使用して IP ホストが検出されます。

- **Address Resolution Protocol (ARP; アドレス解決プロトコル)** ベース トリガー：ARP リダイレクト Access Control List (ACL; アクセス コントロール リスト) により、スタティック IP アドレスまたはダイナミック IP アドレスでホストを検出できます。
- **ダイナミック ARP インスペクション**
- **DHCP スヌーピング**：スイッチがホストの Dynamic Host Configuration Protocol (DHCP) バインディング エントリを作成すると、Web ベース認証が通知されます。

セッションの作成

Web ベース認証で新規ホストが検出されると、次のようにセッションを作成します。

- 例外リストを確認します。
ホスト IP が例外リストに含まれている場合、例外リスト エントリからのポリシーが適用され、セッションが確立されます。
- 認可バイパスを確認します。
ホスト IP が例外リストにない場合、Web ベース認証は Nonresponsive Host (NRH; 非応答ホスト) 要求をサーバに送信します。
サーバ応答が *Access Accepted* である場合、このホストの認可がバイパスされます。セッションは確立されます。
- HTTP 代行受信 ACL を設定します。
NRH 要求に対するサーバ応答が *Access Rejected* である場合、HTTP 代行受信 ACL がアクティブになり、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証がイネーブルの場合、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認可が開始されます。スイッチからユーザにログイン ページが送信されます。ユーザがユーザ名とパスワードを入力すると、スイッチからサーバにエントリが送信されます。
- 認証に成功すると、ユーザのアクセス ポリシーが認証サーバからスイッチにダウンロードされて、アクティブになります。ログイン成功ページがユーザに送信されます。
- 認証に失敗すると、ログイン失敗ページがスイッチから送信されます。ユーザがログインを再試行します。試行の最大数を超過すると、ログイン期限切れページがスイッチから送信され、ホストがウォッチ リストに配置されます。ウォッチ リストのタイムアウト後、ユーザは認証プロセスを再試行できます。
- 認証サーバがスイッチに応答せず、かつ AAA 失敗ポリシーが設定されている場合は、スイッチによって、その失敗アクセス ポリシーがクライアントに適用されます。ログイン成功ページがユーザに送信されます（「ローカル Web 認証バナー」(P.11-4) を参照）。
- ホストがレイヤ 2 インターフェイスの ARP プロープに応答しない場合、またはホストがレイヤ 3 インターフェイスのアイドル タイムアウト内にトラフィックを送信しない場合は、スイッチによってクライアントが再認証されます。
- この機能は、ダウンロードされたタイムアウトまたはローカルに設定されたセッション タイムアウトに適用されます。
- 終了処理が Remote Authentication Dial-In User Service (RADIUS) の場合は、非応答ホスト (NRH) 要求がサーバに送信されます。終了処理は、サーバからの応答に含まれています。
- 終了処理がデフォルトの場合は、セッションが破棄され、適用されたポリシーが削除されます。

ローカル Web 認証バナー

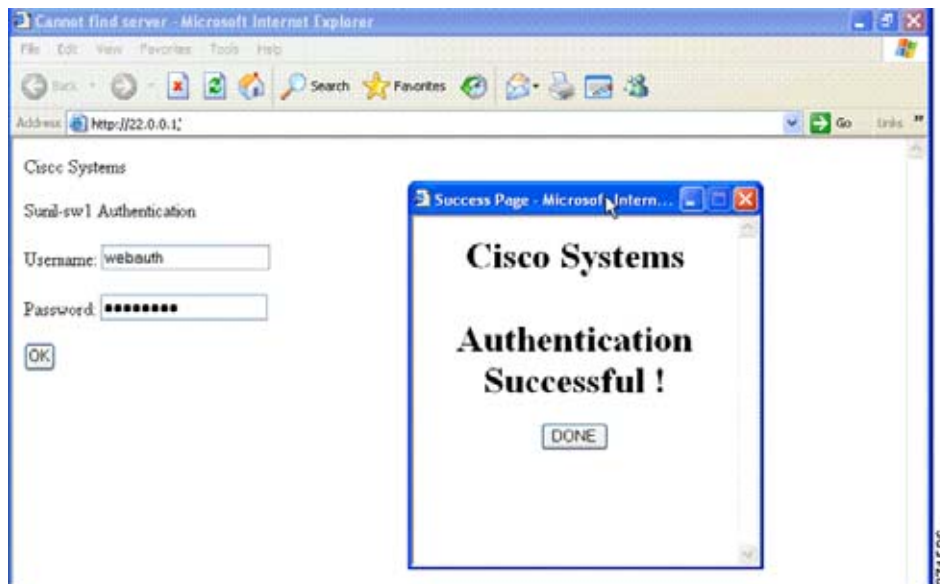
Web 認証を使用すると、スイッチへのログイン時に表示されるバナーを作成できます。

バナーはログイン ページと認証結果のポップアップ ページの両方に表示されます。

- [Authentication Successful]
- [Authentication Failed]
- [Authentication Expired]

バナーは、**ip admission auth-proxy-banner http** グローバル コンフィギュレーション コマンドを使用して作成します。ログイン ページに表示されるデフォルトのバナーは、[Cisco Systems] および [Switch host-name Authentication] です。Cisco Systems のバナーは、[図 11-2](#) のように認証結果のポップアップ ページに表示されます。

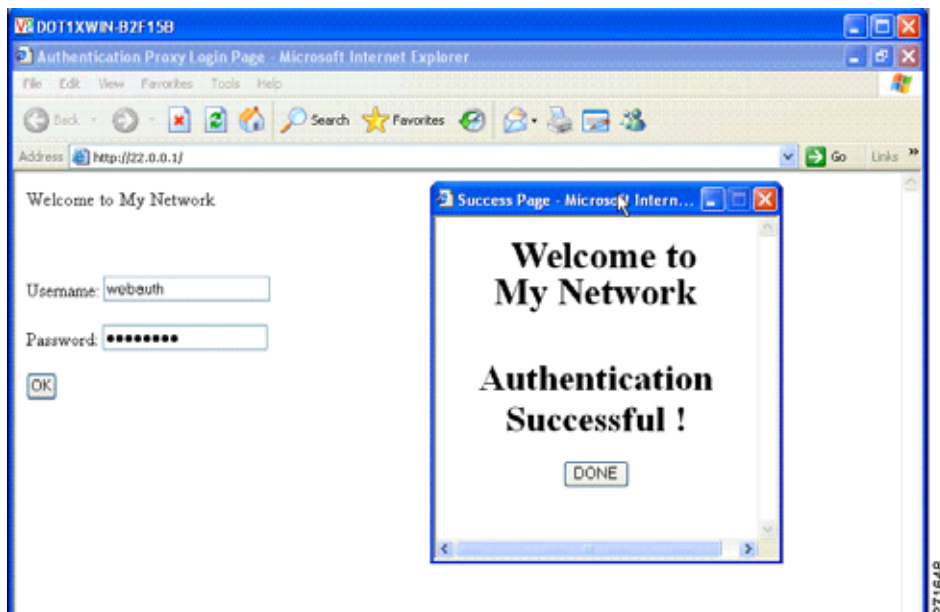
図 11-2 [Authentication Successful] バナー



バナーは[図 11-3](#) のようにカスタマイズすることもできます。

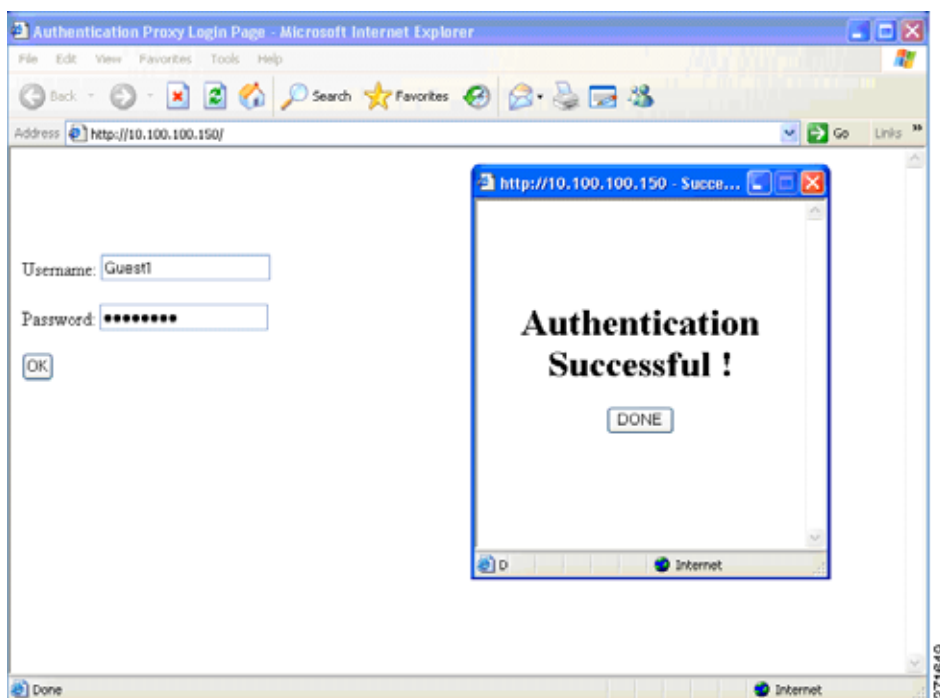
- **ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用して、スイッチ、ルータ、または会社名をバナーに追加します。
- **ip admission auth-proxy-banner http file-path** グローバル コンフィギュレーション コマンドを使用して、ログまたはテキスト ファイルをバナーに追加します。

図 11-3 カスタマイズされた Web パナー



パナーを有効にしない場合、ユーザ名とパスワードのダイアログボックスのみが Web 認証ログイン画面に表示されます。スイッチへのログイン時にパナーは表示されません (図 11-4 を参照)。

図 11-4 パナーのないログイン画面



詳細については、『Cisco IOS Security Command Reference』および「Web 認証ローカル パナーの設定」(P.11-17) を参照してください。

Web 認証のカスタマイズ可能な Web ページ

Web ベース認証プロセス中、スイッチの内部 HTTP サーバは、認証クライアントに配信される 4 つの HTML ページをホストします。これらのページにより、次の 4 つの認証プロセス ステートがユーザに通知されます。

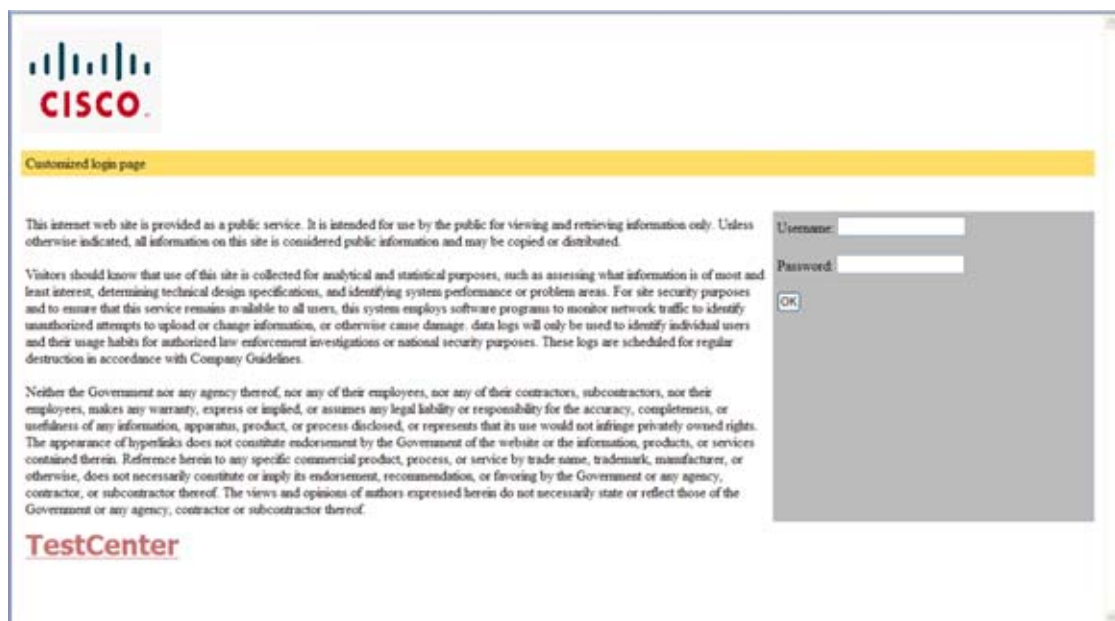
- ログイン：ユーザの認定証が要求されます。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：過剰なログイン失敗のため、ログインセッションがログインセッションが期限切れになりました。

注意事項

- デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。
- ロゴを使用し、ログイン、成功、失敗、および期限切れ Web ページのテキストを指定できます。
- バナー ページでは、ログイン ページのテキストを指定できます。
- これらのページは HTML 形式です。
- 特定の Universal Resource Locator (URL) にアクセスするには、HTML リダイレクト コマンドを含める必要があります。
- URL 文字列には、有効な URL (たとえば、<http://www.cisco.com>) を指定する必要があります。URL が不完全である場合は、Web ページ上に "page not found" (ページが見つかりません) または同様のエラーが表示される可能性があります。
- HTTP 認証の Web ページを設定する場合は、適切な HTML コマンド (ページのタイムアウトを設定するコマンド、非表示のパスワードを設定するコマンド、同じページが 2 回送信されていないことを確認するコマンドなど) をページに含める必要があります。
- 設定済みのログイン フォームがイネーブルである場合、ユーザを特定の URL にリダイレクトする CLI コマンドは使用できません。管理者は、Web ページ内でリダイレクションが設定されていることを確認する必要があります。
- 認証後にユーザを特定の URL にリダイレクトする CLI コマンドを入力した後で Web ページを設定するコマンドを入力すると、ユーザを特定の URL にリダイレクトする CLI コマンドは機能しません。
- 設定した Web ページは、スイッチのブート フラッシュまたはフラッシュにコピーできます。
- 設定したページには、スタック マスターまたはスタック メンバーからアクセスできます。
- ログイン ページを 1 つのフラッシュ上に配置し、成功ページと失敗ページを別のフラッシュ (たとえば、スタック マスターまたはスタック メンバー) 上に配置することもできます。
- 4 つのページをすべて設定する必要があります。
- バナー ページを Web ページと一緒に設定しても効果はありません。
- システム ディレクトリ (フラッシュ、ディスク 0、ディスクなど) 内に保存され、ログイン ページに表示される必要があるすべてのロゴ ファイル (イメージ、フラッシュ、音声、ビデオなど) は、ファイル名として `web_auth_<filename>` を使用する必要があります。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートします。

図 11-5 (P.11-7) に示すように、デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。認証のユーザのリダイレクト先 URL を指定することにより、内部の成功ページを置き換えることもできます。

図 11-5 カスタマイズ可能な認証ページ



詳細については、「[認証プロキシ Web ページのカスタマイズ](#)」(P.11-14) を参照してください。

Web ベース認証とその他の機能の相互作用

- 「ポートセキュリティ」(P.11-7)
- 「LAN ポート IP (LPIP)」(P.11-8)
- 「ゲートウェイ IP (GWIP)」(P.11-8)
- 「ACL」(P.11-8)
- 「コンテキストベース アクセス コントロール (CBAC)」(P.11-8)
- 「802.1X 認証」(P.11-8)
- 「EtherChannel」(P.11-8)

ポート セキュリティ

同一ポート上に Web ベース認証とポートセキュリティを設定することができます。Web ベース認証を使用してポートを認証し、ポートセキュリティを使用して、クライアントを含むすべての Media Access Control (MAC; メディア アクセス制御) アドレスに対するネットワーク アクセスを管理します。この場合、ポートを介してネットワークへアクセスできるクライアントの数またはグループを制限できます。

ポートセキュリティのイネーブル化の詳細については、「[ポートセキュリティの設定](#)」(P.26-9) を参照してください。

LAN ポート IP (LPIP)

同一ポート上に LAN Port IP (LPIP; LAN ポート IP) とレイヤ 2 Web ベース認証を設定できます。まず Web ベース認証を使用してホストが認証され、次に LPIP ポスチャ検証が実行されます。LPIP ホストポリシーは、Web ベース認証ホストポリシーを上書きします。

Web ベース認証アイドルタイマーの期限が満了すると、NAC ポリシーが削除されます。ホストが認証され、ポスチャが再び検証されます。

ゲートウェイ IP (GWIP)

Web ベース認証が VLAN のいずれかのスイッチポートに設定されている場合は、レイヤ 3 VLAN インターフェイス上に Gateway IP (GWIP; ゲートウェイ IP) を設定できません。

ゲートウェイ IP と同じレイヤ 3 インターフェイスに Web ベース認証を設定できます。両方の機能のホストポリシーがソフトウェアによって適用されます。GWIP ポリシーは、Web ベース認証ホストポリシーを上書きします。

ACL

VLAN ACL または Cisco IOS ACL をインターフェイス上に設定すると、Web ベース認証ホストポリシーが適用されたあとに ACL がホストトラフィックに適用されます。

レイヤ 2 Web ベース認証の場合は、ポートに接続されたホストからの入力トラフィックのデフォルトアクセスポリシーとして Port ACL (PACL; ポート ACL) を設定する必要があります。認証後、Web ベース認証ホストポリシーによって PACL が上書きされます。

MAC ACL と Web ベース認証は同じインターフェイス上に設定できません。

Web ベース認証は、アクセス VLAN が VACL キャプチャ用に設定されているポート上には設定できません。

コンテキストベースアクセスコントロール (CBAC)

Context-based Access Control (CBAC; コンテキストベースアクセスコントロール) がポート VLAN のレイヤ 3 VLAN インターフェイス上に設定されている場合は、Web ベース認証をレイヤ 2 ポート上に設定できません。

802.1X 認証

Web ベース認証は、フォールバック認証メソッドとして設定する場合を除き、802.1X 認証と同じポート上には設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定はすべてのメンバチャンネルに適用されます。

Web ベース認証の設定

- 「Web ベース認証のデフォルト設定」 (P.11-9)
- 「Web ベース認証の設定時の注意事項および制限事項」 (P.11-9)
- 「Web ベース認証設定のタスク リスト」 (P.11-10)
- 「認証ルールとインターフェイスの設定」 (P.11-10)
- 「AAA 認証の設定」 (P.11-11)
- 「スイッチと RADIUS サーバ間の通信設定」 (P.11-12)
- 「HTTP サーバの設定」 (P.11-13)
- 「Web ベース認証パラメータの設定」 (P.11-16)
- 「Web ベース認証のキャッシュ エントリの削除」 (P.11-17)

Web ベース認証のデフォルト設定

表 11-1 に、Web ベース認証のデフォルト設定を示します。

表 11-1 Web ベース認証のデフォルト設定

機能	デフォルト設定値
AAA	ディセーブル
RADIUS サーバ	
<ul style="list-style-type: none"> • IP アドレス • User Datagram Protocol (UDP; ユーザ データグラム プロトコル) 認証ポート • 鍵 	<ul style="list-style-type: none"> • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定時の注意事項および制限事項

- Web ベース認証は入力のための機能です。
- Web ベース認証はアクセス ポートだけに設定できます。Web ベース認証はトランク ポート、EtherChannel のメンバー ポート、およびダイナミック トランク ポート上ではサポートされません。
- Web ベースを設定する前に、デフォルト ACL をインターフェイス上に設定する必要があります。レイヤ 2 インターフェイスのポート ACL を設定するか、レイヤ 3 インターフェイスの Cisco IOS ACL を設定します。
- スタティック ARP キャッシュが割り当てられたレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能によって検出されません。
- デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルです。Web ベース認証を使用するには、IP デバイス トラッキング機能をイネーブルにする必要があります。

- スイッチの HTTP サーバを実行するには、少なくとも 1 つの IP アドレスを設定する必要があります。各ホストの IP アドレスに到達するためのルートを設定する必要があります。HTTP サーバからホストに HTTP ログイン ページが送信されます。
- 複数ホップ離れているホストでは、Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) トポロジの変更によってホスト トラフィックが別のポートに到着すると、トラフィックが中断する可能性があります。これは、レイヤ 2 (STP) トポロジの変更後に ARP および DHCP アップデートが送信されていない可能性があるためです。
- Web ベース認証は、ダウンロード可能なホスト ポリシーとして VLAN 割り当てをサポートしていません。
- IPv6 トラフィックに対しては、Web ベース認証はサポートされません。

Web ベース認証設定のタスク リスト

- 「認証ルールとインターフェイスの設定」 (P.11-10)
- 「AAA 認証の設定」 (P.11-11)
- 「スイッチと RADIUS サーバ間の通信設定」 (P.11-12)
- 「HTTP サーバの設定」 (P.11-13)
- 「AAA 失敗ポリシーの設定」 (P.11-16)
- 「Web ベース認証パラメータの設定」 (P.11-16)
- 「Web ベース認証のキャッシュ エントリの削除」 (P.11-17)

認証ルールとインターフェイスの設定

	コマンド	目的
ステップ 1	<code>ip admission name name proxy http</code>	Web ベース許可の認証ルールを設定します。
ステップ 2	<code>interface type slot/port</code>	インターフェイス コンフィギュレーション モードを開始し、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。 <i>type</i> には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 3	<code>ip access-group name</code>	デフォルトの ACL を適用します。
ステップ 4	<code>ip admission name</code>	指定したインターフェイス上に Web ベース認証を設定します。
ステップ 5	<code>exit</code>	コンフィギュレーション モードに戻ります。
ステップ 6	<code>ip device tracking</code>	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show ip admission configuration</code>	設定を表示します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ファストイーサネットポート 5/1 で Web ベース認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name webauth1
http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

	コマンド	目的
ステップ1	<code>aaa new-model</code>	AAA 機能をイネーブルにします。
ステップ2	<code>aaa authentication login default group {tacacs+ radius}</code>	ログイン時の認証方式のリストを定義します。
ステップ3	<code>aaa authorization auth-proxy default group {tacacs+ radius}</code>	Web ベース認可の認可方式のリストを作成します。
ステップ4	<code>tacacs-server host {hostname ip_address}</code>	AAA サーバを指定します。RADIUS サーバについては、「スイッチと RADIUS サーバ間の通信設定」(P.11-12)を参照してください。
ステップ5	<code>tacacs-server key {key-data}</code>	スイッチと Terminal Access Controller Access Control System (TACACS) サーバの間で使用される認可および暗号鍵を設定します。
ステップ6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

次に、AAA をイネーブルにする例を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group tacacs+
Switch(config)# aaa authorization auth-proxy default group tacacs+
```

スイッチと RADIUS サーバ間の通信設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリを同じサービス（例えば認証など）に対して設定すると、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして機能します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>ip radius source-interface interface_name</code>	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	<code>radius-server host {hostname ip-address} test username username</code>	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 test username username オプションを使用すると、RADIUS サーバとの接続を自動的にテストできます。 username には、有効なユーザ名を指定する必要はありません。 key オプションには、スイッチと RADIUS サーバとの間で使用する認証および暗号鍵を指定します。 複数の RADIUS サーバを使用する場合は、このコマンドをサーバごとに再入力します。
ステップ 3	<code>radius-server key string</code>	スイッチと RADIUS サーバ上で動作する RADIUS デーモンの間で使用される認可および暗号鍵を設定します。
ステップ 4	<code>radius-server vsa send authentication</code>	RADIUS サーバからの ACL のダウンロードをイネーブルにします。この機能は、Cisco IOS Release 12.2(50)SG でサポートされています。
ステップ 5	<code>radius-server dead-criteria tries num-tries</code>	サーバを非アクティブにすることを検討する前に、RADIUS サーバへの未応答の送信メッセージの数を指定します。指定できる num-tries の範囲は 1 ~ 100 です。

RADIUS サーバ パラメータを設定する際には、次の作業を行います。

- **key string** は別のコマンドラインで指定します。
- **key string** には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵はテキスト スtring で、RADIUS サーバで使用されている暗号鍵と一致する必要があります。
- **key string** を指定する場合は、鍵の途中および末尾でスペースを使用します。鍵でスペースを使用する場合は、引用符が鍵の一部である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵と一致している必要があります。

- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵の値をグローバルに設定するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、次の URL の『Cisco IOS Security Configuration Guide』 Release 12.2 および『Cisco IOS Security Command Reference』 Release 12.2 を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html



(注) RADIUS サーバ上でも、スイッチの IP アドレス、サーバとスイッチの双方で共有されるキー スtring、ダウンロード可能な ACL (DAACL) など、いくつかの値を設定する必要があります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。イネーブルにできるサーバは、HTTP または HTTPS です。

	コマンド	目的
ステップ 1	ip http server	HTTP サーバをイネーブルにします。Web ベース認証機能では、HTTP サーバを使用してユーザ認証用のホストと通信します。
ステップ 2	ip http secure-server	HTTPS をイネーブルにします。

カスタム認証プロキシ Web ページを設定するか、またはログインに成功した場合のリダイレクション URL を指定できます。



(注) **ip http secure-secure** コマンドの実行時にセキュアな認証を保證するため、ユーザが HTTP 要求を送信しても、ログイン ページは常に HTTPS (セキュア HTTP) となります。

- 認証プロキシ Web ページのカスタマイズ
- ログインに成功した場合のリダイレクション URL の指定

認証プロキシ Web ページのカスタマイズ

Web ベース認証時に、スイッチのデフォルト HTML ページではなく 4 つの代替 HTML ページをユーザに表示する Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、スイッチのフラッシュ メモリにカスタム HTML ファイルを保存してから、このタスクをグローバル コンフィギュレーション モードで実行します。

	コマンド	目的
ステップ 1	ip admission proxy http login page file <i>device:login-filename</i>	デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの、スイッチのメモリ ファイル システムにおける場所を指定します。 <i>device:</i> はフラッシュ メモリを表します。
ステップ 2	ip admission proxy http success page file <i>device:success-filename</i>	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 3	ip admission proxy http failure page file <i>device:fail-filename</i>	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 4	ip admission proxy http login expired page file <i>device:expired-filename</i>	デフォルトのログイン期限切れページの代わりに使用するカスタム HTML ファイルの場所を指定します。

カスタマイズされた認証プロキシ Web ページを設定する場合は、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、4 つのカスタム HTML ファイルをすべて指定します。4 つのファイルをすべて指定しないと、デフォルトの内部 HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルは、スイッチのフラッシュ メモリ上に存在する必要があります。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のすべてのイメージは、アクセス可能な HTTP サーバに存在する必要があります。管理ルール内に代行受信 ACL を設定します。
- カスタム ページからの外部リンクには、管理ルール内に代行受信 ACL を設定する必要があります。
- 有効な Domain Name System (DNS; ドメイン ネーム システム) サーバにアクセスするには、外部リンクまたは外部イメージに必要な名前解決で、管理ルール内に代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルである場合、設定された `auth-proxy-banner` は使用されません。
- カスタム Web ページ機能がイネーブルである場合、ログインの失敗機能のリダイレクション URL は使用できません。
- カスタム ファイルの指定を削除するには、このコマンドの `no` 形式を使用します。

カスタム ログイン ページはパブリック Web 形式であるため、このページに関する次の注意事項に従ってください。

- ログイン フォームは、ユーザ名とパスワードに対するユーザ エントリを受け入れ、`uname` と `pwd` をユーザに表示する必要があります。
- カスタム ログイン ページは、ページのタイムアウト、非表示のパスワード、冗長送信の防止など、Web フォームに関するベストプラクティスに従っている必要があります。

次に、カスタム認証プロキシ Web ページを設定する例を示します。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
```

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

次に、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
Switch# show ip admission configuration
Authentication proxy webpage
  Login page           : flash:login.htm
  Success page        : flash:success.htm
  Fail Page           : flash:fail.htm
  Login expired Page  : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

ログインに成功した場合のリダイレクション URL の指定

内部の成功 HTML ページを効果的に置き換えることにより、認証後のユーザのリダイレクト先 URL を指定できます。

コマンド	目的
<code>ip admission proxy http success redirect url-string</code>	デフォルトのログイン成功ページの代わりに、ユーザのリダイレクション URL を指定します。

ログインに成功した場合のリダイレクション URL を設定する場合は、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルの場合、リダイレクション URL 機能はディセーブルになり、CLI で使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルである場合、設定された `auth-proxy-banner` は使用されません。
- リダイレクション URL の指定を削除するには、このコマンドの `no` 形式を使用します。

次に、ログインに成功した場合のリダイレクション URL を設定する例を示します。

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

次に、ログインに成功した場合のリダイレクション URL を確認する例を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

	コマンド	目的
ステップ 1	<code>ip admission name rule-name proxy http event timeout aaa policy identity identity_policy_name</code>	AAA の失敗ルールを作成し、AAA サーバに到達できない場合にセッションに適用されるアイデンティティ ポリシーを関連付けます。 (注) ルールを削除するには、 <code>no ip admission name rule-name proxy http event timeout aaa policy identity</code> グローバル コンフィギュレーション コマンドを使用します。
ステップ 2	<code>ip admission ratelimit aaa-down number_of_sessions</code>	(任意) サービスを返すときの AAA サーバのフラッディングを防ぐため、AAA ダウン ステートのホストからの認証試行回数に対してレート制限を実施します。

次に、AAA の失敗ポリシーを適用する例を示します。

```
Switch(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy  
identity GLOBAL_POLICY1
```

次に、接続されているホストが AAA ダウン ステートであるかどうかを判断する例を示します。

```
Switch# show ip admission cache  
Authentication Proxy Cache  
Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて、特定のセッションに関する詳細情報を表示する例を示します。

```
Switch# show ip admission cache 209.165.201.11  
Address          : 209.165.201.11  
MAC Address      : 0000.0000.0000  
Interface        : Vlan333  
Port             : 3999  
Timeout          : 60  
Age              : 1  
State            : AAA Down  
AAA Down policy  : AAA_FAIL_POLICY
```

Web ベース認証パラメータの設定

ユーザを一定の待機時間、ウォッチ リストに配置するまでに許容する失敗ログイン試行の最大数を設定できます。

	コマンド	目的
ステップ 1	<code>ip admission max-login-attempts number</code>	失敗ログイン試行の最大数を設定します。設定範囲は 1 ~ 2147483647 回です。デフォルトは 5 です。
ステップ 2	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 3	<code>show ip admission configuration</code>	認証プロキシ設定を表示します。
ステップ 4	<code>show ip admission cache</code>	認証エントリのリストを表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、失敗ログイン試行の最大数を 10 回に設定する例を示します。

```
Switch(config)# ip admission max-login-attempts 10
```

Web 認証ローカル バナーの設定

Web 認証を設定したスイッチにローカル バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip admission auth-proxy-banner http [banner-text file-path]	ローカル バナーをイネーブルにします。 (任意) <i>C banner-text C</i> を入力し、カスタム バナーを作成します。 <i>C</i> は、バナーに表示されるファイルのファイル パスを示しています (ロゴまたはテキスト ファイルなど)。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、カスタム メッセージ *My Switch* を表示するローカル バナーを設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com にある『[Cisco IOS Security Command Reference](#)』の「Authentication Proxy Commands」の章を参照してください。

Web ベース認証のキャッシュ エントリの削除

コマンド	目的
clear ip auth-proxy cache {* <i>host ip address</i> }	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するにはアスタリスクを使用します。単一ホストのエントリを削除するには、特定の IP アドレスを入力します。
clear ip admission cache {* <i>host ip address</i> }	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するにはアスタリスクを使用します。単一ホストのエントリを削除するには、特定の IP アドレスを入力します。

次に、IP アドレスが 209.165.201.1 のクライアントに対する Web ベース認証セッションを削除する例を示します。

```
Switch# clear ip auth-proxy cache 209.165.201.1
```

Web ベース認証ステータスの表示

すべてのインターフェイスまたは特定のポートの Web ベース認証設定を表示するには、次の作業を行います。

コマンド	目的
ステップ1 show authentication sessions [<i>interface type slot/port</i>]	Web ベース認証設定を表示します。 type = fastethernet、gigabitethernet、または tengigabitethernet (任意) interface キーワードを使用して、特定のインターフェイスの Web ベース認証設定を表示します。

次に、グローバル Web ベース認証ステータスだけを表示する例を示します。

```
Switch# show authentication sessions
```

次に、ギガビット インターフェイス 3/27 の Web ベース認証設定を表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet 3/27
```



CHAPTER 12

インターフェイス特性の設定

この章では、Catalyst 3750 スイッチ上の各種インターフェイスのタイプ、およびその設定方法について説明します。



(注) 特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

この章で説明する内容は、次のとおりです。

- 「インターフェイス タイプの概要」 (P.12-1)
- 「インターフェイス コンフィギュレーション モードの使用方法」 (P.12-12)
- 「イーサネット インターフェイスの設定」 (P.12-17)
- 「レイヤ 3 インターフェイスの設定」 (P.12-28)
- 「システム MTU の設定」 (P.12-30)
- 「インターフェイスのモニタリングおよびメンテナンス」 (P.12-34)



(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスおよび『Cisco IOS Interface Command Reference』Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

インターフェイス タイプの概要

ここでは、スイッチによってサポートされる各種インターフェイス タイプについて説明するとともに、これらのインターフェイス タイプの設定に関する詳細情報が記載された章についても言及します。



(注) スイッチ背面のスタック ポートは、イーサネット ポートではないため設定できません。

- 「ポートベースの VLAN」 (P.12-2)
- 「スイッチ ポート」 (P.12-3)
- 「ルーテッド ポート」 (P.12-5)
- 「スイッチ仮想インターフェイス」 (P.12-5)
- 「EtherChannel ポート グループ」 (P.12-7)

- 「10 ギガビット イーサネット インターフェイス」 (P.12-7)
- 「Power over Ethernet (PoE) ポート」 (P.12-8)
- 「インターフェイスの接続」 (P.12-11)



(注)

Catalyst 3750G Integrated Wireless LAN Controller スイッチの内部ポートの詳細については、次を参照してください。付録 A 「Catalyst 3750G Integrated Wireless LAN Controller スイッチの設定」

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的に分割されたスイッチによるネットワークです。VLAN の詳細については、第 14 章「VLAN の設定」を参照してください。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC (メディア アクセス制御) アドレス テーブルがあります。VLAN が認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) トランク上のネイバーからその存在を学習したとき、またはユーザが VLAN を作成したときです。

VLAN を設定するには、`vlan vlan-id` グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の VLAN 設定情報は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 である場合、拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定するには、まず VTP モードを透過に設定する必要があります。透過モードで作成された拡張範囲 VLAN は、VLAN データベースに追加されませんが、スイッチの実行コンフィギュレーション ファイルに保存されます。VTP がバージョン 3 である場合、クライアント モードまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN データベースに保存されます。

VLAN は、スタック全体にまたがり、複数のポートで構成することができます。VLAN データベースは、スタックのすべてのスイッチにダウンロードされ、スタックのすべてのスイッチは、同一の VLAN データベースを構築します。実行コンフィギュレーションと保存済みコンフィギュレーションは、スタック内のすべてのスイッチで同一です。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。
- トンネル ポートの場合は、カスタマー固有の VLAN タグ用に VLAN ID の設定と定義を行います。第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。スイッチ ポートは、1 つ以上の VLAN に所属します。物理インターフェイスおよび対応付けられたレイヤ 2 プロトコルの管理にスイッチ ポートを使用します。スイッチ ポートは、ルーティングおよびブリッジングを処理しません。

スイッチ ポートは、アクセス ポート、トランク ポート、または、トンネル ポートである可能性があります。ポートは、アクセス ポートまたはトランク ポートに設定できます。また、ポート単位で Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチ ポート モードも設定できます。IEEE 802.1Q トランク ポートに接続した非対称リンクの一部として、トンネル ポートを手動で設定する必要があります。

スイッチ ポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。

レイヤ 3 モードのインターフェイスをレイヤ 2 モードにするには、**switchport** コマンドを **no** キーワードで使用します。



(注)

レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

アクセス ポート特性およびトランク ポート特性の詳細については、第 14 章「VLAN の設定」を参照してください。トンネル ポートの詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

アクセス ポート

アクセス ポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タギングなしのネイティブ フォーマットで送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。

アクセス ポートがタグ付きパケット (Inter-Switch Link (ISL; スイッチ間リンク) またはタグ付き IEEE 802.1Q) を受信した場合、そのパケットは廃棄され、送信元アドレスは学習されません。

2 種類のアクセス ポートがサポートされています。

- スタティック アクセス ポート。このポートは、手動で VLAN に割り当てます (IEEE 802.1X で使用する場合は RADIUS サーバを使用します。詳細については、「VLAN 割り当てを使用した 802.1X 認証」(P.10-16) を参照してください。
- ダイナミック アクセス ポートの VLAN メンバシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの伝送はポートの VLAN メンバシップが検出されたときにだけイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN Membership Policy Server (VMPS; VLAN メンバシップ ポリシー サーバ) によって VLAN に割り当てられます。VMPS として動作できるのは、Catalyst 6500 シリーズ スイッチです。Catalyst 3750 スイッチを VMPS サーバにすることはできません。

また、Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータトラフィック用に使用するように設定できます。音声 VLAN ポートの詳細については、第 16 章「音声 VLAN の設定」を参照してください。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバーとなります。

サポートされているトランク ポートのタイプは次のとおりです。

- ISL トランク ポートでは、受信パケットはすべて ISL ヘッダーを使用してカプセル化されているものと見なされ、送信パケットはすべて ISL ヘッダーとともに送信されます。ISL トランク ポートから受信したネイティブ (タグなし) フレームは廃棄されます。
- IEEE 802.1Q トランク ポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートは、デフォルトの Port VLAN ID (PVID; ポート VLAN ID) に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。NULL VLAN ID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。残りのトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは、VTP に認識されているすべての VLAN のメンバーですが、トランク ポートごとに VLAN の許可リストを設定して、VLAN メンバシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN (VLAN ID 1 ~ 4094) が許可リストに含まれます。トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブル状態にある場合に限り、VLAN のメンバーになることができます。VTP が新しいイネーブル VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバーになり、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランク ポートの許可リストに登録されていない、新しいイネーブル VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トランク ポートの詳細については、第 14 章「VLAN の設定」を参照してください。

トンネル ポート

トンネル ポートは IEEE 802.1Q トンネリングで使用され、サービスプロバイダー ネットワークの顧客のトラフィックを、同じ VLAN 番号を使用するその他の顧客から分離します。サービスプロバイダー エッジスイッチのトンネル ポートから顧客のスイッチの IEEE 802.1Q トランク ポートに、非対称リンクを設定します。エッジスイッチのトンネル ポートに入るパケットには、顧客の VLAN すでに IEEE802.1Q タグが付いており、顧客ごとに IEEE 802.1Q タグの別のレイヤ (メトロ タグと呼ばれる) でカプセル化され、サービスプロバイダー ネットワークで一意的 VLAN ID が含まれます。タグが 2 重に付いたパケットは、その他の顧客のものとは異なる、元の顧客の VLAN が維持されてサービスプロバイダー ネットワークを通過します。発信インターフェイス、およびトンネル ポートでは、メトロ タグが削除されて顧客のネットワークのオリジナル VLAN 番号が取得されます。

トンネル ポートは、トランク ポートまたはアクセス ポートにすることができず、それぞれの顧客に固有の VLAN に属する必要があります。

トンネル ポートの詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

ルーテッド ポート

ルーテッド ポートは物理ポートであり、ルータ上にあるポートのように動作しますが、ルータに接続されている必要はありません。ルーテッド ポートは、アクセス ポートとは異なり、特定の VLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスのように動作します。ルーテッド ポートは、レイヤ 3 ルーティング プロトコルで設定できます。ルーテッド ポートはレイヤ 3 インターフェイス専用で、DTP や Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) などのレイヤ 2 プロトコルはサポートしません。ルーテッド ポートは、IP ベース イメージまたは IP サービス イメージが実行されているスイッチ上でだけサポートされます。

ルーテッド ポートを設定するには、**no switchport** インターフェイス コンフィギュレーション コマンドでインターフェイスをレイヤ 3 モードにします。次に、ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、**ip routing** および **router protocol** グローバル コンフィギュレーション コマンドを使用してルーティング プロトコルの特性を指定します。



(注) **no switchport** インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスがいったんシャットダウンしてから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 2 モードのインターフェイスをレイヤ 3 モードにした場合、影響のあるインターフェイスに関連する以前の設定が消失する可能性があります。

ソフトウェアに、設定できるルーテッド ポートの個数制限はありません。ただし、ハードウェアには限界があるため、この個数と設定されている他の機能の数との相互関係によって CPU パフォーマンスに影響が及ぶことがあります。ハードウェアのリソース制限に達したときに何が発生するかについては、「レイヤ 3 インターフェイスの設定」(P.12-28) を参照してください。

IP ユニキャストおよびマルチキャストのルーティングおよびルーティング プロトコルの詳細については、第 38 章「IP ユニキャスト ルーティングの設定」および第 46 章「IP マルチキャスト ルーティングの設定」を参照してください。



(注) IP ベース イメージは、スタティック ルーティングおよび Routing Information Protocol (RIP) をサポートします。フル レイヤ 3 ルーティングまたはフォールバック ルーティングを行う場合、IP サービス イメージを搭載する必要があります。スイッチ スタックでは、スタック マスターに IP サービス イメージを搭載する必要があります。

スイッチ仮想インターフェイス

Switch Virtual Intertface (SVI; スイッチ仮想インターフェイス) は、スイッチ ポートの VLAN を、システムのルーティング機能またはブリッジング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に対応付けできるのは 1 つの SVI ですが、VLAN 間でルーティングする場合、VLAN 間でルーティングできないプロトコルをフォールバック ブリッジングする場合、またはスイッチと IP ホストの接続を行う場合のみ、VLAN に SVI を設定する必要があります。

デフォルトでは、SVI はデフォルト VLAN (VLAN 1) 用に作成され、リモート スイッチの管理を可能にします。追加の SVI は明示的に設定する必要があります。



(注) インターフェイス VLAN 1 は削除できません。

SVI はシステムにしか IP ホスト接続を行いません。レイヤ 3 モードでは、SVI 全体にルーティングを設定できます。

スイッチは合計 1005 の VLAN (および SVI) をサポートしますが、ハードウェアには限界があるため、SVI とルーテッド ポートの数および設定されている他の機能の数との相互関係によって、CPU パフォーマンスに影響が及ぶことがあります。ハードウェアのリソース制限に達したときに何が発生するかについては、「[レイヤ 3 インターフェイスの設定](#)」(P.12-28) を参照してください。

SVI は、VLAN インターフェイスに対して **vlan** インターフェイス コンフィギュレーション コマンドを実行したときに初めて作成されます。VLAN は、ISL または IEEE802.1Q カプセル化トランク上のデータ フレームに関連付けられた VLAN タグ、あるいはアクセス ポート用に設定された VLAN ID に対応します。トラフィックをルーティングするそれぞれの VLAN に対して VLAN インターフェイスを設定し、IP アドレスを割り当ててください。詳細については、「[手動でのスイッチ情報の割り当て](#)」(P.3-16) を参照してください。



(注) 作成した SVI をアクティブにするには、物理ポートに関連付ける必要があります。

SVI は、ルーティング プロトコルとブリッジング設定をサポートします。IP ルーティング設定の詳細については、[第 38 章「IP ユニキャスト ルーティングの設定](#)」、[第 46 章「IP マルチキャスト ルーティングの設定](#)」および[第 48 章「フォールバック ブリッジングの設定](#)」を参照してください。



(注) IP ベース イメージはスタティック ルーティングおよび RIP をサポートします。より高度なルーティングやフォールバック ブリッジングを行う場合は、IP サービス イメージを搭載する必要があります。

SVI Autostate Exclude

VLAN 上で複数のポートを持つ SVI のライン ステートは、次の条件を満たした場合、*up* ステートになります。

- スwitchに VLAN が存在し、その VLAN データベースでアクティブである。
- VLAN インターフェイスが存在し、管理上のダウン ステートではない。
- 少なくとも 1 つのレイヤ 2 (アクセスまたはトランク) ポートが存在し、VLAN に *up* ステートのリンクがある。さらにその VLAN でスパニングツリー フォワーディング ステートにある。



(注) 対応する VLAN リンクに属する最初のスイッチポートがアップし、STP フォワーディング ステートになると、VLAN インターフェイスのプロトコル リンク ステートがアップします。

VLAN が複数のポートを持っている場合のデフォルト アクションは、VLAN のすべてのポートがダウンすると、SVI がダウンします。SVI Autostate Exclude 機能を使用すると、SVI ライン ステートのアップまたはダウン計算からポートが除外されるように設定できます。たとえば、VLAN のアクティブ ポートだけがポートをモニタリングしている場合、ポートに Autostate Exclude を設定し、他のすべてのポートがダウンしたときに VLAN をダウンできるように設定できます。ポートで **autostate exclude** がイネーブルの場合、ポートでイネーブルのすべての VLAN に適用されます。

VLAN の 1 つのレイヤ 2 ポートがコンバージェンス (STP リスニング ラーニング ステートからフォワーディング ステートへ移行) を実行すると、VLAN インターフェイスがアップします。これにより、ルーティング プロトコルなどの機能が VLAN インターフェイスを使用できなくなります (ルーティングのブラック ホールなど他の大きな問題が緩和され、完全に動作しているかようになります)。Autostate Exclude の設定については、「[SVI Autostate Exclude の設定](#)」(P.12-29) を参照してください。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱います。このようなポート グループは、スイッチ間、またはスイッチおよびサーバ間で広帯域接続を行う単一論理ポートとして動作します。EtherChannel は、チャンネルのリンク全体でトラフィックの負荷を分散させます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。複数のトランク ポートを 1 つの論理トランク ポートにグループ化したり、複数のアクセス ポートを 1 つの論理アクセスポートに、複数のトンネル ポートを 1 つの論理トンネル ポートに、または複数のルーテッド ポートを 1 つの論理ルーテッド ポートにグループ化したりできます。

ほとんどのプロトコルは、単一ポートまたは集約スイッチ ポート上で動作し、ポート グループ内の物理ポートを認識しません。例外は、DTP、Cisco Discovery Protocol (CDP; シスコ検出プロトコル)、および Port Aggregation Protocol (PAgP; ポート集約プロトコル) で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャンネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。channel-group インターフェイス コンフィギュレーション コマンドを使用して、ダイナミックにポート チャンネル論理インターフェイスを作成します。このコマンドは物理および論理ポートをバインドします。

レイヤ 3 インターフェイスの場合は、interface port-channel グローバル コンフィギュレーション コマンドを使用して手動で論理インターフェイスを作成します。そのあと、channel-group インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

詳細は、第 37 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

10 ギガビット イーサネット インターフェイス

Catalyst 3750G-16TD スイッチには 10 ギガビット イーサネット インターフェイスが 1 つ搭載されています。スイッチでは 10 ギガビット イーサネット XENPAK モジュールを使用してネットワークへの接続を確立します。

10 ギガビット イーサネット インターフェイスは全二重モードでのみ動作します。インターフェイスはスイッチ ポートまたはルーテッド ポートとして設定可能です。Catalyst 3750 スイッチのスタックでは最大で 9 つの 10 ギガビット イーサネット インターフェイスを持つことができます。クロススタック EtherChannel では最大 2 つの 10 ギガビット モジュール ポートをサポートしています。

スイッチでサポートされる XENPAK モジュールの最新情報については、リリース ノートを参照してください。

XENPAK モジュールの詳細については、XENPAK モジュールのマニュアルを参照してください。



(注)

10 ギガビット イーサネット モジュール ポートは、『Hardware Installation Guide』では 10 ギガビット イーサネット XENPAK モジュールと呼ばれています。

Power over Ethernet (PoE) ポート

Power over Ethernet (PoE; イーサネット経由の電源供給) 対応スイッチ ポートでは、接続している次のデバイスに電力が自動的に供給されます (回路に電力が供給されていないことをスイッチが感知した場合)。

- シスコ先行標準受電装置 (Cisco IP Phone および Cisco Aironet アクセス ポイントなど)
- IEEE 802.3af 準拠の受電装置

受電装置が PoE スイッチおよび AC 電源に接続されている場合だけ、冗長電力として利用できます。

PoE に関する内容は次のとおりです。

- 「サポート対象のプロトコルおよび標準」 (P.12-8)
- 「受電装置検出および初期電力割り当て」 (P.12-9)
- 「電力管理モード」 (P.12-10)

サポート対象のプロトコルおよび標準

スイッチでは、次のプロトコルおよび標準を使用して PoE をサポートしています。

- 電力消費を含む CDP: 受電装置は、消費している電力量をスイッチに通知します。スイッチは、電力消費メッセージに応答しません。スイッチは、PoE ポートに電力を供給するか、PoE ポートから電力を取り除くだけです。
- シスコ インテリジェント電力管理: 受電装置およびスイッチは、電力ネゴシエーション CDP メッセージによって電力消費レベルについてネゴシエーションを行います。このネゴシエーションにより、7 W を超える電力を消費する高電力シスコ受電装置は、最高電力モードで動作できるようになります。受電装置は、最初に低電力モードでブートして 7 W 未満の電力を消費し、ネゴシエーションを行って高電力モードで動作するための十分な電力を得ます。受電装置は、スイッチから確認を受信した場合に限って高電力モードに切り替わります。

高電力デバイスは、電力ネゴシエーション CDP がサポートされていないスイッチにおいて、低電力で動作できます。

Cisco IOS Release 12.2(25)SE 以前の場合、PoE 対応スイッチ (インテリジェント電力管理がサポート非対象) では、インテリジェント電力管理がサポートされている高電力受電装置が、低電力モードで動作します。低電力モードのデバイスでは、すべての機能は動作しません。

シスコ インテリジェント電力管理には、電力消費を含む CDP との下位互換性があります。スイッチは、受信した CDP メッセージに従って応答します。CDP は、サードパーティ製受電装置でサポートされません。このため、スイッチは IEEE 分類を使用してデバイスの電力使用量を判断しません。

- IEEE 802.3af: この標準の主な機能は、受電装置検出、電力管理、切断検出、オプションの受電装置電力分類です。詳細については、標準を参照してください。

受電装置検出および初期電力割り当て

スイッチは、PoE 対応ポートがシャットダウン状態でなく、PoE がイネーブルになっていて（デフォルト）、接続したデバイスが AC アダプタによって電力供給されていない場合、シスコ先行標準受電装置または IEEE 準拠の受電装置を検出します。

デバイスが検出されると、スイッチは、デバイスのタイプに基づいてデバイスの電力要件を判断します。

- シスコ先行標準の受電装置は、スイッチがそのデバイスを検出しても電力要件を提供しないので、スイッチは、パワーバジェットの初期割り当てとして 15.4 W を割り当てます。
初期電力割り当ては、受電装置が要求する最大電力量です。スイッチは、受電装置を検出して電力供給する場合、この量の電力を最初に割り当てます。スイッチが受電装置から CDP メッセージを受信し、受電装置が CDP 電力ネゴシエーション メッセージでスイッチと電力レベルについてネゴシエーションを行った場合、初期電力割り当ては調整されることがあります。
- スイッチは、検出した IEEE デバイスを電力消費クラス内で分類します。スイッチは、パワーバジェットで使用可能な電力に基づいて、ポートに電力供給できるかどうか判断します。表 12-1 は、電力レベルの一覧です。

表 12-1 IEEE 電力分類

クラス	スイッチから要する最大電力レベル
0 (クラス ステータス不明)	15.4 W
1	4 W
2	7 W
3	15.4 W
4 (将来の使用のために予約)	クラス 0 としての扱い

スイッチは電力要求のモニタとトラッキングを行い、電力が使用可能である場合に限り電力を供給します。スイッチはパワーバジェット（スイッチで PoE に使用できる電力量）をトラッキングします。電力の供給または拒否がポートで行われると、スイッチはパワーアカウンティング計算を実行し、パワーバジェットを最新に保ちます。

電力がポートに適用されたあとで、スイッチは CDP を使用して、接続されたシスコ受電装置の実際の電力消費要件を判断し、パワーバジェットを相応に調整します。これはサードパーティ製 PoE デバイスには適用されません。スイッチは要件を処理して電力の供給または拒否を行います。要求が認可されると、スイッチはパワーバジェットを更新します。要求が拒否された場合、スイッチは、ポートの電力がオフに切り替わっていることを確認し、Syslog メッセージを生成して LED を更新します。受電装置は、追加の電力についてもスイッチとネゴシエーションを行うこともできます。

不足電圧、過電圧、過熱、オシレータ障害、または短絡状態による障害をスイッチが検出した場合、ポートへの電源をオフにし、Syslog メッセージを生成し、パワーバジェットと LED を更新します。

PoE 機能は、スイッチがスタック メンバーであるかどうかに関わらず同じように動作します。パワーバジェットはスイッチ単位で、スタック内の他のスイッチの影響を受けません。新しいスタック マスターが選出されても、PoE の動作には影響しません。スタック マスターは、スタック内のすべてのスイッチおよびポートの PoE のステータスをトラッキングし続け、出力表示にそのステータスを含めます。

電力管理モード

スイッチでは、次の PoE モードがサポートされます。

- **auto** : 接続されているデバイスで電力が必要かどうか、スイッチが自動的に検出します。ポートに接続されている受電装置をスイッチが検出し、スイッチに十分な電力がある場合、スイッチは電力を供給してパワー バジレットを更新し、先着順でポートの電力をオンに切り替えて LED を更新します。LED の詳細については、『Hardware Installation Guide』を参照してください。

すべての受電装置用としてスイッチに十分な電力がある場合は、すべての受電装置がアップします。スイッチに接続された受電装置すべてに対し十分な電力が利用できる場合、すべてのデバイスに電力を供給します。利用できる PoE が十分でない場合、または他のデバイスが電力を待っている間にデバイスが切断されて再接続された場合、どのデバイスへ電力が供給されるかが定義できなくなります。

許可電力がシステム パワー バジレットを超える場合、スイッチは電力を拒否し、ポートへの電力がオフになっていることを確認したうえで、Syslog メッセージを生成し、LED を更新します。電力が拒否されたあと、スイッチは定期的にパワー バジレットを再確認し、続けて電力要求の許可を試行します。

スイッチにより電力を供給されているデバイスが、さらに壁面コンセントに接続されている場合、スイッチはデバイスに電力を供給し続けることがあります。この時、デバイスがスイッチから電力を供給されているか、AC 電源から電力を供給されているかにかかわらず、スイッチは自身が引き続きデバイスへ電力を供給しているとの通知を行うことがあります。

受電装置が取り外された場合、スイッチは切断を自動的に検出し、ポートから電力を取り除きます。非受電装置を接続しても、そのデバイスに障害は発生しません。

ポートで許可される最大ワット数を指定できます。受電装置の IEEE クラス最大ワット数が、設定した最大値より大きい場合、スイッチはそのポートに電力を供給しません。スイッチが受電装置に電力を供給したが、受電装置が設定最大値より多くの電力を CDP メッセージによってあとで要求した場合、スイッチはポートの電力を取り除きます。その受電装置に割り当てられていた電力は、グローバル パワー バジレットに戻されます。ワット数を指定しない場合、スイッチは最大値の電力を供給します。任意の PoE ポートで **auto** 設定を使用してください。auto モードがデフォルト設定です。

- **static** : スwitchは、受電装置が接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。スイッチは、設定した最大ワット数をポートに割り当てますが、その量は、IEEE クラスまたは受電装置からの CDP メッセージによって調整されません。電力があらかじめ割り当てられているので、最大ワット数以下の電力を使用する受電装置は、固定ポートに接続されている場合、電力が保証されます。ポートは先着順方式に関連しなくなります。

しかし受電装置の IEEE クラスが最大ワット数より大きい場合、スイッチはその受電装置に電力を供給しません。受電装置で最大ワット数を超える電力が必要になったことを CDP メッセージによってスイッチが学習した場合、その受電装置はシャットダウンされます。

ワット数を指定しない場合、スイッチは最大値をあらかじめ割り当てます。スイッチは、受電装置を検出した場合に限り、ポートに電力を供給します。優先順位が高いインターフェイスには、**static** 設定を使用してください。

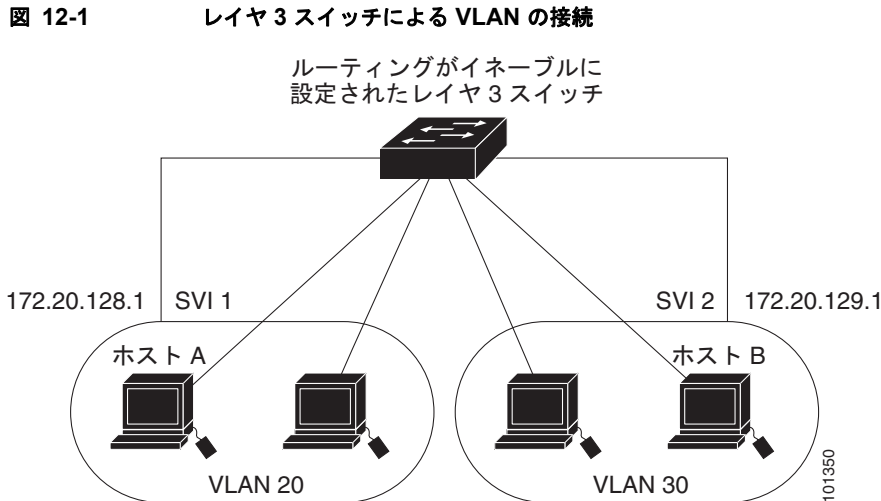
- **never** : スwitchは受電装置検出をディセーブルにして、電力供給されていないデバイスが接続されても、PoE ポートに電力を供給しません。PoE 対応ポートに電力を絶対に適用せず、そのポートをデータ専用ポートにする場合に限り、このモードを使用してください。

PoE ポートの設定の詳細については、「PoE ポートの電力管理モードの設定」(P.12-24) を参照してください。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。

標準のレイヤ 2 スイッチを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。ルーティングがイネーブルに設定されたスイッチを使用することにより、IP アドレスを割り当てた SVI で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、スイッチを介してパケットをホスト A からホスト B に直接送信できます (図 12-1 を参照)。



IP サービス イメージが稼動している場合、スイッチはインターフェイス間でトラフィックを転送する方式として、ルーティングおよびフォールバック ブリッジングの 2 通りをサポートします。IP ベース イメージが稼動している場合は、基本ルーティング (スタティック ルーティングと RIP) だけがサポートされます。高いパフォーマンスを維持するため、可能な場合は常にスイッチ ハードウェアによって転送を行います。ただし、ハードウェア内をルーティングできるのは、イーサネット II カプセル化機能を備えた IP バージョン 4 パケットだけです。非 IP トラフィックと、他のカプセル化方式を使用しているトラフィックは、ハードウェアによってフォールバック ブリッジングできます。

- ルーティング機能は、すべての SVI およびルーテッド ポートでイネーブルにできます。スイッチは、IP トラフィックだけをルーティングします。IP ルーティング プロトコル パラメータとアドレス設定が SVI またはルーテッド ポートに追加されると、このポートで受信した IP トラフィックはルーティングされます。詳細については、第 38 章「IP ユニキャスト ルーティングの設定」、第 46 章「IP マルチキャスト ルーティングの設定」、または第 47 章「MSDP の設定」を参照してください。
- フォールバック ブリッジングを行うと、スイッチでルーティングされないトラフィックや、DECnet などのルーティングできないプロトコルに属するトラフィックが転送されます。また、フォールバック ブリッジングは、2 つ以上の SVI またはルーテッド ポート間のブリッジングによって、複数の VLAN を 1 つのブリッジ ドメインに接続します。フォールバック ブリッジングを設定する場合は、ブリッジ グループに SVI またはルーテッド ポートを割り当てます。各 SVI またはルーテッド ポートにはそれぞれ 1 つしかブリッジ グループが割り当てられません。同じグループ内のすべてのインターフェイスは、同じブリッジ ドメインに属します。詳細は、第 48 章「フォールバック ブリッジングの設定」を参照してください。

インターフェイス コンフィギュレーション モードの使用法

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート：スイッチ ポートおよびルーテッド ポート
- VLAN：スイッチ仮想インターフェイス
- ポート チャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます（「[インターフェイス範囲の設定](#)」(P.12-14) を参照）。

物理インターフェイス（ポート）を設定するには、インターフェイスのタイプ、スタック メンバー番号、モジュール番号、およびスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

- タイプ：スイッチでサポートされるポートに応じたポートの種類 使用できるタイプ：10/100 Mbps イーサネット対応のファスト イーサネット（fastethernet または fa）、10/100/1000 Mbps イーサネット ポート対応のギガビット イーサネット（gigabitethernet または gi）、10,000 Mbps 対応の 10 ギガビット イーサネット（tengigabitethernet または te）、または Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュール ギガビット イーサネット インターフェイス。
- スタック メンバー番号：スタック内のスイッチを識別するための番号。スイッチ番号は 1～9 の範囲で、スイッチの初回初期化時に割り当てられます。スイッチ スタックに統合される前までのデフォルトのスイッチ番号は 1 です。スイッチにスタック メンバー番号が割り当てられると、別の番号が割り当てられるまではその番号が保持されます。

スタック モードでのスイッチ ポート LED を使用して、スイッチ内のスタック メンバー番号を識別できます。

スタック メンバー番号の詳細については、「[メンバー番号](#)」(P.5-6) を参照してください。

- モジュール番号：スイッチのモジュール番号またはスロット番号（常に 0）。
- ポート番号：スイッチ上のインターフェイス番号。ポート番号は、fastethernet1/0/1 または gigabitethernet1/0/1 のように、必ず 1 から始まります。スイッチ前面に向かい左のポートから順に番号が付けられています。複数のインターフェイス タイプがある場合（10/100 ポートと SFP モジュール ポートなど）、ポート番号は 2 番目のインターフェイス タイプから再開され、gigabitethernet1/0/1 となります。

物理インターフェイスはスイッチを実際に見ることで特定できます。一方、特定のインターフェイスまたはすべてのインターフェイスに関する情報は、**show** 特権 EXEC コマンドを使用して見ることができます。以降、この章では、主に物理インターフェイスの設定手順について説明します。

次の例では、インターフェイスを識別しています。

- スタンドアロン スwitch に 10/100/1000 ポート 4 を設定するには、次のコマンドを入力します。

```
Switch(config)# interface gigabitethernet1/0/4
```

- スタック メンバー 3 に 10/100 ポート 4 を設定するには、次のコマンドを入力します。

```
Switch(config)# interface gigabitethernet3/0/4
```

- スタンドアロン スwitch に 10 ギガビット モジュール ポート 1 を設定するには、次のコマンドを入力します。

```
Switch(config)# interface tengigabitethernet1/0/1
```

- スタック メンバー 3 に 10 ギガビット モジュール ポートを設定するには、次のコマンドを入力します。

```
Switch(config)# interface tengigabitethernet3/0/1
```

スイッチに SFP モジュールがある場合、これらのポートは、スイッチ上の他のインターフェイスのタイプに応じ番号が付けられます。ポートタイプがファストイーサネットからギガビットイーサネット (SFP) に変更されると、ポート番号は新たに 1 から開始されます。ポートタイプがギガビットイーサネットのままの場合は、ポート番号は連続して付けられます。

- スタック メンバー 1 の 1 番目の SFP モジュール ポートに 24 の 10/100/1000 ポートを設定するには、次のコマンドを入力します。

```
Switch(config)# interface gigabitethernet1/0/25
```

- スタック メンバー 1 の 1 番目の SFP モジュール ポートに 24 の 10/100 ポートを設定するには、次のコマンドを入力します。

```
Switch(config)# interface gigabitethernet1/0/1
```

インターフェイスの設定手順

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

- ステップ 1** 特権 EXEC プロンプトに **configure terminal** コマンドを入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- ステップ 2** **interface** グローバル コンフィギュレーション コマンドを入力します。

インターフェイスのタイプ、スイッチ番号、およびインターフェイス番号を特定します。次の例では、スイッチ 1 上のギガビットイーサネット ポート 1 が選択されています。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)#
```



(注) インターフェイス タイプとインターフェイス番号の間のスペース入力は任意です。

- ステップ 3** 各 **interface** コマンドの後ろに、インターフェイスに必要なコンフィギュレーション コマンドを続けて入力します。入力するコマンドによって、そのインターフェイスで稼動するプロトコルとアプリケーションが定義されます。別のインターフェイス コマンドまたは **end** を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。

また、**interface range** または **interface range macro** グローバル コンフィギュレーション コマンドを使用すると、一定範囲のインターフェイスを設定することもできます。ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。

- ステップ 4** インターフェイスを設定してから、「[インターフェイスのモニタリングおよびメンテナンス](#)」(P.12-34) に示した **show** 特権 EXEC コマンドで、そのステータスを確認してください。

show interfaces 特権 EXEC コマンドを使用して、スイッチ上のまたはスイッチ用に設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイス範囲の設定

interface range グローバル コンフィギュレーション コマンドを使用して、同じコンフィギュレーション パラメータを持つ複数のインターフェイスを設定できます。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンド パラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

同じパラメータでインターフェイス範囲を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	<p>設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> • interface range コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。 • macro 変数については、「インターフェイス レンジ マクロの設定および使用方法」(P.12-15) を参照してください。 • カンマで区切った <i>port-range</i> では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。 • ハイフンで区切った <i>port-range</i> では、インターフェイス タイプの再入力は不要ですが、ハイフンの前後にスペースを入力する必要があります。
ステップ 3		この時点で、通常のコンフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces [<i>interface-id</i>]	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

interface range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- スイッチのポート タイプに応じて、*port-range* に有効なエントリは次のとおりです。
 - **vlan** *vlan-ID* : *vlan-ID*、VLAN ID は 1 ~ 4094
 - **fastethernet** stack member/module/{*first port*} : {*last port*}、module は常に 0
 - **gigabitethernet** stack member/module/{*first port*} : {*last port*}、module は常に 0
 - **port-channel** *port-channel-number* : *port-channel-number*、*port-channel-number* は 1 ~ 48



(注) ポート チャネルを指定して **interface range** コマンドを使用する場合は、先頭および最後のチャンネル番号をアクティブなポート チャネルにする必要があります。

- **interface range** コマンドを使用するときは、先頭のインターフェイス番号とハイフンの間にスペースが必要です。
たとえば、インターフェイス範囲 **gigabitethernet1/0/1 - 4** は有効な範囲ですが、インターフェイス範囲 **gigabitethernet1/0/1-4** は無効な範囲です。
- **0/1 - 4 0/1-4 interface range** コマンドが機能するのは、**interface vlan** コマンドで設定された VLAN インターフェイスに限られます。**show running-config** 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。**show running-config** コマンドで表示されない VLAN インターフェイスに **interface range** コマンドを使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ（すべてがファスト イーサネット ポート、すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN）でなければなりません。ただし、1 つのコマンド内で複数のレンジを組み合わせることができます。

次の例では、**interface range** グローバル コンフィギュレーション コマンドを使用して、ポート 1 ～ 2 の速度を 100 Mbps に設定します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 2
Switch(config-if-range)# speed 100
```

この例では、カンマを使用して別のインターフェイス タイプ スtring を追加し、スイッチ 1 上のファスト イーサネット ポート 1 ～ 3 と、スイッチ 2 上のギガビット イーサネット ポート 1 および 2 をイネーブルにし、フロー制御ポーズ フレームを受信できるようにします。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 3, gigabitethernet1/0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイス レンジ モードを終了したあとで、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジ モードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンドプロンプトが再表示されるのを待ってから、インターフェイス レンジ コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用方法

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバル コンフィギュレーション コマンドで **macro** キーワードを使用するには、まず **define interface-range** グローバル コンフィギュレーション コマンドでマクロを定義する必要があります。

インターフェイス レンジ マクロを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	define interface-range <i>macro_name</i> <i>interface-range</i>	インターフェイス レンジ マクロを定義して NVRAM (不揮発性 RAM) に保存します。 <ul style="list-style-type: none"> <i>macro_name</i> は、最大 32 文字の文字列です。 マクロには、カンマで区切ったインターフェイスを 5 つまで含めることができます。 それぞれの <i>interface-range</i> は、同じポート タイプで構成されていなければなりません。
ステップ 3	interface range macro <i>macro_name</i>	<i>macro_name</i> の名前でインターフェイス レンジ マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。 ここで、通常のコन्フィギュレーション コマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config include define	定義済みのインターフェイス レンジ マクロの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マクロを削除するには、**no define interface-range macro_name** グローバル コンフィギュレーション コマンドを使用します。

define interface-range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意してください。

- スイッチのポート タイプに応じて、*interface-range* に有効なエントリは次のとおりです。
 - vlan** *vlan-ID* : *vlan-ID*、VLAN ID は 1 ~ 4094
 - fastethernet** stack member/module/{*first port*} : {*last port*}、module は常に 0
 - gigabitethernet** stack member/module/{*first port*} : {*last port*}、module は常に 0
 - fastethernet** module/{*first port*} : {*last port*}、module は常に 0
 - gigabitethernet** module/{*first port*} : {*last port*}、module は常に 0
port-channel *port-channel-number* : *port-channel-number*、*port-channel-number* は 1 ~ 48



(注) ポート チャネルを指定して **interface range** コマンドを使用する場合は、先頭および最後のチャンネル番号をアクティブなポート チャネルにする必要があります。

- interface-range* を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。
たとえば、**gigabitethernet1/0/1 - 4** は有効な範囲ですが、**gigabitethernet1/0/1-4** は無効な範囲です。
- VLAN インターフェイスは、**interface vlan** コマンドで設定しておかなければなりません。**show running-config** 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。**show running-config** コマンドで表示されない VLAN インターフェイスを *interface-range* として使用することはできません。

- ある範囲内のすべてのインターフェイスは、同じタイプ（すべてがファストイーサネットポート、すべてがギガビットイーサネットポート、すべてが EtherChannel ポート、またはすべてが VLAN）でなければなりません。ただし、1つのマクロ内で複数のインターフェイスタイプを組み合わせたことができます。

次に、*enet_list* という名前のインターフェイスレンジマクロを定義してポート 1 および 2 を含め、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet1/0/1 - 2
```

次に、複数のタイプのインターフェイスを含むマクロ *macrol* を作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macrol gigabitethernet1/0/1 - 2,
gigabitethernet1/0/1 - 2
Switch(config)# end
```

次に、インターフェイスレンジマクロ *enet_list* に対するインターフェイスレンジコンフィギュレーションモードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイスレンジマクロ *enet_list* を削除し、処理を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

イーサネット インターフェイスの設定

ここでは、次の設定情報について説明します。

- 「イーサネット インターフェイスのデフォルト設定」 (P.12-18)
- 「10 ギガビットイーサネット インターフェイスの設定時の注意事項」 (P.12-19)
- 「インターフェイス速度およびデュプレックスモードの設定」 (P.12-19)
- 「IEEE 802.3X フロー制御の設定」 (P.12-22)
- 「インターフェイスでの Auto-MDIX の設定」 (P.12-23)
- 「PoE ポートの電力管理モードの設定」 (P.12-24)
- 「PoE ポートに接続された受電装置のパワー バジェット」 (P.12-25)
- 「インターフェイスに関する記述の追加」 (P.12-27)

イーサネット インターフェイスのデフォルト設定

表 12-2 にイーサネット インターフェイスのデフォルト設定を示します。表に示されている VLAN パラメータの詳細については、第 14 章「VLAN の設定」を参照してください。また、ポートへのトラフィック制御の詳細については、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。



(注)

インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

表 12-2 レイヤ 2 イーサネット インターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ 2 またはスイッチング モード (switchport コマンド)
VLAN 許容範囲	VLAN 1 ~ 4094
デフォルト VLAN (アクセスポート用)	VLAN 1 (レイヤ 2 インターフェイスだけ)
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1 (レイヤ 2 インターフェイスだけ)
VLAN トランキング	Switchport mode dynamic auto (DTP をサポート) (レイヤ 2 インターフェイスだけ)
ポート イネーブル ステート	すべてのポートがイネーブル
ポート記述	未定義
速度	自動ネゴシエーション (10 ギガビット インターネット上では未サポート)
デュプレックス モード	自動ネゴシエーション (10 ギガビット インターネット上では未サポート)
フロー制御	フロー制御は receive: off に設定されます。送信パケットでは常にオフです。
EtherChannel (PAgP)	すべてのイーサネット ポートでディセーブル。第 37 章「EtherChannel およびリンクステート トラッキングの設定」
ポート ブロッキング (不明マルチキャストおよび不明ユニキャストトラフィック)	ディセーブル (ブロッキングされない) (レイヤ 2 インターフェイスだけ)。「ポート ブロッキングの設定」(P.26-7) を参照してください。
ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御	ディセーブル。「ストーム制御のデフォルト設定」(P.26-3) を参照してください。
保護ポート	ディセーブル (レイヤ 2 インターフェイスだけ)。「保護ポートの設定」(P.26-6) を参照してください。
ポート セキュリティ	ディセーブル (レイヤ 2 インターフェイスだけ)。「ポート セキュリティのデフォルト設定」(P.26-11) を参照してください。

表 12-2 レイヤ 2 イーサネット インターフェイスのデフォルト設定 (続き)

機能	デフォルト設定
PortFast	ディセーブル。「オプションのスパニング ツリー機能のデフォルト設定」(P.21-12) を参照してください。
Auto-MDIX	イネーブル (注) 受電装置がクロス ケーブルでスイッチに接続されている場合、スイッチは、IEEE 802.3af に完全には準拠していない、Cisco IP Phone やアクセス ポイントなどの準規格の受電をサポートしていない場合があります。これは、スイッチ ポート上で Automatic Medium-Dependent Interface Crossover (Auto-MIDX) がイネーブルかどうかは関係ありません。
PoE	イネーブル (auto)
キープアライブ メッセージ	SFP モジュールでディセーブル。他のすべてのポートでイネーブル。

10 ギガビット イーサネット インターフェイスの設定時の注意事項

設定上の問題を防ぐため、次の注意事項に従ってください。

- 速度およびデュプレックス機能はサポートされていません。
- 10 ギガビット インターフェイスは次の Quality of Service (QoS) 機能をサポートしません。
 - ポリシング
 - Cisco IP Phone を使用した VoIP における自動 QoS
 - Shaped Round Robin (SRR) のウェイトを使用した出力キューの提供
 - 出力インターフェイスの帯域幅の制限
- 10 ギガビット モジュール ポートが Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) または Remote SPAN (RSPAN) 宛先ポートとして設定されている場合、リンク速度が低下します。
- クロススタック EtherChannel では最大 2 つの 10 ギガビット モジュール ポートをサポートしています。

インターフェイス速度およびデュプレックス モードの設定

サポートされるポート タイプに応じて、スイッチのイーサネット インターフェイスは、全二重または半二重モードのいずれかで、10、100、1000 Mbps、または 10,000 Mbps で動作します。全二重モードの場合、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。これは、各ステーションがトラフィックを受信するか、送信するかのどちらか一方しかできないことを意味します。

スイッチ モデルには、ファストイーサネット (10/100 Mbps) ポート、ギガビットイーサネット (10/100/1000 Mbps) ポート、10 ギガビット モジュール ポートと、SFP モジュールをサポートする着脱可能小型フォームファクタ (SFP) モジュール スロットの組み合わせが含まれます。

ここでは、インターフェイス速度とデュプレックス モードの設定手順について説明します。

- 「速度とデュプレックス モードの設定時の注意事項」 (P.12-20)
- 「インターフェイス速度およびデュプレックス パラメータの設定」 (P.12-21)

速度とデュプレックス モードの設定時の注意事項

インターフェイス速度およびデュプレックス モードを設定するときには、次の注意事項に留意してください。

- ファストイーサネット (10/100 Mbps) ポートは、すべての速度およびデュプレックス オプションをサポートします。
- ギガビットイーサネット (10/100/1000 Mbps) ポートは、すべての速度オプションとデュプレックス オプション (自動、半二重、全二重) をサポートします。ただし、1000 Mbps で稼働させているギガビットイーサネット ポートは、半二重モードをサポートしません。
10 ギガビット モジュール ポートでは、速度またはデュプレックス モードの設定はできません。これらのポートは 10,000 Mbps および全二重モードだけで動作します。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI (コマンドラインインターフェイス) オプションが変わります。
 - 1000 BASE-x (x には、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポートは、**speed** インターフェイス コンフィギュレーション コマンドで **nonegotiate** キーワードをサポートします。デュプレックス オプションはサポートされません。
 - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックス オプションをサポートします。
 - 100BASE-x (x には、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポートは、100 Mbps だけサポートします。これらのモジュールは、全二重および半二重オプションをサポートしますが、自動ネゴシエーションをサポートしません。
 スイッチでサポートされる SFP モジュールについては、各製品のリリース ノートを参照してください。
- 回線の両側で自動ネゴシエーションがサポートされる場合は、できるだけデフォルトの **auto** ネゴシエーションを使用してください。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、スイッチがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。



注意

インターフェイス速度とデュプレックス モードの設定を変更すると、再設定時にシャットダウンが発生し、インターフェイスが再びイネーブルになることがあります。

インターフェイス速度およびデュプレックス パラメータの設定

物理インターフェイスの速度およびデュプレックス モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>speed {10 100 1000 auto [10 100 1000] nonegotiate}</code>	<p>このコマンドは 10 ギガビット イーサネット インターフェイスでは使用できません。</p> <p>インターフェイスに対する適切な速度パラメータを入力します。</p> <ul style="list-style-type: none"> インターフェイスの速度を指定するには、10、100、または 1000 を入力します。1000 キーワードを使用できるのは、10/100/1000 Mbps ポートに対してだけです。 インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、auto を入力します。auto キーワードと一緒に 10、100、または 1000 キーワードを使用した場合、ポートは指定の速度でだけ自動ネゴシエートします。 nonegotiate キーワードを使用できるのは、SFP モジュールポートに対してだけです。SFP モジュールポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように設定できます。 <p>速度の設定の詳細については、「速度とデュプレックス モードの設定時の注意事項」(P.12-20) を参照してください。</p>
ステップ 4	<code>duplex {auto full half}</code>	<p>このコマンドは 10 ギガビット イーサネット インターフェイスでは使用できません。</p> <p>インターフェイスのデュプレックス パラメータを入力します。</p> <p>半二重モードをイネーブルにします (10 または 100Mbps だけで動作するインターフェイスの場合)。1000 Mbps で動作するインターフェイスには半二重モードを設定できません。</p> <p>デュプレックスの設定の詳細については、「デュプレックスの設定の詳細については、「速度とデュプレックス モードの設定時の注意事項」」(P.12-20) を参照してください。</p>
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id</code>	インターフェイス速度およびデュプレックス モード設定を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの速度およびデュプレックス設定 (自動ネゴシエーション) に戻すには、**no speed** および **no duplex** インターフェイス コンフィギュレーション コマンドを使用します。すべてのインターフェイス設定をデフォルトに戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、10/100Mbps ポートでインターフェイスの速度を 10 Mbps に、デュプレックス モードを半二重に設定する例を示します。

```
Switch# configure terminal
```

```
Switch(config)# interface fasttetheretnet1/0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitetheretnet1/0/2
Switch(config-if)# speed 100
```

IEEE 802.3X フロー制御の設定

フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズフレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。



(注)

スイッチ上のポートは、ポーズフレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスのポーズフレームを受信 (**receive**) する能力を **on**、**off**、または **desired** に設定します。デフォルトの状態は **off** です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイス、または必要ではないがフロー制御パケットを送信できる接続デバイスに対して動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on** (または **desired**) : ポートはポーズフレームを送信できませんが、ポーズフレームを送信する必要がある、または送信できる接続デバイスと組み合わせて使用できます。ポーズフレームの受信は可能です。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側のデバイスもポーズフレームの送受信を行いません。



(注)

コマンドの設定と、その結果生じるローカルおよびリモート ポートでのフロー制御解決の詳細については、このリリースのコマンド リファレンスに記載された **flowcontrol** インターフェイス コンフィギュレーション コマンドを参照してください。

インターフェイス上でフロー制御を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	flowcontrol {receive} {on off desired}	ポートのフロー制御モードを設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id	インターフェイス フロー制御の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フロー制御をディセーブルにする場合は、**flowcontrol receive off** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のフロー制御をオンにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```

インターフェイスでの Auto-MDIX の設定

インターフェイス上の Auto-MDIX がイネーブルに設定されている場合、インターフェイスが必要なケーブル接続タイプ（ストレートまたはクロス）を自動的に検出し、接続を適切に設定します。

Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータなどのデバイスの接続にはストレート ケーブルを使用し、他のスイッチやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、『Hardware Installation Guide』を参照してください。

Auto-MDIX はデフォルトでイネーブルです。Auto-MDIX をイネーブルに設定する場合、Auto-MDIX 機能が正しく動作するようにインターフェイスの速度およびデュプレックスを **auto** に設定する必要があります。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mb/s インターフェイスでサポートされます。Auto-MDIX は、10/100/1000BASE-TX 着脱可能小型フォーム ファクタ（SFP）モジュール インターフェイスでサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされていません。

表 12-3 に、Auto-MDIX の設定および正しいケーブル接続と正しくないケーブル接続の結果として発生するリンク ステータスを示します。

表 12-3 リンク状態と Auto-MDIX の設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい場合	ケーブル接続が正しくない場合
オン	オン	リンク アップ	リンク アップ
オン	オフ	リンク アップ	リンク アップ
オフ	オン	リンク アップ	リンク アップ
オフ	オフ	リンク アップ	リンク ダウン

インターフェイス上で Auto-MDIX を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 speed auto	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 4 duplex auto	接続されたデバイスとデュプレックス モードの自動ネゴシエーションを行うようにインターフェイスを設定します。

	コマンド	目的
ステップ 5	mdix auto	インターフェイス上で Auto-MDIX をイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show controllers ethernet-controller interface-id phy	インターフェイスで Auto-MDIX の動作ステータスを確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Auto-MDIX をディセーブルにするには、**no mdix auto** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上の Auto-MDIX をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

PoE ポートの電力管理モードの設定

通常デフォルト設定（自動モード）での動作は適切に行われ、プラグアンドプレイ動作が提供されます。それ以上の設定は必要ありません。ただし、PoE ポートの優先順位を上げたり、PoE ポートをデータ専用にしたり、最大ワット数を指定して高電力受電装置をポートで禁止したりする場合は、次の手順を実行します。



(注)

PoE 設定を変更するとき、設定中のポートでは電力が低下します。新しい設定、その他の PoE ポートの状態、パワー バジレットの状態により、そのポートの電力は再びアップしない場合があります。たとえばポート 1 が自動でオンの状態になっており、そのポートを固定モードに設定するとします。スイッチはポート 1 から電力を排除し、受電装置を検出してポートに電力を再び供給します。ポート 1 が自動でオンの状態になっており、最大ワット数を 10 W に設定した場合、スイッチはポートから電力を排除し、受電装置を再び検出します。受電装置がクラス 1、クラス 2、シスコ専用受電装置のうちいずれかである場合、スイッチはポートに電力を再び供給します。

電力管理モードを PoE 対応ポートで設定するには、特権 EXEC モードで次の手順を実行します。

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

コマンド	目的
ステップ 3 <code>power inline {auto [max max-wattage] never static [max max-wattage]}</code>	<p>ポートに PoE モードを設定します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • auto : 受電装置検出をイネーブルにします。十分な電力が使用可能である場合、デバイスの検出後、PoE ポートに電力が自動的に割り当てられます。これがデフォルトの設定です。 • (任意) max max-wattage : ポートで許可する電力を制限します。指定できる範囲は 4000 ~ 15400 ミリワットです。値を指定しない場合は、最大値が許可されます (15400 ミリワット)。 • never : デバイス検出およびポートの電力をディセーブルにします。 <p>(注) シスコ受電装置がポートに接続されている場合は、ポートの設定に power inline never コマンドを使用しないでください。問題のあるリンクアップが発生し、ポートが errdisable ステータスになることがあります。</p> <ul style="list-style-type: none"> • static : 受電装置検出をイネーブルにします。スイッチが受電装置を検出する前に、電力がポートにあらかじめ割り当てられます (予約されます)。スイッチは、デバイスが接続されていなくてもこのポートに電力を予約し、デバイスの検出時に電力が供給されることを保証します。 <p>スイッチは、固定モードに設定されているポートに電力を割り当ててから、自動モードに設定されているポートに電力を割り当てます。</p>
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show power inline [interface-id module switch-number]</code>	指定したインターフェイスまたは指定したスタック メンバーのスイッチまたはスイッチ スタックの PoE ステータスを表示します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

show power inline ユーザ EXEC コマンドの出力については、このリリースのコマンド リファレンスを参照してください。PoE 関連コマンドの詳細については、「[PoE スイッチ ポートのトラブルシューティング](#)」(P.49-13) を参照してください。音声 VLAN の設定の詳細については、[第 16 章「音声 VLAN の設定](#)」を参照してください。

PoE ポートに接続された受電装置のパワー バジェット

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol (CDP) を使用して、デバイスの実際の電力消費を判断し、パワー バジェットをそれに合わせて調整します。CDP プロトコルは Cisco 製のデバイスで機能します。IEEE のサードパーティ デバイスでは機能しません。これらのデバイスでは、スイッチは電力要件を許可すると、受電装置の IEEE 分類に従って、パワー バジェットを調整します。受電装置が Class 0 (クラス ステータスは不明) または Class 3 である場合、実際に必要な電力量に関係なく、スイッチはポート用に 15,400 ミリワットの電力を確保します。受電装置が実際の消費よりも高いクラスをレポートしたり、または電力分類 (デフォルトはクラス 0) をサポートしていない場合、スイッチは IEEE クラス情報を使用してグローバル パワー バジェットをトラッキングするため、電力供給できるデバイスが少なくなります。

power inline consumption wattage コンフィギュレーション コマンドを使用すれば、IEEE 分類で指定されたデフォルトの電力要件を上書きできます。IEEE 分類により命令された電力とデバイスが実際に必要な電力の差は、その他のデバイスで使用するために、グローバル パワー バジェットに戻されます。これにより、スイッチのパワー バジェットが拡大され、より効果的に使用できるようになります。

たとえば、スイッチが PoE ポートごとに 15,400 ミリワットを計上する場合、接続できるクラス 0 の受電装置は 24 デバイスだけです。クラス 0 デバイスの実際の電力要件が 5000 ミリワットの場合、消費ワットを 5000 ミリワットに設定し、最大 48 デバイスまで接続できます。24 ポートまたは 48 ポートのスイッチで利用可能な PoE 出力電力の合計は、370,000 ミリワットです。



注意

スイッチのパワー バジェットは慎重に計画し、電力供給をオーバーサブスクライブしないようにする必要があります。



(注)

パワー バジェットを手動で設定する場合は、スイッチと受電装置間のケーブルでの電力損失も考慮する必要があります。

power inline consumption default wattage または **no power inline consumption default** グローバル コンフィギュレーション コマンドを入力した場合、もしくは **power inline consumption wattage** または **no power inline consumption** インターフェイス コンフィギュレーション コマンドを入力した場合は、次の注意メッセージが表示されます。

```
%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty.Take precaution not to
oversubscribe the power supply.
Refer to documentation.
```

電源装置の電力が 20% 近くまで使用されている場合、スイッチは動作しますが信頼性が損なわれます。電源装置の電力が 20% を超えて使用されている場合、ショート保護回路が呼び出され、スイッチがシャットダウンします。

IEEE 電力分類の詳細については、「[Power over Ethernet \(PoE\) ポート](#)」(P.12-8) を参照してください。

スイッチの各 PoE ポートに接続された受電装置へのパワー バジェット量を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	(任意) CDP をディセーブルにします。
ステップ 3	power inline consumption default wattage	スイッチの各 PoE ポートに接続された受電装置の電力消費を設定します。各デバイスで指定できる範囲は 4000 ~ 15400 ミリワットです。デフォルト値は 15400 ミリワットです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show power inline consumption	電力消費ステータスを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトに戻すには、**no power inline consumption default** グローバル コンフィギュレーション コマンドを使用します。

特定の PoE ポートに接続された受電装置へのパワー バジェット量を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	(任意) CDP をディセーブルにします。
ステップ 3	interface interface-id	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	power inline consumption wattage	スイッチの PoE ポートに接続された受電装置の電力消費を設定します。各デバイスで指定できる範囲は 4000 ~ 15400 ミリワットです。デフォルト値は 15400 ミリワットです。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show power inline consumption	電力消費ステータスを表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトに戻すには、**no power inline consumption** インターフェイス コンフィギュレーション コマンドを使用します。

show power inline consumption 特権 EXEC コマンドの出力の詳細については、このリリースのコマンド リファレンスを参照してください。

インターフェイスに関する記述の追加

インターフェイスの機能に関する記述を追加できます。記述は、特権 EXEC コマンド **show configuration**、**show running-config**、および **show interfaces** の出力に表示されます。

インターフェイスに関する記述を追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	記述を追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに関する記述を追加します (最大 240 文字)。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id description または show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

記述を削除するには、**no description** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに記述を追加して、その記述を確認する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status      Protocol Description
Gi1/0/2    admin down    down    Connects to Marketing
```

レイヤ 3 インターフェイスの設定

スイッチは、次に示す 3 種類のレイヤ 3 インターフェイスをサポートします。

- トラフィックをルーティングする VLAN に対応する SVI を設定する必要があります。SVI は、**interface vlan** グローバル コンフィギュレーション コマンドのあとに VLAN ID を入力して作成します。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス VLAN 1 は削除できません。



(注) 作成した SVI をアクティブにするには、物理ポートに関連付ける必要があります。VLAN へのレイヤ 2 ポートの割り当てについては、第 14 章「VLAN の設定」を参照してください。

SVI 作成時、SVI のポートに SVI Autostate Exclude を設定し、SVI ライン ステート ステータスの計算から除外することもできます。「SVI Autostate Exclude の設定」(P.12-29) を参照してください。

- ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。
- レイヤ 3 EtherChannel ポート: ルーテッド ポートで構成された EtherChannel インターフェイスです。

EtherChannel ポートについては、第 37 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

レイヤ 3 スイッチでは、ルーテッド ポートおよび SVI ごとに IP アドレスを 1 つ割り当てることができません。

スイッチ スタックに設定可能な SVI とルーテッド ポートの数について定義済みの制限はありません。ただし、ハードウェアには限界があるため、SVI およびルーテッド ポートの個数と、設定されている他の機能の個数の組み合わせによっては、CPU 利用率が影響を受けることがあります。スイッチが最大限のハードウェア リソースを使用している場合にルーテッド ポートまたは SVI を作成しようとする、次のような結果になります。

- 新たなルーテッド ポートを作成しようとする、スイッチはインターフェイスをルーテッド ポートに変換するための十分なリソースがないことを示すメッセージを表示し、インターフェイスはスイッチポートのままとなります。
- 拡張範囲の VLAN を作成しようとする、エラー メッセージが生成され、拡張範囲の VLAN は拒否されます。
- VTP が新たな VLAN をスイッチへ通知すると、スイッチは使用可能な十分なハードウェア リソースがないことを示すメッセージを送り、その VLAN をシャットダウンします。**show vlan** ユーザ EXEC コマンドの出力に、サスペンド ステートの VLAN が示されます。
- スイッチが、ハードウェアのサポート可能な数を超える VLAN とルーテッド ポートが設定されたコンフィギュレーションを使って起動を試みると、VLAN は作成されますが、ルーテッド ポートはシャットダウンされ、スイッチはハードウェア リソースが不十分であるという理由を示すメッセージを送信します。

すべてのレイヤ 3 インターフェイスには、トラフィックをルーティングするための IP アドレスが必要です。次の手順は、レイヤ 3 インターフェイスとしてインターフェイスを設定する方法およびインターフェイスに IP アドレスを割り当てる方法を示します。



(注)

物理ポートがレイヤ 2 モードである (デフォルト) 場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを実行してインターフェイスをレイヤ 3 モードにする必要があります。**no switchport** コマンドを実行すると、インターフェイスがディセーブルになってから再度イネーブルになります。これにより、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。さらに、レイヤ 2 モードのインターフェイスをレイヤ 3 モードにすると、影響を受けたインターフェイスに関連する前の設定情報は失われ、インターフェイスはデフォルト設定に戻る可能性があります。

レイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface {{fastethernet gigabitethernet} interface-id} {vlan vlan-id} {port-channel port-channel-number}	レイヤ 3 インターフェイスとして設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 4	ip address ip_address subnet_mask	IP アドレスおよび IP サブネットを設定します。
ステップ 5	no shutdown	インターフェイスをイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [interface-id] show ip interface [interface-id] show running-config interface [interface-id]	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスの IP アドレスを削除するには、**no ip address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをルーテッドポートとして設定し、IP アドレスを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

SVI Autostate Exclude の設定

SVI のアクセスまたはトランク ポートに SVI Autostate Exclude を設定すると、同じ VLAN に属していた場合でも、SVI ステータスの計算 (アップまたはダウン ライン ステート) からポートを除外できます。除外されたポートがアップステートで、VLAN の他のすべてのポートがダウンステートである場合、SVI ステートがダウンに変わります。

SVI ライン ステート アップを保持するには、VLAN で少なくとも 1 つのポートがアップで除外されていない必要があります。このコマンドを使用すると、SVI ステータス判断時に、モニタリングしているポート ステータスを除外できます。

SVI ステート変更計算からポートを除外するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	レイヤ 2 インターフェイス（物理ポートまたはポートチャネル）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport autostate exclude</code>	SVI ライン ステートのステータス判断時（アップまたはダウン）にアクセスまたはトランク ポートを除外します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running config interface interface-id</code> <code>show interface interface-id switchport</code>	(任意) 実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、SVI のアクセスまたはトランク ポートを設定して、ステータス計算から除外する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```

システム MTU の設定

すべてのインターフェイスで送受信されるフレームのデフォルト Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズは、1500 バイトです。10 または 100 Mbps で動作するすべてのインターフェイスで MTU サイズを増やすには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。また、**system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、すべてのギガビットイーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。

system mtu routing グローバル コンフィギュレーション コマンドを使用すると、ルーテッド ポートの MTU サイズを変更できます。



(注)

システムの MTU サイズを超えるルーティング MTU サイズは設定できません。システムの MTU サイズを現在設定されているルーティング MTU サイズより小さい値に変更する場合、設定変更は許可されますが、次にスイッチがリセットされるまで適用されません。設定変更が有効になると、ルーティング MTU サイズは自動的にデフォルトの新しいシステム MTU サイズになります。

system mtu コマンドはギガビットイーサネット ポートには影響せず、**system mtu jumbo** コマンドは 10/100 ポートには影響しません。**system mtu jumbo** コマンドを設定していない場合、**system mtu** コマンドの設定はすべてのギガビットイーサネット インターフェイスに適用されます。

個々のインターフェイスに MTU サイズを設定することはできません。すべての 10/100 インターフェイスまたはすべてのギガビットイーサネットインターフェイスに対して設定されます。システムまたはジャンボ MTU サイズを変更する場合、新規設定を有効にするにはスイッチをリセットする必要があります。system mtu routing コマンドは、スイッチをリセットしなくても有効になります。

スイッチの CPU が受信できるフレームサイズは、system mtu または system mtu jumbo コマンドで入力した値に関係なく、1998 バイトに制限されています。通常、転送またはルーティングされたフレームは CPU によって受信されませんが、場合によっては、制御トラフィック、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)、Telnet、またはルーティングプロトコルへ送信されたトラフィックなどのパケットが CPU へ送信されることがあります。

ルーテッドパケットは、出力ポートで MTU チェックの対象となります。ルーテッドポートで使われる MTU 値は (system mtu jumbo 値ではなく) 適用された system mtu 値から抽出されます。つまり、ルーテッド MTU はどの VLAN のシステム MTU よりも大きくなりません。ルーティングプロトコルは、隣接関係とリンクの MTU をネゴシエーションする場合にシステム MTU 値を使用します。たとえば、Open Shortest Path First (OSPF) プロトコルは、ピア ルータとの隣接関係を設定する前にこの MTU 値を使用します。特定の VLAN のルーテッドパケットの MTU 値を表示するには、show platform port-asic mvid 特権 EXEC コマンドを使用します。



(注) レイヤ 2 ギガビットイーサネットインターフェイスが、10/100 インターフェイスより大きいサイズのフレームを受け取るように設定されている場合、レイヤ 2 ギガビットイーサネットインターフェイスに着信するジャンボフレームとレイヤ 2 10/100 インターフェイスで発信されるジャンボフレームは廃棄されます。

すべての 10/100 またはギガビットイーサネットインターフェイスで MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	system mtu bytes	(任意) 10 または 100 Mbps で稼動するスイッチ スタックのすべてのインターフェイスに対して MTU サイズを変更します。 指定できる範囲は 1500 ~ 1998 バイトです。デフォルトは 1500 バイトです。
ステップ 3	system mtu jumbo bytes	(任意) スイッチ スタックのすべてのギガビットイーサネットインターフェイスに対して MTU サイズを変更します。 指定できる範囲は 1500 ~ 9000 バイトです。デフォルトは 1500 バイトです。
ステップ 4	system mtu routing bytes	(任意) ルーテッドポートのシステム MTU を変更します。指定できる範囲は 1500 ~ システム MTU 値で、すべてのポートにルーティング可能な最大 MTU 値です。 これより大きなパケットは受け入れられますが、ルーティングされません。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	reload	OS (オペレーティングシステム) をリロードします。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

スイッチのリロード後、**show system mtu** 特権 EXEC コマンドを入力することによって、設定値を確認できます。

次に、ギガビット イーサネット ポートの最大パケット サイズを 1800 バイトに設定する例を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

次に、ギガビット イーサネット インターフェイスを範囲外の値に設定しようとした場合に表示される応答の例を示します。

```
Switch(config)# system mtu jumbo 25000
                          ^
% Invalid input detected at '^' marker.
```

Cisco 冗長電源システム (RPM) 2300 の設定

次の注意事項に従ってください。

- Redundant Power System (RPM; 冗長電源システム) 名は、最大 16 文字の文字列です。
- スタンドアロン Catalyst 3750v2 スイッチでは、RPS 名は接続された RPS 2300 に適用されます。
- スイッチ スタックでは、RPS 名は指定されたスイッチに接続された RPS ポートに適用されます。
- RPS 2300 からスイッチに電力を提供したくない場合に、スイッチと RPS 2300 の間のケーブルの接続を解除しないときは、**power rps switch-number port rps-port-id mode standby** ユーザ EXEC コマンドを使用します。
- 1 ~ 6 の RPS 2300 ポートのプライオリティを設定できます。値 1 は最高のプライオリティをポートおよびそれに接続されたデバイスに割り当てます。値 6 は最小のプライオリティをポートおよびそれに接続されたデバイスに割り当てます。

RPS 2300 に接続された複数のスイッチが電力を必要とする場合、RPS 2300 は最高のプライオリティでそれらに電力を供給します。よりプライオリティが低いスイッチには、その他の利用可能な電力を適用します。

ユーザ EXEC モードで実行します。

	コマンド	目的
ステップ 1	power rps <i>switch-number</i> name { <i>string</i> <i>serialnumber</i> }	<p>RPS 2300 の名前を指定します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • switch-number : RPS 2300 が接続されるスタック メンバーを指定します。指定できる範囲は 1 ~ 9 です (スタックのスイッチ メンバー番号に対応)。このキーワードは Catalyst 3750v2 スイッチだけでサポートされます。 • name : RPS 2300 の名前を設定し、次のオプションのうちの 1 つを入力します。 <ul style="list-style-type: none"> – string : 「<i>port1</i>」や「"<i>port 1</i>"」などの名前を指定します。名前の前後での引用符の使用は任意ですが、ポート名に空白を含める場合は引用符を使用する必要があります。名前は最大 16 文字です。 – serialnumber : RPS 2300 シリアル番号を名前として使用するようにスイッチを設定します。
ステップ 2	power rps <i>switch-number</i> port <i>rps-port-id</i> mode { active standby }	<p>RPS 2300 ポートのモードを指定します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • switch-number : RPS 2300 に接続されるスタック メンバーを指定します。指定できる範囲は 1 ~ 9 です (スタックのスイッチ メンバー番号に対応)。このキーワードは Catalyst 3750v2 スイッチだけでサポートされます。 • port <i>rps-port-id</i> : RPS 2300 ポートを指定します。有効な範囲は 1 ~ 6 です。 • mode : RPS 2300 ポートのモードを設定します。 <ul style="list-style-type: none"> – active : RPS 2300 は、スイッチ内部電源モジュールが供給できないときにスイッチに電力を供給します。 – standby : RPS 2300 はスイッチに電力を供給しません。 <p>RPS ポートのデフォルトモードは active です。</p>
ステップ 3	power rps <i>switch-number</i> priority <i>priority</i>	<p>RPS 2300 ポートのプライオリティを設定します。有効範囲は 1 ~ 6 です。1 は最高のプライオリティを、6 は最小のプライオリティを示します。</p> <p>デフォルトのポート プライオリティは 6 です。</p>
ステップ 4	show env rps	設定値を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの名前設定（設定された名前がない）に戻すには、**power rps switch-number port rps-port-id name** ユーザ EXEC コマンドを引用符の間にスペースを入れずに使用します。

デフォルトのポート モードに戻すには、**power rps switch-number port rps-port-id active** コマンドを使用します。

デフォルトのポート プライオリティに戻すには、**power rps switch-number port rps-port-id priority** コマンドを使用します。

power rps ユーザ EXEC コマンドの使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

インターフェイスのモニタリングおよびメンテナンス

ここでは、インターフェイスのモニタおよびメンテナンスについて説明します。

- 「インターフェイス ステータスのモニタ」(P.12-34)
- 「インターフェイスおよびカウンタのクリアとリセット」(P.12-35)
- 「インターフェイスのシャットダウンおよび再起動」(P.12-36)

インターフェイス ステータスのモニタ

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を表示できます。表 12-4 に、このようなインターフェイス モニタ コマンドの一部を示します（特権 EXEC プロンプトに **show ?** コマンドを入力すると、すべての **show** コマンド のリストが表示されます）。これらのコマンドについては、『Cisco IOS Interface Command Reference』Release 12.2 で詳しく説明しています。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

表 12-4 インターフェイス用の show コマンド

コマンド	目的
show interfaces [<i>interface-id</i>]	(任意) すべてのインターフェイスまたは特定のインターフェイスのステータスおよび設定を表示します。
show interfaces <i>interface-id</i> status [err-disabled]	(任意) インターフェイスのステータス、または errdisable ステートにあるインターフェイスのリストを表示します。
show interfaces [<i>interface-id</i>] switchport	(任意) スイッチング ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [<i>interface-id</i>] description	(任意) 1 つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
show ip interface [<i>interface-id</i>]	(任意) IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [<i>interface-id</i>] stats	(任意) インターフェイスのパスごとに入出力パケットを表示します。
show interfaces tengigabitethernet <i>interface-id</i> detail	(任意) 接続した 10 ギガビット モジュールのステータス（温度およびアラーム ステータスなど）を表示します。

表 12-4 インターフェイス用の show コマンド (続き)

コマンド	目的
<code>show interfaces tengigabitethernet interface-id properties detail</code>	(任意) 接続した 10 ギガビット モジュールの速度とデュプレックス設定を表示します。
<code>show interfaces transceiver properties</code>	(任意) インターフェイスの速度、デュプレックス、およびインライン電力設定を表示します。
<code>show interfaces transceiver detail</code>	(任意) インターフェイスの温度、電圧、電流量を表示します。
<code>show interfaces [interface-id] [{transceiver properties detail}] module number</code>	SFP モジュールに関する物理および動作ステータスを表示します。
<code>show running-config interface [interface-id]</code>	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
<code>show version</code>	ハードウェア構成、ソフトウェアのバージョン、コンフィギュレーションファイルの名前とソース、ブート イメージを表示します。
<code>show controllers ethernet-controller interface-id phy</code>	インターフェイスの Auto-MDIX 動作ステータスを表示します。
<code>show power inline [interface-id module switch-number]</code>	スイッチまたはスイッチ スタック、インターフェイス、またはスタック内の特定のスイッチの PoE ステータスを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 12-5 に、カウンタのクリアとインターフェイスのリセットに使用できる特権 EXEC モードの `clear` コマンドを示します。

表 12-5 インターフェイス用の clear コマンド

コマンド	目的
<code>clear counters [interface-id]</code>	インターフェイスのカウンタをクリアします。
<code>clear interface interface-id</code>	インターフェイスのハードウェア ロジックをリセットします。
<code>clear line [number console 0 vty number]</code>	非同期シリアル回線に関するハードウェア ロジックをリセットします。

`show interfaces` 特権 EXEC コマンドによって表示されたインターフェイス カウンタをリセットするには、`clear counters` 特権 EXEC コマンドを使用します。オプションの引数が特定のインターフェイス番号から特定のインターフェイス タイプだけをクリアするように指定する場合を除いて、`clear counters` コマンドは、インターフェイスから現在のインターフェイス カウンタをすべてクリアします。



(注) `clear counters` 特権 EXEC コマンドは、SNMP を使用して取得されたカウンタをクリアしません。`show interface` 特権 EXEC コマンドで表示されるカウンタだけをクリアします。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブルになり、使用不可能であることがすべての `show` コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

インターフェイスをシャットダウンするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface {vlan <i>vlan-id</i>} {{fastethernet gigabitethernet} <i>interface-id</i>} {port-channel <i>port-channel-number</i>}</code>	設定するインターフェイスを選択します。
ステップ 3	<code>shutdown</code>	インターフェイスをシャットダウンします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。

インターフェイスを再起動するには、`no shutdown` インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスがディセーブルになっていることを確認するには、`show interfaces` 特権 EXEC コマンドを使用します。ディセーブルになっているインターフェイスは、出力に *administratively down* と表示されます。



CHAPTER 13

Auto Smartport マクロの設定

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

Catalyst 3750 スイッチ コマンド リファレンスには、コマンドの構文と使用方法が記載されています。

- 「[Auto Smartport マクロおよびスタティック Smartports マクロの概要](#)」 (P.13-1)
- 「[Auto Smartport の設定](#)」 (P.13-3)
- 「[スタティック Smartport マクロの設定](#)」 (P.13-17)
- 「[Auto Smartport マクロおよびスタティック Smartport マクロの表示](#)」 (P.13-20)

Auto Smartport マクロおよびスタティック Smartports マクロの概要

Auto Smartport マクロは、ポートで検出されたデバイス タイプに基づいてポートを動的に設定します。スイッチはポート上で新しいデバイスを検出すると、ポートに適切な Auto Smartport マクロを適用します。ポートでリンクダウン イベントが発生すると、スイッチによってマクロは削除されます。たとえば、Cisco IP Phone をポートに接続すると、Auto Smartport は IP Phone マクロを自動的に適用します。IP Phone マクロを使用すると、QoS (Quality of Service)、セキュリティ機能、および専用の音声 VLAN で遅延に影響されやすい音声トラフィックを適切に処理できます。Auto Smartport では、デバイスからマクロへのマッピングにイベント トリガーが使用されます。

スイッチ ソフトウェアに組み込まれている Auto Smartport マクロは、CLI コマンドのグループです。ポート上で CISCO_PHONE イベントが検出されると、スイッチによって CISCO_PHONE_AUTO_SMARTPORT マクロでコマンドが適用されます。Cisco IOS シェル スクリプト機能 (コマンドの自動化や変数の代入を行うための BASH に似ている言語構文) を使用してユーザ定義のマクロを作成することもできます。

スタティック Smartport マクロでは、ポートに接続されているデバイスに基づいて手動で適用するポート設定が提供されるため、Auto Smartport マクロはスタティック Smartport マクロとは異なります。スタティック Smartport マクロを適用すると、マクロ内の CLI コマンドが既存のポート設定に追加されます。ポート上でリンクダウン イベントが発生した場合、スイッチはスタティック マクロ設定を削除しません。

Auto Smartport はイベントを使用してマクロをイベントの発信元ポートにマッピングします。接続されたデバイスからの Cisco Discovery Protocol (CDP) メッセージに基づくイベント トリガーが最も一般的です。デバイス (Cisco IP Phone、(Autonomous アクセス ポイントおよび Lightweight アクセス ポイントを含む) Cisco ワイヤレス Access Point (AP; アクセス ポイント)、シスコ製スイッチ、シスコ製ルータ、および Cisco IP Video Surveillance Camera) の検出により、CDP イベント トリガーが呼び出されます。

シスコ製およびサードパーティ製デバイスのその他のイベント トリガーは、ユーザ定義 MAC アドレス グループ、MAC authentication bypass (MAB; MAC 認証バイパス) メッセージ、802.1X 認証メッセージ、および、Link Layer Discovery Protocol (LLDP) メッセージです。

LLDP は一連のアトリビュートをサポートし、これらを使用して隣接するデバイスを検出します。アトリビュートには **Type**、**Length**、および **Value** があり、これらを TLV と呼びます。LLDP をサポートするデバイスは、情報の送受信に TLV を使用できます。このプロトコルは、設定の情報、デバイスの機能、デバイス ID などの詳細情報をアドバタイズします。Auto Smartport は LLDP *system capabilities* TLV をイベント トリガーとして使用します。Auto Smartport の LLDP *system capabilities* TLV アトリビュートの設定の詳細については、第 28 章「LLDP、LLDP-MED、および接続された場所のサービスの設定」を参照してください。

CDP、MAB、802.1X 認証をいずれもサポートしていないデバイス (ネットワーク プリンタ、LLDP、または、レガシーな Cisco Digital Media Player など) の場合は、MAC Operationally Unique Identifier (OUI) ベースのトリガーを使用して MAC アドレス グループを設定できます。必要な設定を含む、組み込みまたはユーザ定義のマクロに MAC アドレスをマッピングします。

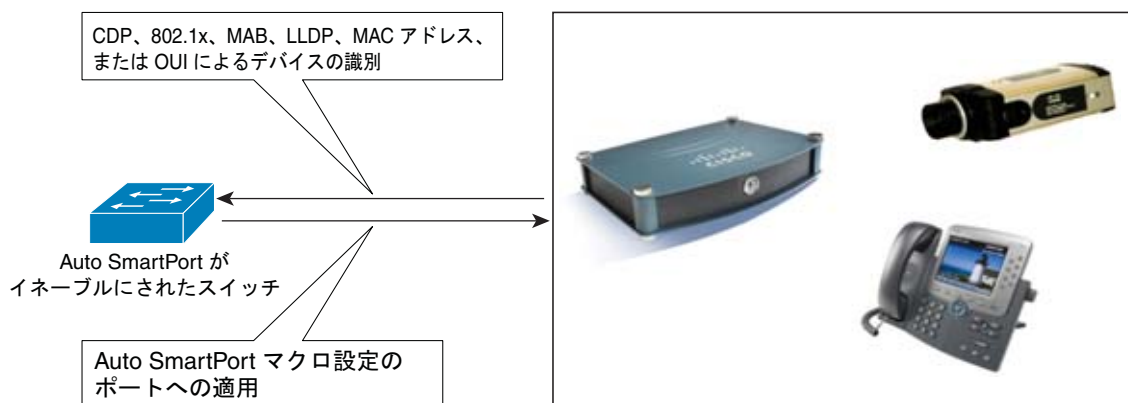
ユーザ定義マクロ ファイルのリモート サーバの場所を指定できます。ネットワークの複数のスイッチによって使用される複数の Auto Smartport マクロ ファイルの 1 セットを更新およびメンテナンスできます。

Auto Smartport マクロ固定機能によって、リンクダウン イベントの検出にかかわらず、マクロ設定をスイッチ ポートに適用されたままにできます。この機能を使用して、スイッチ上の Auto Smartport マクロ設定をスタティックにできます。これは、スイッチにリンクアップ イベントおよびリンクダウン イベントがある場合や、EnergyWise の設定されたネットワークに参加するエンティティである場合に、複数のシステム ログおよび設定変更イベントを防止します。

Auto Smartport および Cisco Medianet

Cisco Medianet は、ネットワーク インフラストラクチャでの幅広いビデオ アプリケーションのインテリジェント サービスを実現します。Medianet のサービスの 1 つは、Auto Smartport による Cisco Digital Media Player および Cisco IP Video Surveillance Camera の自動プロビジョニングです。スイッチは、CDP、802.1X、MAB、LLDP、および MAC アドレスを使用して、Cisco 製およびサードパーティ製のビデオ デバイスを特定します (図 13-1)。スイッチは、適切な Auto Smartport マクロを適用して、デバイスに適切な VLAN および QoS 設定をイネーブルにします。スイッチは、組み込み MAC アドレス グループを使用して、of4400 または 23ac00 の OUI に基づいて、レガシー Cisco DMP を検出します。任意のビデオ デバイスのカスタム ユーザ定義マクロも作成できます。

図 13-1 Cisco Medianet 配置例



Auto Smartport の設定

- 「デフォルトの Auto Smartport 設定」 (P.13-3)
- 「Auto Smartport の設定に関する注意事項」 (P.13-4)
- 「Auto Smartport のイネーブル化」 (P.13-5)
- 「Auto Smartport デフォルト パラメータ値の設定」 (P.13-5)
- 「Auto Smartport MAC アドレス グループの設定」 (P.13-7)
- 「Auto Smartport マクロ固定の設定」 (P.13-8)
- 「Auto Smartport 組み込みマクロ オプションの設定」 (P.13-9)
- 「ユーザ定義イベント トリガーの作成」 (P.13-11)
- 「Auto Smartport ユーザ定義マクロの設定」 (P.13-15)

デフォルトの Auto Smartport 設定

- Auto Smartport は、インターフェイス単位でグローバルにディセーブルに設定され、イネーブルに設定されます。
- CDP フォールバックは、インターフェイス単位でグローバルにディセーブルに設定され、イネーブルに設定されます。
- Cisco IOS シェルはイネーブルに設定されます。
- 表 13-1 に示されるデバイスに対して ASP がイネーブルに設定されている場合、Auto Smartport マクロがデフォルトで使用されます。

表 13-1 Auto Smartport 組み込みマクロ

マクロ名	説明
CISCO_PHONE_AUTO_SMARTPORT	このマクロは、Cisco IP Phone に IP Phone マクロを適用します。QoS、ポートセキュリティ、ストーム制御、DHCP スヌーピング、およびスパニングツリー保護をイネーブルにします。インターフェイスのアクセス VLAN と音声 VLAN も設定します。
CISCO_SWITCH_AUTO_SMARTPORT	このマクロは、Cisco スイッチにスイッチ マクロを適用します。QoS および 802.1Q カプセル化によるトランッキングをイネーブルにします。インターフェイス上のネイティブ VLAN も設定します。
CISCO_ROUTER_AUTO_SMARTPORT	このマクロは、Cisco ルータにルータ マクロを適用します。QoS および 802.1Q カプセル化によるトランッキング、および、スパニングツリー BPDU 保護をイネーブルにします。
CISCO_AP_AUTO_SMARTPORT	このマクロは Cisco AP にワイヤレス アクセス ポイント マクロを適用します。QoS および 802.1Q カプセル化によるトランッキングをイネーブルにします。インターフェイス上のネイティブ VLAN も設定します。
CISCO_LWAP_AUTO_SMARTPORT	このマクロは、シスコ製軽量ワイヤレス AP に軽量ワイヤレス アクセス ポイント マクロを適用します。QoS、ポートセキュリティ、ストーム制御、DHCP スヌーピング、およびスパニングツリー保護をイネーブルにします。インターフェイスのアクセス VLAN を設定し、未知のユニキャスト パケットからネットワークを保護します。

表 13-1 Auto Smartport 組み込みマクロ (続き)

マクロ名	説明
CISCO_IPVSC_AUTO_SMARTPORT	このマクロは、Cisco IP Video Surveillance Camera に IP camera マクロを適用します。QoS trust、ポートセキュリティ、およびスパンニングツリー保護をイネーブルにします。インターフェイスのアクセス VLAN を設定し、未知のユニキャストパケットからネットワークを保護します。
CISCO_DMP_AUTO_SMARTPORT	このマクロは、Cisco Digital Media Player に Digital Media Player マクロを適用します。QoS trust、ポートセキュリティ、およびスパンニングツリー保護をイネーブルにします。インターフェイスのアクセス VLAN を設定し、未知のユニキャストパケットからネットワークを保護します。

Auto Smartport の設定に関する注意事項

- 組み込みマクロは削除または変更を行うことはできません。ただし、同じ名前ユーザ定義のマクロを作成して組み込みマクロを上書きすることはできます。元の組み込みマクロを復元するには、ユーザ定義のマクロを削除します。
- **macro auto device** グローバル コンフィギュレーション コマンドおよび **macro auto execute** グローバル コンフィギュレーション コマンドの両方をイネーブルにする場合、最後に実行されたコマンドのパラメータがスイッチに適用されます。スイッチ上では 1 つのコマンドだけがアクティブになります。
- Auto Smartport マクロの適用時にシステムの競合を回避するためには、802.1x 認証以外のすべてのポート設定を削除します。
- スイッチ上で Auto Smartport をイネーブルにする場合、ポートセキュリティを設定しません。
- マクロがオリジナルの設定と矛盾する場合は、マクロはオリジナルの設定コマンドの一部を適用しないか、また、アンチマクロがそれらを削除しません (アンチマクロはリンク ダウン イベント時に適用されるマクロを削除する適用済みマクロの一部です)。

たとえば、802.1x 認証がイネーブルの場合は、**switchport mode access** 設定を削除できません。**switchport mode** 設定を削除する前に 802.1x 認証を削除します。
- Auto Smartport マクロを適用するときは、ポートを EtherChannel のメンバーにしないでください。EtherChannel を使用する場合は、**no macro auto processing** インターフェイス コンフィギュレーション コマンドを使用して EtherChannel のメンバーであるインターフェイス上で Auto Smartport をディセーブルにします。
- 組み込みマクロのデフォルトのデータ VLAN は VLAN 1 です。組み込みマクロのデフォルトの音声 VLAN は VLAN 2 です (VLAN 1 はすべてのマクロのデフォルトのデータ VLAN です。VLAN 2 はすべてのマクロのデフォルトの音声 VLAN です)。スイッチが異なるアクセス VLAN、ネイティブ VLAN または音声 VLAN を使用する場合は、**macro auto device** グローバル コンフィギュレーション コマンドまたは **macro auto execute** グローバル コンフィギュレーション コマンドを使用して該当する非デフォルトの値を設定します。
- **show macro auto device** 特権 EXEC コマンドを使用して、デフォルト マクロに加えて、各マクロのデフォルト パラメータ値、現在の値、および、設定可能なパラメータの一覧を表示します。**show shell functions** 特権 EXEC コマンドを使用しても、組み込みマクロのデフォルト値を表示できます。
- 802.1x 認証または MAB の場合は、Cisco Attribute-Value (AV; アトリビュート値) ペアの **auto-smart-port=event trigger** をサポートしてシスコ以外のデバイスを検出するように RADIUS サーバを設定します。

- CDP、MAB、802.1X 認証をいずれもサポートしないステーションリ デバイス（ネットワーク プリンタなど）の場合は、MAC OUI ベースのトリガーを使用して MAC アドレス グループを設定し、必要な設定を含むユーザ定義マクロにマッピングできます。
- スイッチは直接接続されたデバイス上でだけ Auto Smartport マクロをサポートします。ハブのような複数のデバイス接続はサポートされません。複数のデバイスが接続されている場合は、適用されるマクロは、検出された最初のデバイスに割り当てられたマクロです。
- ポートで認証がイネーブルに設定されている場合、認証が失敗したときは、スイッチは MAC アドレス トリガーを無視します。
- マクロ内の CLI コマンドの順序と対応するアンチマクロは異なる場合があります。
- Auto SmartPort はグローバル コンフィギュレーションを実行しません。インターフェイス レベルの Auto Smartport マクロがグローバル設定を必要とする場合は、手動でグローバル コンフィギュレーションを追加する必要があります。

Auto Smartport のイネーブル化

スイッチ上で Auto Smartport マクロをグローバルにイネーブルにするには、次の手順を実行します。この手順は必須です。特定のポート上で Auto Smartport マクロをディセーブルにするには、**no auto global processing** インターフェイス コンフィギュレーション コマンドを使用します。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto global processing	スイッチで Auto Smartport をグローバルにイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	Auto Smartport がイネーブルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

show macro auto device、**show shell functions**、および **show shell triggers** 特権 EXEC コマンドを使用してイベント トリガー、組み込みマクロ、および組み込みマクロのデフォルト値を表示します。

次に、スイッチ上で Auto Smartport をイネーブルにする方法と、特定のインターフェイス上で機能をディセーブルにする例を示します。

```
Switch(config)# macro auto global processing
Switch(config)# interface interface_id
Switch(config-if)# no macro auto processing
```

Auto Smartport デフォルト パラメータ値の設定

スイッチはイベント トリガーから組み込みマクロへ自動的にマッピングします。Auto Smartport デフォルト パラメータ値をスイッチ固有の値に置き換えるには次の手順を実行します。この手順は任意です。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	show macro auto device	マクロ デフォルト パラメータ値を表示します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	macro auto device {access-point ip-camera lightweight-ap media-player phone router switch} [parameter=value]	指定したマクロ デフォルト パラメータ値を置き換えます。それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します (例: [<name1>=<value1> <name2>=<value2>...])。各マクロ デフォルト パラメータ値のデフォルト値は、次のとおりです。 <ul style="list-style-type: none"> • access-point NATIVE_VLAN=1 • ip-camera ACCESS_VLAN=1 • lightweight-ap ACCESS_VLAN=1 • media-player ACCESS_VLAN=1 • phone ACCESS_VLAN=1 VOICE_VLAN=2 • router NATIVE_VLAN=1 • switch NATIVE_VLAN=1 (注) パラメータ名のテキストは、組み込みマクロ定義のテキスト文字列に一致する必要があるため、正確なパラメータ名 (例: VOICE_VLAN) を入力しなければなりません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show macro auto device	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no macro auto device {macro name} parameter=value** グローバル コンフィギュレーション コマンドを使用します。

次に、IP Phone マクロ パラメータ値を表示する方法と、デフォルト音声 VLAN を 20 に変更する例を示します。デフォルト値を変更したとき、すでにマクロが適用されたインターフェイスには適用されません。設定された値は、次のリンクアップ イベント時に適用されます。VOICE_VLAN に正確なテキスト文字列が使用されていることに注意してください。エントリでは大文字と小文字が区別されます。

```
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:ACCESS_VLAN=1 VOICE_VLAN=2

Switch# configure terminal
Switch(config)# macro auto device phone VOICE_VLAN=20
Switch(config)# end
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:voice_vlan=20
```


Auto Smartport MAC アドレス グループの設定

CDP や LLDP などの近隣探索プロトコルをサポートしないデバイス（プリンターなど）では、Auto Smartport のために MAC アドレス ベースのトリガー設定を使用します。この手順は任意で、次のステップが必要です。

- **macro auto mac-address** グローバル コンフィギュレーション コマンドを使用して MAC アドレス ベースのトリガーを設定します。
- **macro auto execute** グローバル コンフィギュレーション コマンドを使用して、MAC アドレス トリガーを組み込みまたはユーザ定義マクロに対応付けます。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto mac-address-group name	グループ名を指定し、MAC アドレス コンフィギュレーション モードを開始します。
ステップ 3	[mac-address list list] [oui [list list range word size number]]	スペースで区切られた MAC アドレスのリストを設定します。 Operationally Unique Identifier (OUI) のリストまたは範囲を指定します。OUI は、MAC アドレスの最初の 3 バイトで、製品の製造業者を特定します。OUI を指定することで、近隣探索プロトコルをサポートしないデバイスが認識されます。 <ul style="list-style-type: none"> • list : スペースで区切られた 16 進数からなる OUI リストを入力します。 • range : OUI 開始範囲を 16 進数で入力します。サイズ (1 ~ 5) を入力して、連続したアドレスを作成します。
ステップ 4	macro auto execute address_trigger built-in macro name	MAC アドレス グループ トリガーを組み込みまたはユーザ定義マクロにマッピングします。 65 秒のホールドタイムの後、MAC アドレス トリガーがインターフェイスに適用されます。ホールドタイムは、MAC アドレスの代わりに CDP または LLDP などの近接探索プロトコルが使用されることを可能にします。
ステップ 5	exit	コンフィギュレーション モードに戻ります。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show macro auto address-group	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アドレス グループを削除するには、**no macro auto mac-address-group name** グローバル コンフィギュレーション コマンドを使用します。**no macro auto mac-address-group name** を入力して、マクロ トリガー、および、**macro auto execute** グローバル コンフィギュレーション コマンドを使用して定義されたマクロに対応付けられたトリガー マッピングを削除します。**no macro auto execute mac-address-group** を入力した場合は、マクロへのトリガーのマッピングを削除するだけです。

次に、*address_trigger* という名前の MAC アドレス グループ イベント トリガーを作成する方法と、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# macro auto address-group mac address_trigger
Switch(config-addr-grp-mac)# mac-address list 2222.3333.3334 22.33.44 a.b.c
Switch(config-addr-grp-mac)# oui list 455555 233244
```

```

Switch(config-addr-grp-mac)# oui range 333333 size 2
Switch(config-addr-grp-mac)# exit
Switch(config)# mac auto execute address-trigger builtin macro
Switch(config)# exit
Switch(config)# end
Switch(config)# macro auto execute mac-address-trigger builtin CISCO_PHONE_AUTO_SMARTPORT
Switch(config)# end
Switch# show running configuration | include macro
macro auto mac-address-group address_trigger
mac auto mad-address-group hel
mac auto execute mad-address-trigger builtin CISCO_PHONE_AUTO_SMARTPORT
macro description CISCO_DMP_EVENT
mac description CISCO_SWITCH_EVENT
!
<output truncated>

```

Auto Smartport マクロ固定の設定

スイッチで Auto Smartport をイネーブルに設定する場合、デフォルトで、リンクアップ イベント時にマクロ設定が適用され、リンクダウン イベント時にマクロ設定が削除されます。マクロ固定機能をイネーブルにすると、設定はリンクアップ時に適用され、リンクダウン時に削除されません。スイッチ上でのリンクアップ イベントまたはリンクダウン イベントにかかわらず、適用された設定は維持されます。実行コンフィギュレーションファイルが保存される場合、マクロ固定機能はリブートを経ても設定されたままです。

Auto Smartport マクロをイネーブルにして、リンクダウン イベント後もスイッチ上でアクティブなままにするには、次の手順を実行します。この手順は任意です。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto sticky	Auto Smartport マクロ設定をイネーブルにし、リンクダウン イベント時にもインターフェイス上で継続されるようにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show macro auto	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Auto Smartport マクロ固定機能をディセーブルにするには、**no macro auto sticky** グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ上で Auto Smartport 自動スティッキー機能をイネーブルにする方法を示します。

```
Switch(config)# macro auto sticky
```

Auto Smartport 組み込みマクロ オプションの設定

この手順を使用してイベント トリガーを組み込みマクロにマッピングし、組み込みマクロ デフォルトパラメータ値をスイッチに固有の値に置き換えます。マクロのデフォルトパラメータ値を置き換える必要がある場合、**macro auto device** グローバル コンフィギュレーション コマンドを使用します。この手順のすべてのコマンドは任意です。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto execute event trigger builtin built-in macro name [parameter=value] [parameter=value]	<p>イベント トリガーから組み込みマクロへのマッピングを定義します。 <i>event trigger</i> を指定します。</p> <ul style="list-style-type: none"> • CISCO_DMP_EVENT • CISCO_IPVSC_EVENT • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • WORD : ユーザ定義のイベント トリガーを適用します。 <p>builtin built-in macro name を指定します。</p> <p>それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します (例 : [<i><name1>=<value1> <name2>=<value2>...</i>])。正確に入力が必要なとおりのデフォルト値は次のとおりです。</p> <ul style="list-style-type: none"> • CISCO_DMP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。 • CISCO_IPVSC_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。 • CISCO_PHONE_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 および VOICE_VLAN=2 を指定します。 • CISCO_SWITCH_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。 • CISCO_ROUTER_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。 • CISCO_AP_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。 • CISCO_LWAP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。

	コマンド	目的
ステップ 3	<code>remote url</code>	<p>リモート マクロ ファイルのリモート サーバの場所を指定します。</p> <ul style="list-style-type: none"> • スタンドアロン スイッチまたはスタック マスター上のローカル フラッシュ ファイル システムの構文 : flash: • スタック メンバー上のローカルフラッシュ ファイル システムの構文 : flash member number: • FTP の構文 : ftp:[[/username[:password]@location]/directory]/filename • HTTP サーバの構文 : http:[/([username:password]@){hostname host-ip}/directory]/filename • セキュア HTTP サーバの構文 : https:[/([username:password]@){hostname host-ip}/directory]/filename • NVRAM の構文 : nvram:[/([username:password]@)/directory]/filename • Remote Copy Protocol (RCP; リモート コピー プロトコル) の構文 : rcp:[/username@location]/directory]/filename • Secure Copy Protocol (SCP; セキュア コピー プロトコル) の構文 : scp:[/username@location]/directory]/filename • Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) の構文 : tftp: [[/location]/directory]/filename
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	コンフィギュレーション ファイルに設定を保存します。

次に、シスコ製スイッチと Cisco IP Phone をスイッチに接続するための 2 つの組み込み Auto Smartport マクロを使用する例を示します。次に、トランク インターフェイスのデフォルトの音声 VLAN、アクセス VLAN、およびネイティブ VLAN を変更する例を示します。

```
Switch# configure terminal
Switch(config)#!!!the next command modifies the access and voice vlans
Switch(config)#!!!for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!!the next command modifies the Native vlan used for inter switch trunks
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config)#
Switch(config)#!!!the next command enables auto smart ports globally
Switch(config)# macro auto global processing cdp-fallback
Switch(config)#
Switch(config)# exit

Switch# !!!here's the running configuration of the interface connected
Switch# !!!to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface gigabitethernet1/0/1
```

```
Building configuration...

Current configuration : 284 bytes
!
interface gigabitethernet1/0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport mode trunk
srr-queue bandwidth share 10 10 60 20
queue-set 2
priority-queue out
mls qos trust cos
auto qos voip trust
macro description CISCO_SWITCH_EVENT
end
```

この例は、リモートマクロをネイティブ VLAN 5 の設定を使用して設定する方法を示します。

- a. **macro.txt** ファイルのリモートマクロを設定します。
- b. **macro auto execute** コンフィギュレーションコマンドを使用して、マクロファイルのリモートの場所を指定します。

```
if [[ $LINKUP -eq YES ]]; then
  conf t
    interface $INTERFACE
      macro description $TRIGGER
      auto qos voip trust
      switchport trunk encapsulation dot1q
      switchport trunk native vlan $NATIVE_VLAN
      switchport trunk allowed vlan ALL
      switchport mode trunk
    exit
  end
else
  conf t
    interface $INTERFACE
      no macro description
      no auto qos voip trust
      no switchport mode trunk
      no switchport trunk encapsulation dot1q
      no switchport trunk native vlan $NATIVE_VLAN
      no switchport trunk allowed vlan ALL
    exit
  end

Switch(config)# macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt
NATIVE_VLAN=5

Switch# show running configuration | include macro
macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt
NATIVE_VLAN=5
Switch#
```

ユーザ定義イベント トリガーの作成

MAB または 802.1x 認証を使用して Auto Smartport マクロをトリガーする場合は、RADIUS サーバから送信された Cisco AV ペア (**auto-smart-port=event trigger**) に対応するイベント トリガーを作成する必要があります。この手順は任意です。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	shell trigger identifier description	イベント トリガー ID および説明を指定します。ID の単語の間にはスペースやハイフンを含めないでください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show shell triggers	スイッチ上のイベント トリガーを表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

no shell trigger identifier グローバル コンフィギュレーション コマンドを使用してイベント トリガーを削除します。

次に、RADIUS_MAB_EVENT という名前のユーザ定義イベント トリガーを組み込みマクロ CISCO_AP_AUTO_SMARTPORT にマッピングし、デフォルト VLAN を VLAN 10 に置き換える例と、設定を確認する例を示します。

- a. デバイスを MAB 対応スイッチ ポートに接続します。
- b. RADIUS サーバ上で、AV ペアを **auto-smart-port=RADIUS_MAB_EVENT** に設定します。
- c. スイッチで、イベント トリガー RADIUS_MAB_EVENT を作成します。
- d. スイッチは、RADIUS サーバからの AV pair=RADIUS_MAB_EVENT 応答を認識し、マクロ CISCO_AP_AUTO_SMARTPORT を適用します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# !!!create a user defined trigger and map
Switch(config)# !!!a system defined macro to it
Switch(config)# !!!first create the trigger event
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
Switch(config)#
Switch(config)#!!!map a system defined macro to the trigger event
Switch(config)# macro auto execute RADIUS_MAB_EVENT builtin ?
_ CISCO_DMP_AUTO_SMARTPORT
_ CISCO_IPVSC_AUTO_SMARTPORT
_ CISCO_AP_AUTO_SMARTPORT
_ CISCO_LWAP_AUTO_SMARTPORT
_ CISCO_PHONE_AUTO_SMARTPORT
_ CISCO_ROUTER_AUTO_SMARTPORT
_ CISCO_SWITCH_AUTO_SMARTPORT
LINE <cr>
Switch(config)# macro auto execute RADIUS_MAB_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=10
Switch(config)# exit
Switch# show shell triggers
User defined triggers
-----
Trigger Id: RADIUS_MAB_EVENT
Trigger description: MAC_AuthBypass Event
Trigger environment:
Trigger mapping function: CISCO_AP_SMARTPORT
<output truncated>
```

次に、**show shell triggers** 特権 EXEC コマンドを使用して、スイッチ ソフトウェアでイベント トリガーを表示する例を示します。

```
Switch# show shell triggers
```

```
User defined triggers
```

```
Built-in triggers
```

```
Trigger Id: CISCO_DMP_EVENT
```

```
Trigger description: Digital media-player device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_DMP_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_IPVSC_EVENT
```

```
Trigger description: IP-camera device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1), The value in parenthesis is a default value
```

```
Trigger mapping function: CISCO_IP_CAMERA_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_PHONE_EVENT
```

```
Trigger description: IP-phone device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $ACCESS_VLAN=(1) and $VOICE_VLAN=(2), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_PHONE_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_ROUTER_EVENT
```

```
Trigger description: Router device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_SWITCH_EVENT
```

```
Trigger description: Switch device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_WIRELESS_AP_EVENT
```

```
Trigger description: Autonomous ap device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_AP_AUTO_SMARTPORT
```

```
Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
```

```
Trigger description: Lightweight-ap device event to apply port configuration
```

```
Trigger environment: Parameters that can be set in the shell - $NATIVE_VLAN=(1), The value in the parenthesis is a default value
```

```
Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT
```

次に、**show shell functions** 特権 EXEC コマンドを使用してスイッチ ソフトウェアの組み込みマクロを表示する例を示します。

```
Switch# show shell functions
```

```
#User defined functions:
```

```
#Built-in functions:
```

```
function CISCO_AP_AUTO_SMARTPORT () {
```

```
    if [[ $LINKUP -eq YES ]]; then
```

```
        conf t
```

```
            interface $INTERFACE
```

```
                macro description $TRIGGER
```

```
                switchport trunk encapsulation dot1q
```

```

        switchport trunk native vlan $NATIVE_VLAN
        switchport trunk allowed vlan ALL
        switchport mode trunk
        switchport nonegotiate
        auto qos voip trust
        mls qos trust cos
    exit
end
fi
if [[ $LINKUP -eq NO ]]; then
    conf t
        interface $INTERFACE
            no macro description
            no switchport nonegotiate
            no switchport trunk native vlan $NATIVE_VLAN
            no switchport trunk allowed vlan ALL
            no auto qos voip trust
            no mls qos trust cos
            if [[ $AUTH_ENABLED -eq NO ]]; then
                no switchport mode
                no switchport trunk encapsulation
            fi
        fi
    exit
end
fi
}

function CISCO_SWITCH_AUTO_SMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface $INTERFACE
                macro description $TRIGGER
                auto qos voip trust
                switchport trunk encapsulation dot1q
                switchport trunk native vlan $NATIVE_VLAN
                switchport trunk allowed vlan ALL
                switchport mode trunk
            exit
        end
    else
        conf t
            interface $INTERFACE
                no macro description
                no auto qos voip trust
                no switchport mode trunk
                no switchport trunk encapsulation dot1q
                no switchport trunk native vlan $NATIVE_VLAN
                no switchport trunk allowed vlan ALL
            exit
        end
    fi
}

<output truncated>

```


Auto Smartport ユーザ定義マクロの設定

Cisco IOS シェルは、ユーザ定義の Auto Smartport マクロを設定するための基本的なスクリプト機能を提供します。これらのマクロには複数の行を含むことができ、どの CLI コマンドでも含めることができます。マクロ内で変数の置換、条件、関数、およびトリガーを定義することもできます。この手順は任意です。

ユーザ定義イベント トリガーをユーザ定義マクロにマップするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto execute event trigger [parameter=value] {function contents}	イベント トリガーにマップするユーザ定義マクロを指定します。 {function contents} : トリガーに関連付けるユーザ定義のマクロを指定します。マクロの内容を波カッコで囲んで入力します。左波カッコで Cisco IOS シェル コマンドを開始し、右波カッコでコマンドのグループ化を終了します。 (任意) parameter=value : \$ から始まるデフォルト値を置き換え、スペースで区切られた名前値のペア ([<name1>=<value1> <name2>=<value2>...]) の形式で新しい値を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、media player と呼ばれるユーザ定義のイベント トリガーをユーザ定義のマクロにマッピングする方法を示します。

- a. media player を 802.1X または MAB 対応のスイッチ ポートに接続します。
- b. RADIUS サーバ上で、AV ペアを **auto-smart-port =MP_EVENT** に設定します。
- c. スイッチで、イベント トリガー MP_EVENT を作成し、次のようにユーザ定義マクロ コマンドを入力します。
- d. スイッチは、属性と値のペアが MP_EVENT であるとの RADIUS サーバからの応答を認識し、このイベント トリガーに関連付けられているマクロを適用します。

```
Switch(config)# shell trigger MP_EVENT mediaplayer
Switch(config)# macro auto execute MP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
  interface $INTERFACE
    macro description $TRIGGER
    switchport access vlan 1
    switchport mode access
    switchport port-security
    switchport port-security maximum 1
    switchport port-security violation restrict
    switchport port-security aging time 2
    switchport port-security aging type inactivity
    spanning-tree portfast
    spanning-tree bpduguard enable
  exit
fi
if [[ $LINKUP -eq NO ]]; then
conf t
```

```

interface $INTERFACE
  no macro description $TRIGGER
  no switchport access vlan 1
  if [[ $AUTH_ENABLED -eq NO ]]; then
    no switchport mode access
  fi
  no switchport port-security
  no switchport port-security maximum 1
  no switchport port-security violation restrict
  no switchport port-security aging time 2
  no switchport port-security aging type inactivity
  no spanning-tree portfast
  no spanning-tree bpduguard enable
  exit
fi
}
Switch(config)# end

```

表 13-2 サポート対象の Cisco IOS シェル キーワード

コマンド	説明
{	コマンドのグループ化を開始します。
}	コマンドのグループ化を終了します。
[[条件付きコンストラクトとして使用します。
]]	条件付きコンストラクトとして使用します。
else	条件付きコンストラクトとして使用します。
-eq	条件付きコンストラクトとして使用します。
fi	条件付きコンストラクトとして使用します。
if	条件付きコンストラクトとして使用します。
then	条件付きコンストラクトとして使用します。
-z	条件付きコンストラクトとして使用します。
\$	\$ 文字で始まる変数はパラメータ値に置き換えられます。
#	コメント テキストを入力するには # 文字を使用します。

表 13-3 サポートされない Cisco IOS シェル予約済みキーワード

コマンド	説明
	パイプライン
case	条件付きコンストラクト
esac	条件付きコンストラクト
for	ルーピング コンストラクト
function	シェル関数
in	条件付きコンストラクト
select	条件付きコンストラクト
time	パイプライン
until	ルーピング コンストラクト
while	ルーピング コンストラクト

スタティック Smartport マクロの設定

- 「デフォルトのスタティック Smartport 設定」 (P.13-17)
- 「スタティック Smartport コンフィギュレーションに関する注意事項」 (P.13-17)
- 「スタティック Smartport マクロの適用」 (P.13-18)

デフォルトのスタティック Smartport 設定

スイッチ上ではスタティック Smartport マクロはイネーブルになっていません。

表 13-4 デフォルトのスタティック Smartport マクロ

マクロ名 ¹	説明
cisco-global	Rapid PVST+, ループ ガード、リンク ステート障害用のダイナミック ポート エラー回復をイネーブルにするには、このグローバル コンフィギュレーション マクロを使用します。
cisco-desktop	PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、ネットワーク セキュリティと信頼性を高めるために、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-phone	Cisco IP Phone を装備した PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。このマクロは、 cisco-desktop マクロの拡張機能で、同じセキュリティ機能と復元力機能を提供します。ただし、遅延に影響されやすい音声トラフィックを適切に処理するために、専用音声 VLAN が追加されています。
cisco-switch	アクセス スイッチとディストリビューション スイッチを接続する場合、または Small Form-Factor Pluggable (SFP) を使用して接続したアクセス スイッチの間で、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-router	スイッチと WAN ルータを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-wireless	スイッチとワイヤレス アクセス ポイントを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。

1. シスコのデフォルト SmartPort マクロは、スイッチで稼動するソフトウェアのバージョンによって異なります。

スタティック Smartport コンフィギュレーションに関する注意事項

- スイッチまたはスイッチ インターフェイスにマクロをグローバルに適用しても、インターフェイスの既存の設定は維持されます。これは、差分設定に適用する場合に役立ちます。
- 構文エラーまたは設定エラーが原因でコマンドが失敗した場合でも、マクロは引き続き残りのコマンドを適用します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、**macro global trace macro-name** グローバル コンフィギュレーション コマンド、または **macro trace macro-name** インターフェイス コンフィギュレーション コマンドを使用できます。
- 特定のインターフェイス タイプ固有の CLI コマンドもあります。設定を受け入れないインターフェイスにマクロを適用すると、マクロは構文チェックまたは設定チェックに失敗し、スイッチはエラー メッセージを返します。
- インターフェイス範囲へのマクロの適用は、単一インターフェイスへのマクロの適用と同じです。インターフェイス範囲を使用すると、インターフェイス範囲内の各インターフェイスへマクロが順番に適用されます。1 つのインターフェイスでマクロ コマンドの実行に失敗しても、マクロは残りのインターフェイス上に適用されます。

- スイッチまたはスイッチ インターフェイスにマクロを適用すると、マクロ名が自動的にスイッチまたはインターフェイスに追加されます。 **show running-config** ユーザ EXEC コマンドを使用して、適用されたコマンドおよびマクロ名を表示できます。

スタティック Smartport マクロの適用

スタティック SmartPort マクロを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show parser macro	スイッチ ソフトウェアに組み込まれたシスコのデフォルト スタティック SmartPort マクロを表示します。
ステップ 2	show parser macro name <i>macro-name</i>	適用する特定のマクロを表示します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	macro global { apply trace } <i>macro-name</i> [parameter { <i>value</i> }] [parameter { <i>value</i> }] [parameter { <i>value</i> }]	マクロに定義されている個々のコマンドをスイッチに適用するには、 macro global apply macro-name を入力します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、 macro global trace macro-name を指定します。 parameter value キーワードを使用して、マクロに必要な値を加えます。 \$ で始まるキーワードには、一意のパラメータ値が必要です。 macro global apply macro-name ? コマンドを使用すると、マクロに必要な値のリストを表示できます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。 (任意) スイッチに固有の一意のパラメータ値を指定します。キーワードの値のペアは、最大 3 つまで入力できます。パラメータ キーワードの照合では大文字と小文字が区別されます。対応する値は、一致するキーワードすべてを置き換えます。
ステップ 5	interface <i>interface-id</i>	(任意) インターフェイス コンフィギュレーション モードを開始し、マクロを適用するインターフェイスを指定します。
ステップ 6	default interface <i>interface-id</i>	(任意) 指定のインターフェイスからすべての設定情報を消去します。
ステップ 7	macro { apply trace } <i>macro-name</i> [parameter { <i>value</i> }] [parameter { <i>value</i> }] [parameter { <i>value</i> }]	マクロに定義されている個々のコマンドをポートに適用するには、 macro global apply macro-name を入力します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、 macro global trace macro-name を指定します。 parameter value キーワードを使用して、マクロに必要な値を加えます。 \$ で始まるキーワードには、一意のパラメータ値が必要です。 macro global apply macro-name ? コマンドを使用すると、マクロに必要な値のリストを表示できます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。 (任意) スイッチに固有の一意のパラメータ値を指定します。キーワードの値のペアは、最大 3 つまで入力できます。パラメータ キーワードの照合では大文字と小文字が区別されます。対応する値は、一致するキーワードすべてを置き換えます。
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	show running-config interface <i>interface-id</i>	マクロがインターフェイスに適用されたことを確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

マクロ内にある各コマンドの **no** バージョンを入力することによってのみ、スイッチ上のグローバルマクロ適用済みの設定を削除できます。ポート上のマクロ適用済みの設定を削除するには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを入力します。

次に、**cisco-desktop** マクロを表示してそのマクロを適用し、インターフェイスのアクセス VLAN ID を 25 に設定する例を示します。

```
Switch# show parser macro cisco-desktop
-----
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-----
Switch#
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

Auto Smartport マクロおよびスタティック Smartport マクロの表示

Auto SmartPort マクロおよびスタティック Smartport マクロを表示するには、表 13-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 13-5 Auto Smartport マクロとスタティック Smartport マクロを表示するためのコマンド

コマンド	目的
<code>show macro auto</code>	Auto Smartport マクロに関する情報を表示します。
<code>show parser macro</code>	すべてのスタティック Smartport マクロを表示します。
<code>show parser macro name <i>macro-name</i></code>	特定のスタティック Smartport マクロを表示します。
<code>show parser macro brief</code>	スタティック Smartport マクロ名を表示します。
<code>show parser macro description [interface <i>interface-id</i>]</code>	すべてのインターフェイスまたは指定されたインターフェイスのスタティック Smartport マクロの説明を表示します。
<code>show shell</code>	Auto Smartport イベント トリガーとマクロに関する情報を表示します。



CHAPTER 14

VLAN の設定

この章では、Catalyst 3750 スイッチでの標準範囲 VLAN (VLAN ID 1 ~ 1005) および拡張範囲 VLAN (VLAN ID 1006 ~ 4094) の設定手順について説明します。VLAN メンバシップ モード、VLAN コンフィギュレーション モード、VLAN トランク、および VLAN Membership Policy Server (VMPS; VLAN メンバシップ ポリシー サーバ) からの動的 VLAN 割り当てについても説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



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

この章で説明する内容は、次のとおりです。

- 「VLAN の概要」 (P.14-1)
- 「標準範囲 VLAN の設定」 (P.14-5)
- 「拡張範囲 VLAN の設定」 (P.14-11)
- 「VLAN の表示」 (P.14-15)
- 「VLAN トランクの設定」 (P.14-15)
- 「VMPS の設定」 (P.14-27)

VLAN の概要

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じアトリビュートをすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラッディングが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に割り当てられていないステーション宛てのパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して転送しなければなりません (図 14-1 を参照)。VLAN は、スタック全体にまたがり、複数のポートで構成することができます。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ MIB (Management Information Base; 管理情報ベース) 情報があり、スパニング ツリーの独自の実装をサポートできます。第 19 章「STP の設定」を参照してください。

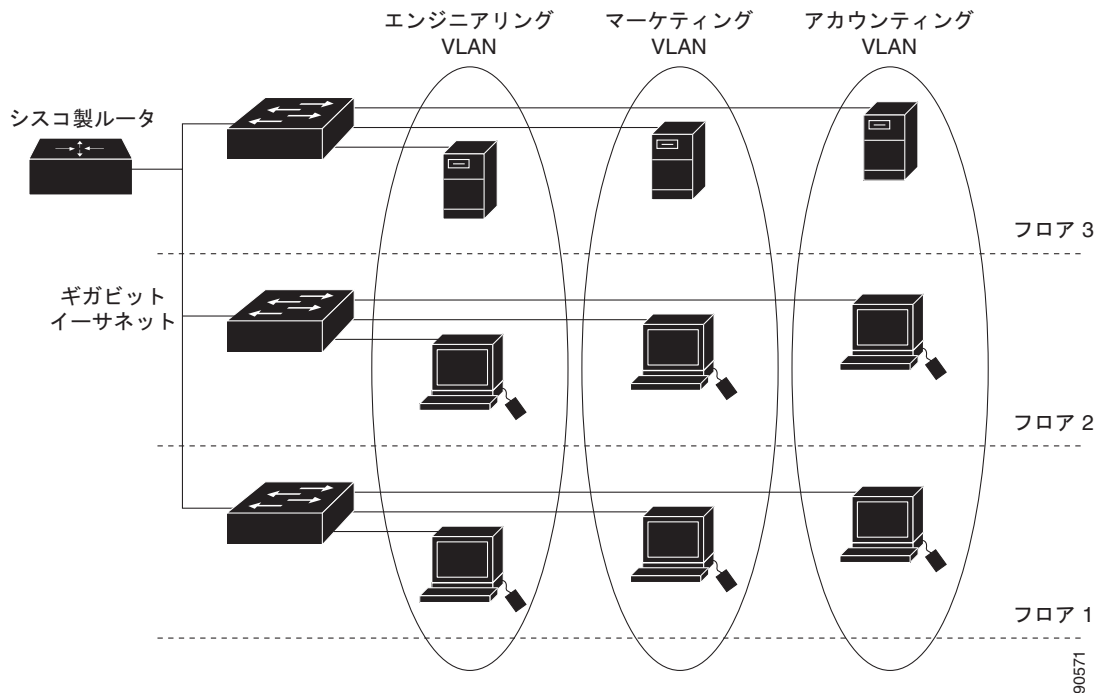


(注)

VLAN を作成する前に、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。VTP の詳細については、第 15 章「VTP の設定」を参照してください。

図 14-1 に、論理的に定義されたネットワークにセグメント化された VLAN の例を示します。

図 14-1 論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットワークに含まれるすべてのエンドステーションは同一の VLAN に所属させます。スイッチ上のインターフェイスの VLAN メンバシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチインターフェイスを VLAN に割り当てた場合、これをインターフェイスベース（またはスタティック）VLAN メンバシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバックブリッジする必要があります。スイッチは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。詳細については、「スイッチ仮想インターフェイス」(P.12-5) および「レイヤ 3 インターフェイスの設定」(P.12-28) を参照してください。



(注)

スイッチに多数の VLAN を設定し、ルーティングをイネーブル化しない予定の場合は、`sdm prefer vlan` グローバル コンフィギュレーション コマンドを使用して Switch Database Management (SDM; スイッチ データベース管理) 機能を VLAN テンプレートに設定できます。このテンプレートは、最大数のユニキャスト MAC (メディア アクセス制御) アドレスをサポートするようにシステム リソースを設定します。SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」、またはこのリリースのコマンドリファレンスの `sdm prefer` コマンドを参照してください。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、および透過モードで VLAN をサポートします。VLAN は、1 ～ 4094 の番号で識別します。VLAN ID 1002 ～ 1005 は、トークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用です。

VTP バージョン 1 およびバージョン 2 は、標準範囲 VLAN (VLAN ID が 1 ～ 1005) だけをサポートします。これらのバージョンで 1006 ～ 4094 の VLAN ID を作成する場合は、スイッチを VTP 透過モードにする必要があります。Cisco IOS Release 12.2(52)SE 以降のリリースは、VTP バージョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体 (1 ～ 4094 の VLAN) をサポートします。拡張範囲 VLAN (1006 ～ 4094 の VLAN) は、VTP バージョン 3 だけでサポートされます。ドメイン内で拡張 VLAN を設定している場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

スイッチ スタックは合計 1005 (標準範囲および拡張範囲) の VLAN をサポートしますが、ルーテッドポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。

スイッチは、最大 128 のスパニング ツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus (PVST+) または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニング ツリー インスタンスを使用できます。スパニング ツリー インスタンス数および VLAN 数の詳細については、「標準範囲 VLAN 設定時の注意事項」(P.14-6) を参照してください。スイッチは、イーサネット ポート経由の VLAN トラフィックの送信方式として、Inter-Switch Link (ISL; スイッチ間リンク) および IEEE 802.1Q トランキングの両方をサポートします。

VLAN ポート メンバシップ モード

VLAN に所属するポートは、メンバシップ モードを割り当てることで設定します。メンバシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

表 14-1 に、各種メンバシップ モード、およびそれぞれのメンバシップと VTP の特性を示します。

表 14-1 ポートのメンバシップ モードとその特性

メンバシップ モード	VLAN メンバシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。 詳細については、「 VLAN へのスタティック アクセス ポートの割り当て 」(P.14-10) を参照してください。	VTP は必須ではありません。VTP を使用して情報をグローバルに伝播させない場合は、VTP モードを透過に設定します。 VTP に加入するには、あるスイッチまたはスイッチ スタックのトランク ポートに接続した別のスイッチ スタック上に 1 つまたは複数のトランク ポートがなければなりません。
トランク (ISL または IEEE 802.1Q)	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバーです。ただし、メンバシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラグディングトラフィックを阻止することもできます。 トランク ポートの設定については、「 トランク ポートとしてのイーサネット インターフェイスの設定 」(P.14-19) を参照してください。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。

メンバシップ モード	VLAN メンバシップの特性	VTP の特性
ダイナミック アクセス	<p>ダイナミック アクセス ポートは 1 つの VLAN (VLAN ID が 1 ~ 4094) だけに所属し、VMPS によって動的に割り当てられます。VMPS には Catalyst 5000 または Catalyst 6500 シリーズ スイッチを使用できますが、Catalyst 3750 スイッチは使用できません。Catalyst 3750 スイッチは、VMPS クライアントです。</p> <p>同一スイッチ上でダイナミック アクセス ポートとトランク ポートを使用できますが、ダイナミック アクセス ポートは別のスイッチではなく、エンドステーションまたはハブに接続する必要があります。</p> <p>設定手順については、「VMPS クライアント上のダイナミック アクセス ポートの設定」(P.14-30) を参照してください。</p>	<p>VTP は必須です。</p> <p>VMPS およびクライアントを同じ VTP ドメイン名で設定してください。</p> <p>VTP に加入するには、あるスイッチまたはスイッチ スタックのトランク ポートに接続した別のスイッチ スタック上に 1 つまたは複数のトランク ポートがなければなりません。</p>
音声 VLAN	<p>音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データトラフィックに別の VLAN を使用するように設定されたアクセス ポートです。</p> <p>音声 VLAN ポートの詳細については、第 16 章「音声 VLAN の設定」 を参照してください。</p>	<p>VTP は不要です。VTP は音声 VLAN に作用しません。</p>
プライベート VLAN	<p>プライベート VLAN ポートは、プライベート VLAN のプライマリまたはセカンダリ VLAN に属するホストまたは混合ポートです。</p> <p>プライベート VLAN の詳細については、第 17 章「プライベート VLAN の設定」 を参照してください。</p>	<p>VTP バージョン 1 およびバージョン 2 でプライベート VLAN を設定する場合は、スイッチを VTP 透過モードにする必要があります。プライベート VLAN がスイッチに設定されている場合、VTP モードを透過モードからクライアント モードやサーバ モードに変更しないでください。</p> <p>VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。</p>
トンネル (dot1q-tunnel)	<p>トンネル ポートは、IEEE 802.1Q トンネリング用に使用され、サービスプロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持します。トンネル ポートをサービスプロバイダー ネットワークのエッジスイッチ上に設定し、カスタマー インターフェイスの IEEE 802.1Q トランク ポートに接続して、非対称リンクを作成します。トンネル ポートは、トンネリング専用の単一の VLAN に属します。</p> <p>トンネル ポートの詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」 を参照してください。</p>	<p>VTP は必須ではありません。switchport access vlan インターフェイス コンフィギュレーション コマンドを使用して、手動で VLAN にトンネル ポートを割り当てます。</p>

アクセス モードとトランク モード、および機能の定義の詳細については、[表 14-4 \(P.14-17\)](#) を参照してください。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。詳細については、「[MAC アドレス テーブルの管理](#)」(P.7-20) を参照してください。

標準範囲 VLAN の設定

標準範囲 VLAN は、VLAN ID が 1 ～ 1005 の VLAN です。スイッチが VTP サーバ モードまたは VTP 透過モードの場合、VLAN データベース内の VLAN 2 ～ 1001 の設定を追加、変更、または削除できます (VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません)。

VTP バージョン 1 およびバージョン 2 で拡張範囲 VLAN (VLAN ID が 1006 ～ 4094) を作成する場合は、スイッチを VTP 透過モードにする必要がありますが、これらの VLAN は VLAN データベースには保存されません。VTP バージョン 3 は、VTP サーバ モードと透過モードで拡張範囲 VLAN をサポートします。「[拡張範囲 VLAN の設定](#)」(P.14-11) を参照してください。

VLAN ID 1 ～ 1005 の設定はファイル *vlan.dat* (VLAN データベース) に書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。*vlan.dat* ファイルは、スタック マスター上のフラッシュ メモリに保存されます。スタック メンバーは、スタック マスターと一貫性のある *vlan.dat* ファイルを持ちます。



注意

vlan.dat ファイルを手動で削除しようとする、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応するコマンドリファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、[第 15 章「VTP の設定」](#)を参照してください。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行 コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ (イーサネット、Fiber Distributed Data Interface (FDDI)、FDDI Network Entity Title (NET)、TrBRF または TrCRF、トークンリング、トークンリング Net)
- VLAN ステート (アクティブまたはサスペンド)
- VLAN の Maximum Transmission Unit (MTU; 最大伝送ユニット)
- Security Association Identifier (SAID)
- Token Ring Bridge Relay Function (TrBRF; トークンリングブリッジリレー機能) VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- Token Ring Concentrator Relay Function (TrCRF; トークンリングコンセンレータリレー機能) VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Protocol (STP; スパニングツリープロトコル) タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号



(注)

ここでは、これらのパラメータの大部分の設定手順について説明しません。VLAN 設定を制御するコマンドおよびパラメータの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

ここでは、標準範囲 VLAN の設定情報について説明します。

- 「トークンリング VLAN」(P.14-6)
- 「標準範囲 VLAN 設定時の注意事項」(P.14-6)
- 「標準範囲 VLAN の設定」(P.14-7)
- 「イーサネット VLAN のデフォルト設定」(P.14-8)
- 「イーサネット VLAN の作成または変更」(P.14-8)
- 「VLAN の削除」(P.14-9)
- 「VLAN へのスタティック アクセス ポートの割り当て」(P.14-10)

トークンリング VLAN

このスイッチはトークンリング接続をサポートしていませんが、トークンリング接続を行っている Catalyst 5000 シリーズスイッチなどのリモート デバイスを、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼動しているスイッチは、次のトークンリング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

トークンリング VLAN の詳しい設定手順については、『*Catalyst 5000 Series Software Configuration Guide*』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- スイッチは、VTP クライアント、サーバ、および透過モードで 1005 VLAN をサポートします。
- 標準範囲 VLAN は、1 ~ 1001 の番号で識別します。VLAN 番号 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 専用です。
- VLAN 1 ~ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードが透過の場合、VTP および VLAN 設定はスイッチの実行コンフィギュレーション ファイルにも格納されます。
- VTP バージョン 1 およびバージョン 2 では、スイッチは VLAN 透過モード (VTP はディセーブル) のみ、VLAN ID 1006 ~ 4094 をサポートします。これらは拡張範囲 VLAN であり、設定オプションには制限があります。VTP 透過モードで作成した拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されることもありません。VTP バージョン 3 は、拡張範囲 VLAN (1006 ~ 4094 の VLAN) データベースの伝播をサポートします。拡張範囲 VLAN を設定していない場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。「[拡張範囲 VLAN の設定](#)」(P.14-11) を参照してください。
- VLAN を作成する前に、スイッチを VTP サーバモードまたは VTP 透過モードにしておく必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を伝播します。

- スイッチは 128 のスパニング ツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニング ツリー インスタンス数よりも多い場合、スパニング ツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニング ツリーはディセーブルになります。スイッチ上の使用可能なスパニング ツリー インスタンスをすべて使い切ってしまったあとに、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニング ツリーが稼動しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニング ツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

スイッチ上の VLAN の数がサポートされているスパニング ツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP (MSTP) を設定して、複数の VLAN を単一のスパニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 20 章「MSTP の設定」を参照してください。

- スタック内のスイッチが新たな VLAN を学習したか、既存の VLAN を（ネットワーク ポート上の VTP または CLI を通じて）削除または変更した場合は、VLAN 情報がすべてのスタック メンバーに通知されます。
- スイッチがスタックに加入したか、複数のスタックがマージされた場合、新規スイッチの VTP 情報（vlan.dat ファイル）はスタック マスターの VTP 情報と一貫性を維持します。

標準範囲 VLAN の設定

vlan グローバル コンフィギュレーション コマンドでは、VLAN ID を入力して VLAN を設定します。新しい VLAN ID を入力して VLAN を作成するか、既存の VLAN ID を入力してその VLAN を変更します。デフォルトの VLAN 設定を使用するか（表 14-2 を参照）、複数のコマンドを入力して VLAN を設定できます。このモードで使用できるコマンドの詳細については、このリリースのコマンドリファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。設定を終了したら、VLAN コンフィギュレーション モードを終了して、設定を有効にする必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN ID 1 ~ 1005 の設定は、常に VLAN データベース（vlan.dat ファイル）に保存されます。VTP モードが透過の場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに格納されません。**copy running-config startup-config** 特権 EXEC コマンドを使用して、スタートアップ コンフィギュレーション ファイルに設定を保存できます。スイッチ スタックでは、スタック全体で同一の vlan.dat ファイルと実行コンフィギュレーションを使用します。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードが透過で、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

- VTP バージョン 1 およびバージョン 2 は、VTP モードがサーバである場合、最初の 1005 個の VLAN のドメイン名および VLAN 設定だけに VLAN データベース情報を使用します。VTP バージョン 3 は、VLAN 1006 ~ 4094 もサポートします。

イーサネット VLAN のデフォルト設定

表 14-2 にイーサネット VLAN のデフォルト設定を示します。



(注) スイッチがサポートするのは、イーサネットインターフェイスだけです。FDDI およびトークンリング VLAN は、ローカルではサポートされないため、FDDI およびトークンリングメディア固有の特性は、他のスイッチに対する VTP グローバルアドバタイズだけに設定します。

表 14-2 イーサネット VLAN のデフォルト値および範囲

パラメータ	デフォルト値	範囲
VLAN ID	1	1 ~ 4094 (注) 拡張範囲 VLAN (VLAN ID 1006 ~ 4094) が VLAN データベースに保存されるのは、VTP バージョン 3 だけです。
VLAN 名	VLANxxxx。xxxx は VLAN ID 番号に等しい 4 桁の数字 (先行ゼロを含む) です。	範囲なし
IEEE 802.10 SAID	100001 (100000 と VLAN ID の和)	1 ~ 4294967294
MTU サイズ	1500	1500 ~ 18190
トランスレーショナルブリッジ 1	0	0 ~ 1005
トランスレーショナルブリッジ 2	0	0 ~ 1005
VLAN ステート	アクティブ	アクティブ、サスペンド
リモート SPAN	ディセーブル	イネーブル、ディセーブル
プライベート VLAN	設定なし	2 ~ 1001、1006 ~ 4094

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN には、1 ~ 1001 の 4 桁の一意的 ID が設定されています。VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。



(注) VTP バージョン 1 および 2 では、スイッチが VTP 透過モードである場合、1006 よりも大きい VLAN ID を割り当てることができますが、それらは VLAN データベースに追加されません。「[拡張範囲 VLAN の設定](#)」(P.14-11) を参照してください。

VLAN の追加時に指定されるデフォルトパラメータの一覧は、「[標準範囲 VLAN の設定](#)」(P.14-5) を参照してください。

イーサネット VLAN を作成または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan vlan-id</code>	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新しい VLAN ID を入力して VLAN を作成するか、既存の VLAN ID を入力してその VLAN を変更します。 (注) このコマンドで指定できる VLAN ID 範囲は 1 ~ 4094 です。1005 を超える VLAN ID (拡張範囲 VLAN) を追加する手順については、「 拡張範囲 VLAN の設定 」(P.14-11) を参照してください。
ステップ 3	<code>name vlan-name</code>	(任意) VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた <code>vlan-id</code> が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	<code>mtu mtu-size</code>	(任意) MTU サイズ (または他の VLAN 特性) を変更します。
ステップ 5	<code>remote-span</code>	(注) (任意) リモート Switched Port Analyzer (SPAN; スイッチドポート アナライザ) セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細は、 第 30 章「SPAN および RSPAN の設定」 を参照してください。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show vlan {name vlan-name id vlan-id}</code>	設定を確認します。
ステップ 8	<code>copy running-config startup config</code>	(任意) スイッチが VTP 透過モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN 名をデフォルトの設定に戻すには、`no name`、`no mtu`、または `no remote-span` コマンドを使用します。

次に、イーサネット VLAN 20 を作成し、`test20` という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP 透過モードのスイッチから VLAN を削除した場合、そのスイッチ スタック上に限り VLAN が削除されます。

メディア タイプが異なるデフォルトの VLAN を削除することはできません。たとえば、イーサネット VLAN 1、および FDDI またはトークン リング VLAN の 1002 ~ 1005 を削除することはできません。

**注意**

VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

スイッチ上で VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 no vlan <i>vlan-id</i>	VLAN ID を入力して、VLAN を削除します。
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show vlan brief	VLAN が削除されたことを確認します。
ステップ 5 copy running-config startup config	(任意) スイッチが VTP 透過モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって (VTP 透過モード)、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバー スイッチのポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバー スイッチにログインします。

**(注)**

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます（「イーサネット VLAN の作成または変更」(P.14-8) を参照）。

VLAN データベース内の VLAN にポートを割り当てるには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface <i>interface-id</i>	VLAN に追加するインターフェイスを入力します。
ステップ 3 switchport mode access	ポート (レイヤ 2 アクセス ポート) の VLAN メンバシップ モードを定義します。
ステップ 4 switchport access vlan <i>vlan-id</i>	VLAN にポートを割り当てます。有効な VLAN ID は 1 ~ 4094 です。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show running-config interface <i>interface-id</i>	インターフェイスの VLAN メンバシップ モードを確認します。
ステップ 7 show interfaces <i>interface-id</i> switchport	表示された <i>Administrative Mode</i> および <i>Access Mode VLAN</i> フィールドの設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

拡張範囲 VLAN の設定

VTP バージョン 1 およびバージョン 2 では、スイッチが VTP 透過モード (VTP がディセーブル) である場合、拡張範囲 VLAN (1006 ~ 4094) を作成できます。VTP バージョン 3 は、サーバ モードまたは透過モードで拡張範囲 VLAN をサポートします。サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている任意の **switchport** コマンドで使用できます。

VTP バージョン 1 または 2 では、拡張範囲 VLAN の設定は VLAN データベースには格納されません。ただし、VTP モードが透過であるため、スイッチの実行コンフィギュレーション ファイルに格納されます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 で作成した拡張範囲 VLAN は、VLAN データベースに格納されません。



(注)

スイッチは 4094 の VLAN ID をサポートしますが、実際にサポートされる VLAN の数については、「サポートされる VLAN」(P.14-3) を参照してください。

ここでは、拡張範囲 VLAN の設定情報について説明します。

- 「VLAN のデフォルト設定」(P.14-11)
- 「拡張範囲 VLAN 設定時の注意事項」(P.14-11)
- 「拡張範囲 VLAN の作成」(P.14-12)
- 「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.14-14)

VLAN のデフォルト設定

イーサネット VLAN のデフォルト設定については、表 14-2 (P.14-8) を参照してください。拡張範囲 VLAN については MTU サイズ、プライベート VLAN、およびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままではありません。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- スイッチで VTP バージョン 3 が稼動していないかぎり、拡張範囲の VLAN ID は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。

- VTP バージョン 1 および 2 で拡張範囲 VLAN を設定する場合は、スイッチを VTP 透過モードにする必要があります。VTP モードがサーバまたはクライアントの場合、エラー メッセージが生成され、拡張範囲 VLAN が拒否されます。VTP バージョン 3 は、サーバモードと透過モードで拡張 VLAN をサポートします。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで VTP モードを透過に設定できます。「[VTP モードの設定](#)」(P.15-12) を参照してください。VTP 透過モードでスイッチが起動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成すると、バージョン 1 または 2 に変換できません。
- 拡張範囲 VLAN では、STP はデフォルトでイネーブルになりますが、**no spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッチ上に最大数のスパンニング ツリー インスタンスが存在している場合に、VLAN を新規作成すると、この VLAN 上でスパンニング ツリーはディセーブルになります。スイッチ上の VLAN の数がスパンニング ツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s MSTP を設定して、複数の VLAN を単一のスパンニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、[第 20 章「MSTP の設定」](#) を参照してください。
- スイッチ上の各ルーテッド ポートは、内部 VLAN を使用するために作成します。この内部 VLAN は拡張範囲 VLAN 番号を使用し、その内部 VLAN ID は拡張範囲 VLAN には使用できません。内部 VLAN として割り当て済みの VLAN ID を指定して拡張範囲 VLAN を作成すると、エラー メッセージが生成され、コマンドは拒否されます。
 - 内部 VLAN ID は拡張範囲の下部の方なので、拡張範囲 VLAN を作成するには最大の番号 (4094) から始めて最小値 (1006) へと動いて、内部 VLAN ID を使用する可能性を減らすことを推奨します。
 - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、どの VLAN が内部 VLAN として割り当てられているかを確認します。
 - 必要に応じて内部 VLAN に割り当てられたルーテッド ポートをシャットダウンできます。これにより、内部 VLAN が解放され、拡張範囲 VLAN を作成してポートを再度イネーブルにし、別の VLAN を内部 VLAN として使用します。「[内部 VLAN ID を指定した拡張範囲 VLAN の作成](#)」(P.14-14) を参照してください。
- スイッチ スタックは合計 1005 (標準範囲および拡張範囲) の VLAN をサポートしますが、ルーテッド ポート、SVI、その他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。拡張範囲 VLAN を作成するときに、使用できるハードウェア リソースが不足していると、エラー メッセージが生成され、拡張範囲 VLAN が拒否されます。
- スイッチ スタックでは、スタック全体が同一の実行コンフィギュレーションと保存済みコンフィギュレーションを使用し、拡張範囲 VLAN 情報はスタック全体で共有されます。

拡張範囲 VLAN の作成

グローバル コンフィギュレーション モードで拡張範囲 VLAN を作成するには、**vlan** グローバル コンフィギュレーション コマンドを入力し、1006 ~ 4094 の VLAN ID を指定します。このコマンドによって **config-vlan** モードが開始されます。拡張範囲 VLAN はイーサネット VLAN のデフォルトの特性を備えており (表 14-2 を参照)、MTU サイズ、プライベート VLAN、RSPAN 設定だけが変更できるパラメータです。すべてのパラメータのデフォルト値については、コマンド リファレンスに記載された **vlan** グローバル コンフィギュレーション コマンドの説明を参照してください。VTP バージョン 1 または 2 では、スイッチが VTP 透過モードでない場合に拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラー メッセージが生成され、拡張範囲 VLAN が作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチの実行コンフィギュレーション ファイルに保存されます。拡張範囲 VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 では、拡張範囲 VLAN は VLAN データベースに保存されます。



(注) 拡張範囲 VLAN を作成する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、VLAN ID が内部的に使用されていないことを確認します。VLAN ID が内部的に使用されている場合に、それを解放するには、「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.14-14) を参照してから拡張範囲 VLAN を作成してください。

拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 vtp mode transparent	スイッチを VTP 透過モードに設定し、VTP をディセーブルにします。 (注) この手順は VTP バージョン 3 の場合は必要ありません。
ステップ 3 vlan vlan-id	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ~ 4094 です。
ステップ 4 mtu mtu-size	(任意) MTU サイズを変更して、VLAN を変更します。 (注) CLI ヘルプにはすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、 mtu mtu-size コマンド、 private-vlan コマンド、 remote-span コマンドだけです。
ステップ 5 remote-span	(任意) RSPAN VLAN として VLAN を設定します。「RSPAN VLAN としての VLAN の設定」(P.30-19) を参照してください。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show vlan id vlan-id	VLAN が作成されたことを確認します。
ステップ 8 copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、VTP 透過モード設定および拡張範囲 VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。 (注) VTP バージョン 3 では、VLAN の設定も VLAN データベースに保存されます。

拡張範囲 VLAN を削除するには、**no vlan vlan-id** グローバル コンフィギュレーション コマンドを使用します。

スタティック アクセス ポートを拡張範囲 VLAN に割り当てる手順は、標準範囲 VLAN の手順と同じです。「VLAN へのスタティック アクセス ポートの割り当て」(P.14-10) を参照してください。

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

内部 VLAN ID を指定した拡張範囲 VLAN の作成

内部 VLAN に割り当て済みの拡張範囲 VLAN ID を入力すると、エラーメッセージが生成され、拡張範囲 VLAN は拒否されます。内部 VLAN ID を手動で解放するには、内部 VLAN ID を使用しているルーテッドポートを一時的にシャットダウンする必要があります。

内部 VLAN に割り当てられた VLAN ID を解放してその ID で拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>show vlan internal usage</code>	スイッチが内部的に使用している VLAN ID を表示します。使用したい VLAN ID が内部 VLAN である場合は、その VLAN ID を使用しているルーテッドポートが表示されます。そのポート番号をステップ 3 で入力してください。
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>interface interface-id</code>	その VLAN ID を使用しているルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>shutdown</code>	ポートをシャットダウンして内部 VLAN ID を解放します。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>vtp mode transparent</code>	VTP モードを透過に設定して拡張範囲 VLAN を作成します。 (注) この手順は VTP バージョン 3 の場合は必要ありません。
ステップ 7	<code>vlan vlan-id</code>	新しい拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。
ステップ 8	<code>exit</code>	VLAN コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface interface-id</code>	ステップ 4 でシャットダウンしたルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	<code>no shutdown</code>	ルーテッドポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>copy running-config startup config</code>	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP 透過モード設定と拡張範囲 VLAN 設定を保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバモードになり、拡張範囲 VLAN ID は保存されません。 (注) VLAN は VLAN データベースに保存されるため、この手順は VTP バージョン 3 の場合は必要ありません。

VLAN の表示

拡張範囲 VLAN を含む、スイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。VLAN ステータス、ポート、および設定情報も表示されます。

表 14-3 に、VLAN をモニタするための特権 EXEC コマンドを示します。

表 14-3 VLAN モニタ コマンド

コマンド	目的
show interfaces [vlan <i>vlan-id</i>]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [id <i>vlan-id</i>]	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。

show コマンド オプションおよび出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VLAN トランクの設定

ここでは、次の概要について説明します。

- 「トランキングの概要」 (P.14-15)
- 「カプセル化タイプ」 (P.14-17)
- 「レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定」 (P.14-18)
- 「トランク ポートとしてのイーサネット インターフェイスの設定」 (P.14-19)
- 「トランク ポートの負荷分散の設定」 (P.14-23)

トランキングの概要

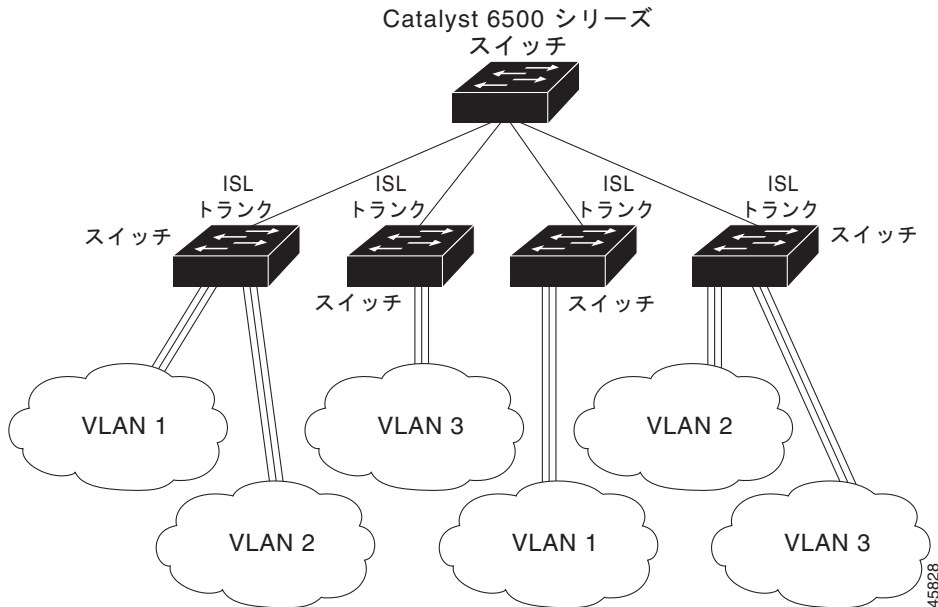
トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーク デバイス (ルータ、スイッチなど) の間のポイントツーポイント リンクです。イーサネット トランクは 1 つのリンクを介して複数の VLAN トラフィックを搬送するので、VLAN をネットワーク全体に拡張できます。

すべてのイーサネット インターフェイス上で、2 種類のトランキング カプセル化方式を使用できます。

- ISL : シスコ独自のトランキング カプセル化方式
- IEEE 802.1Q : 業界標準のトランキング カプセル化

図 14-2 に、ISL トランクで接続されているスイッチ ネットワークを示します。

図 14-2 ISL トランキング環境のスイッチ



トランクを設定できるのは、1つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。EtherChannel の詳細については、第 37 章「EtherChannel およびリンクステート トランキングの設定」を参照してください。

イーサネット トランク インターフェイスは、表 14-4 に示す トランキング モードをサポートしています。インターフェイスを トランキング または 非トランキング として設定したり、近接インターフェイスと トランキング のネゴシエーションを行ったりするように設定できます。トランキングの自動ネゴシエーションを行うには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、PPP (ポイントツーポイント プロトコル) である Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) によって管理されます。ただし、一部のイーサネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

この事態を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介して トランキング を行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへの トランキング をイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスが トランク になっても DTP フレームを生成しないように設定します。
switchport trunk encapsulation isl または **switchport trunk encapsulation dot1q** インターフェイスを使用して、トランク ポートのカプセル化タイプを選択します。

トランクに ISL カプセル化を使用させるのか、IEEE 802.1Q カプセル化を使用させるのか、それともカプセル化タイプの自動ネゴシエーションを行うのかを DTP インターフェイス上で指定することもできます。DTP は ISL トランク および IEEE 802.1Q トランク の両方の自動ネゴシエーションをサポートします。



(注) DTP はプライベート VLAN ポートまたはトンネル ポートではサポートされていません。

表 14-4 レイヤ 2 インターフェイス モード

モード	機能
<code>switchport mode access</code>	インターフェイス (アクセス ポート) を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、近接インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
<code>switchport mode dynamic auto</code>	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、近接インターフェイスが <i>trunk</i> または <i>desirable</i> モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは dynamic auto です。
<code>switchport mode dynamic desirable</code>	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、近接インターフェイスが <i>trunk</i> 、 <i>desirable</i> 、または <i>auto</i> モードに設定されている場合、トランク インターフェイスになります。
<code>switchport mode trunk</code>	インターフェイスを永続的なトランキング モードにして、近接リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、近接インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
<code>switchport nonegotiate</code>	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが access または trunk の場合だけ使用できます。トランク リンクを確立するには、手動で近接インターフェイスをトランク インターフェイスとして設定する必要があります。
<code>switchport mode dot1q-tunnel</code>	インターフェイスをトンネル (非トランキング) ポートとして設定し、IEEE 802.1Q トランク ポートと非対称リンクで接続されるようにします。IEEE 802.1Q トンネリングは、サービス プロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持するのに使用されます。トンネル ポートについての詳細は、 第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」 を参照してください。

カプセル化タイプ

表 14-5 に、イーサネット トランクのカプセル化タイプおよびキーワードを示します。

表 14-5 イーサネット トランクのカプセル化タイプ

カプセル化	機能
<code>switchport trunk encapsulation isl</code>	トランク リンクに ISL カプセル化を指定します。
<code>switchport trunk encapsulation dot1q</code>	トランク リンクに IEEE 802.1Q カプセル化を指定します。
<code>switchport trunk encapsulation negotiate</code>	インターフェイスが近接インターフェイスとネゴシエーションを行い、近接インターフェイスの設定および機能に応じて ISL トランク (優先) または IEEE 802.1Q トランクになるように指定します。これがスイッチのデフォルトです。



(注)

スイッチはレイヤ 3 トランクをサポートしません。したがって、サブインターフェイスを設定したり、レイヤ 3 インターフェイスで **encapsulation** キーワードを使用したりできません。ただし、スイッチは、同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

リンクが ISL トランクまたは IEEE 802.1Q トランクのどちらになるかは、接続された 2 つのインターフェイスのトランキング モード、トランク カプセル化タイプ、およびハードウェア機能によって決まります。

IEEE 802.1Q の設定に関する考慮事項

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続しているシスコ製スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニング ツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニング ツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続する場合、シスコ製スイッチは、トランクの VLAN のスパニング ツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニング ツリー インスタンスと結合します。ただし、各 VLAN のスパニング ツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離されたシスコ製スイッチによって維持されます。シスコ製スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニング ツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニング ツリーをディセーブルにせず、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニング ツリーをディセーブルにすると、スパニング ツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニング ツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニング ツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニング ツリーをディセーブルにしてください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 14-6 に、レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 14-6 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	switchport mode dynamic auto
トランク カプセル化	switchport trunk encapsulation negotiate
VLAN 許容範囲	VLAN 1 ~ 4094
ブルーニングに適格な VLAN 範囲	VLAN 2 ~ 1001
デフォルト VLAN (アクセス ポート用)	VLAN 1
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。

ここでは、次の設定情報について説明します。

- 「他の機能との相互作用」(P.14-19)
- 「トランクでの許可 VLAN の定義」(P.14-21)
- 「プルーニング適格リストの変更」(P.14-22)
- 「タグなしトラフィック用ネイティブ VLAN の設定」(P.14-23)



(注)

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルトモードは、**switchport mode dynamic auto** です。近接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ 2 トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。デフォルトでは、トランクはカプセル化のネゴシエーションを行います。近接インターフェイスが ISL および IEEE 802.1Q カプセル化をサポートしていて、なおかつ両方のインターフェイスがカプセル化タイプのネゴシエーションを行うように設定されている場合、トランクは ISL カプセル化を使用します。

他の機能との相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランク ポートはトンネル ポートにできません。
- トランク ポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかについて、設定を変更すると、入力した設定値がスイッチによってグループ内のすべてのポートに伝播されます。
 - 許可 VLAN リスト
 - 各 VLAN の STP ポート プライオリティ
 - STP PortFast の設定値
 - ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- PVST モードで設定するトランク ポートの数は 24 まで、MST モードで設定するトランク ポートの数は 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1X をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1X をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートをダイナミックに変更しようとしても、ポート モードは変更されません。

トランク ポートの設定

ポートをトランク ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートする、またはカプセル化タイプについて近接インターフェイスとネゴシエーションを行う（デフォルト）ようにポートを設定します。 同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 4	<code>switchport mode {dynamic {auto desirable} trunk}</code>	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります）。 <ul style="list-style-type: none"> • dynamic auto : 近接インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これがデフォルトです。 • dynamic desirable : 近接インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • trunk : 近接インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	<code>switchport access vlan vlan-id</code>	(任意) インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 6	<code>switchport trunk native vlan vlan-id</code>	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show interfaces interface-id switchport</code>	インターフェイスのスイッチポート設定を表示します。 <i>Administrative Mode</i> および <i>Administrative Trunking Encapsulation</i> フィールドに表示されます。
ステップ 9	<code>show interfaces interface-id trunk</code>	インターフェイスのトランク設定を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。トランキング インターフェイスのすべてのトランキング特性をデフォルトにリセットするには、**no switchport trunk** インターフェイス コンフィギュレーション コマンドを使用します。トランキングをディセーブルにするには、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、ポートをスタティック アクセス ポートとして設定します。

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、近接インターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# end
```

トランクでの許可 VLAN の定義

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID (1 ~ 4094) が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。トランクが伝送するトラフィックを制限するには、**switchport trunk allowed vlan remove vlan-list** インターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除します。



(注)

VLAN 1 は、すべてのシスコ製スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック (スパニング ツリー アドバタイズなど) は VLAN 1 で送受信されなくなります。

スパニング ツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol (CDP)、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバーになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバーになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバーにはなりません。

トランクの許可リストを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。

■ VLAN トランクの設定

コマンド	目的
ステップ 4 switchport trunk allowed vlan {add all except remove} vlan-list	(任意) トランク上で許可される VLAN のリストを設定します。 add 、 all 、 except 、および remove キーワードの使用方法については、このリリースに対応するコマンドリファレンスを参照してください。 <i>vlan-list</i> パラメータは、1 ~ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号 (小さい方が先、ハイフンで区切る) で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れないでください。 デフォルトでは、すべての VLAN が許可されます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show interfaces interface-id switchport	表示された <i>Trunking VLANs Enabled</i> フィールドの設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN の許可 VLAN リストをデフォルトに戻すには、**no switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに専用の適格リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。VTP プルーニングをイネーブルにする方法については、「[VTP プルーニングのイネーブル化](#)」(P.15-16) を参照してください。

トランク ポートのプルーニング適格リストから VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 switchport trunk pruning vlan {add except none remove} vlan-list [,vlan[,vlan[,...]]]	トランクからのプルーニングを許可する VLAN のリストを設定します (「VTP プルーニング」 (P.15-6) を参照)。 add 、 except 、 none 、および remove キーワードの使用方法については、このリリースに対応するコマンドリファレンスを参照してください。 連続していない VLAN ID は、カンマ (スペースなし) で区切ります。ID の範囲はハイフンで指定します。有効な VLAN ID は 2 ~ 1001 です。拡張範囲 VLAN (VLAN ID 1006 ~ 4094) はプルーニングできません。 プルーニング不適格の VLAN は、フラッドイング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ~ 1001 が含まれます。
ステップ 4 end	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 5 show interfaces interface-id switchport	表示された <i>Pruning VLANs Enabled</i> フィールドの設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

すべての VLAN のプルーンング適格リストをデフォルトに戻すには、**no switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。ネイティブ VLAN は、デフォルトでは VLAN 1 です。



(注) ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定についての詳細は、「[IEEE 802.1Q の設定に関する考慮事項](#)」(P.14-18) を参照してください。

IEEE 802.1Q トランクでネイティブ VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 switchport trunk native vlan vlan-id	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show interfaces interface-id switchport	<i>Trunking Native Mode VLAN</i> フィールドの設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ネイティブ VLAN をデフォルト (VLAN 1) に戻すには、**no switchport trunk native vlan** インターフェイス コンフィギュレーション コマンドを使用します。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

トランク ポートの負荷分散の設定

負荷分散により、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リンクを同じスイッチに接続する必要があります。STP パス コストを使用して負荷分散を設定する場合には、それぞれの負荷分散リンクを同一のスイッチにも、2 台の異なるスイッチにも接続できます。STP の詳細については、第 19 章「STP の設定」を参照してください。

STP ポート プライオリティによる負荷分散

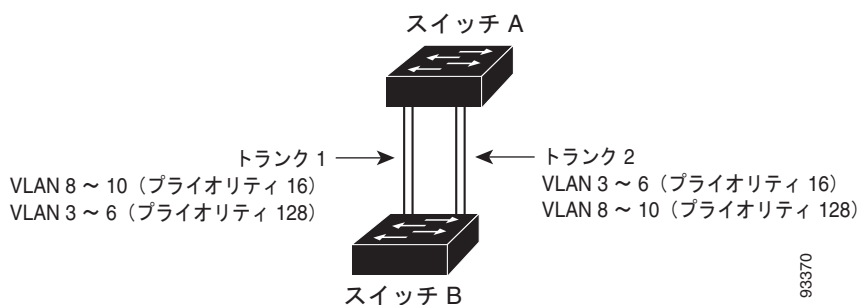
同一スイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

図 14-3 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ~ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ~ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ~ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ~ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ~ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ~ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。

図 14-3 STP ポート プライオリティによる負荷分散



(注)

スイッチがスイッチ スタックのメンバーの場合は、`spanning-tree [vlan vlan-id] port-priority priority` インターフェイス コンフィギュレーション コマンドの代わりに、`spanning-tree [vlan vlan-id] cost cost` インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させたいインターフェイスには小さいコスト値を、最後に選択させたいインターフェイスには大きいコスト値を割り当てます。詳細については、「STP パス コストによる負荷分散」(P.14-26)を参照してください。

図 14-3 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp domain domain-name</code>	VTP 管理ドメインを設定します。 1 ~ 32 文字のドメイン名を使用できます。
ステップ 3	<code>vtp mode server</code>	スイッチ A を VTP サーバとして設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show vtp status</code>	スイッチ A および B の両方で、VTP 設定を確認します。 表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドをチェックします。
ステップ 6	<code>show vlan</code>	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 7	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 8	<code>interface interface-id_1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートする、または近接インターフェイスとネゴシエーションを行うようにポートを設定します。同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 10	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show interfaces interface-id_1 switchport</code>	VLAN 設定を確認します。
ステップ 13		スイッチ スタックの別のポートについて、スイッチ A でステップ 7 ~ 11 を実行します。
ステップ 14		スイッチ B でステップ 7 ~ 11 を繰り返し、スイッチ A で設定されたトランク ポートに接続するトランク ポートを設定します。
ステップ 15	<code>show vlan</code>	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 16	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 17	<code>interface interface-id_1</code>	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	<code>spanning-tree vlan 8-10 port-priority 16</code>	VLAN 8 ~ 10 にポート プライオリティ 16 を割り当てます。
ステップ 19	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 20	<code>interface interface-id_2</code>	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	<code>spanning-tree vlan 3-6 port-priority 16</code>	VLAN 3 ~ 6 にポート プライオリティ 16 を割り当てます。
ステップ 22	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 23	<code>show running-config</code>	設定を確認します。
ステップ 24	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

STP パス コストによる負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

図 14-4 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2 ~ 4 は、トランク ポート 1 で 30 というパス コストが割り当てられています。
- VLAN 8 ~ 10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8 ~ 10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2 ~ 4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コストである 19 のままです。

図 14-4 パス コストによってトラフィックが分散される負荷分散トランク

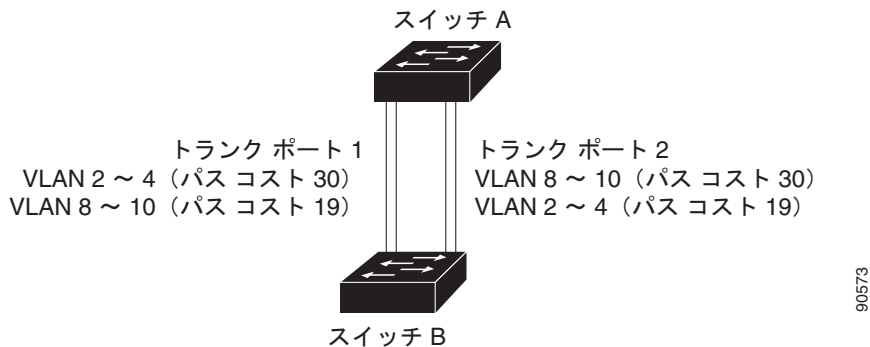


図 14-4 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	スイッチ A で、グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id_1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートするようにポートを設定します。同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 4	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。トランクのデフォルトは ISL トランキングです。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6		スイッチ A のスタック内の別のインターフェイスでステップ 2 ~ 5 を繰り返します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。

	コマンド	目的
ステップ 9	<code>show vlan</code>	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。スイッチ A が VLAN 設定を学習したことを確認します。
ステップ 10	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 11	<code>interface interface-id_1</code>	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	<code>spanning-tree vlan 2-4 cost 30</code>	VLAN 2 ~ 4 のスパニング ツリー パス コストを 30 に設定します。
ステップ 13	<code>end</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 14		スイッチ A に設定したもう一方のトランク インターフェイスで、ステップ 9 ~ 13 を繰り返し、VLAN 8、9、および 10 のスパニング ツリー パス コストを 30 に設定します。
ステップ 15	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 16	<code>show running-config</code>	設定を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 17	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VMPS の設定

VLAN Query Protocol (VQP) は、ダイナミック アクセス ポートをサポートする場合に使用します。ダイナミック アクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC 送信元アドレスに基づいて VLAN を割り当てます。未知の MAC アドレスが検出されるたびに、スイッチはリモート VMPS に VQP クエリーを送信します。クエリーには新たに検出された MAC アドレスとそのアドレスを検出したポートが含まれます。VMPS はそのポートの VLAN 割り当てで応答します。このスイッチを VMPS サーバにすることはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信できます。

ここでは、次の情報について説明します。

- 「VMPS の概要」 (P.14-27)
- 「VMPS クライアントのデフォルト設定」 (P.14-29)
- 「VMPS 設定時の注意事項」 (P.14-29)
- 「VMPS クライアントの設定」 (P.14-30)
- 「VMPS のモニタリング」 (P.14-32)
- 「ダイナミック アクセス ポート VLAN メンバシップのトラブルシューティング」 (P.14-33)
- 「VMPS の設定例」 (P.14-33)

VMPS の概要

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを送信します。このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピングを検索します。サーバの応答は、このマッピングと、サーバがオープン モードかセキュア モードかに基づいて行われます。セキュア モードの場合、サーバは不正なホストが検出されると、ポートをシャットダウンします。オープン モードでは、サーバはホストに対してポート アクセスを拒否するだけです。

ポートが未割り当ての場合（つまり、VLAN 割り当てがまだ設定されていない場合）、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホストへのアクセスを許可する *VLAN 割り当て* 応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS は *アクセス拒否* 応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS は *ポートシャットダウン* 応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は *成功* 応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、*アクセス拒否* または *ポートシャットダウン* 応答を送信します。

VMPS から *アクセス拒否* 応答を受信した場合、スイッチはそのホスト MAC アドレスのトラフィックを双方向で引き続きブロックします。スイッチはポート宛の packets を引き続きモニタし、新しいホストアドレスを検出すると VMPS にクエリーを送信します。VMPS から *ポートシャットダウン* 応答を受信した場合、スイッチはそのポートをディセーブルにします。Network Assistant、CLI（コマンドラインインターフェイス）、または SNMP（簡易ネットワーク管理プロトコル）を使用して、ポートを手動で再びイネーブルにする必要があります。

ダイナミック アクセス ポート VLAN メンバシップ

ダイナミック アクセス ポートが所属できるのは、VLAN ID が 1 ~ 4094 の 1 つの VLAN だけです。リンクがアップになっても、VMPS によって VLAN が割り当てられるまで、このポートとの間でトラフィック転送は行われません。VMPS は、ダイナミック アクセス ポートに接続した新しいホストの最初の packet から送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレスを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。クライアントスイッチがまだ設定されていない場合は、スイッチは VMPS からトランク ポートで受信した最初の VTP packet からドメイン名を使用します。クライアントスイッチがすでに設定されている場合は、クエリー packet にスイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。VMPS は packet 内のドメイン名が自身のドメイン名と一致することを確認したあと、要求を受け入れ、クライアントに割り当てられた VLAN 番号を応答します。一致しない場合、(VMPS セキュア モードの設定に応じて) VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミック アクセス ポート上で複数のホスト (MAC アドレス) をアクティブにできますが、それらのホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数が 20 を超えると、VMPS はダイナミック アクセス ポートをシャットダウンします。

ダイナミック アクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、VLAN の所属から外れます。ポート経由でオンラインになるホストは VMPS によって VQP 経由で再チェックされてから、ポートが VLAN に割り当てられます。

ダイナミック アクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。スイッチ上のポートごとに、最大 20 の MAC アドレスを使用できます。ダイナミック アクセス ポートが一度に所属できる VLAN は 1 つですが、VLAN は検出された MAC アドレスに基づいてあとで変更されることがあります。

VMPS クライアントのデフォルト設定

表 14-7 に、クライアント スイッチ上の VMPS およびダイナミック アクセス ポートのデフォルト設定を示します。

表 14-7 VMPS クライアントおよびダイナミック アクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミック アクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミック アクセス ポート VLAN メンバシップには、次の注意事項および制限事項があります。

- VMPS を設定してから、ポートをダイナミック アクセス ポートとして設定する必要があります。
- ポートをダイナミック アクセス ポートとして設定すると、そのポートに対してスパンニング ツリーの PortFast 機能が自動的にイネーブルになります。PortFast モードにより、ポートをフォワーディング ステートに移行させるプロセスが短縮されます。
- IEEE 802.1X ポートをダイナミック アクセス ポートとして設定することはできません。ダイナミック アクセス (VQP) ポートで IEEE 802.1X をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートをダイナミック アクセス ポートにすることはできませんが、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力することは可能です。その場合、スイッチの設定は維持され、あとにアクセス ポートとして設定された場合には、その設定が適用されます。

ダイナミック アクセス設定を有効にするには、ポート上でトランキングをオフにしておく必要があります。

- ダイナミック アクセス ポートをモニタ ポートにすることはできません。
- セキュア ポートをダイナミック アクセス ポートにすることはできません。ポートをダイナミックにするには、ポート上でポート セキュリティをディセーブルにしておく必要があります。
- プライベート VLAN をダイナミック アクセス ポートにすることはできません。
- ダイナミック アクセス ポートを EtherChannel グループのメンバーにすることはできません。
- ポート チャンネルをダイナミック アクセス ポートとして設定することはできません。
- ダイナミック アクセス ポートは、フォールバック ブリッジングに加入できます。
- VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。
- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。

VMPS クライアントの設定

ダイナミック VLAN を設定するには、VMPS (サーバ) を使用します。スイッチを VMPS クライアントにすることはできますが、VMPS サーバにすることはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。



(注)

スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

VMPS の IP アドレスを入力するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vmips server ipaddress primary</code>	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	<code>vmips server ipaddress</code>	(任意) セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show vmips</code>	表示された <i>VMPS Domain Server</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

ダイナミック アクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。IP 接続が可能かどうかをテストするには、VMPS の IP アドレスに ping を実行し、応答が得られるかどうかを確認します。

VMPS クライアント上のダイナミック アクセス ポートの設定

クラスタ メンバー スイッチのポートをダイナミック アクセス ポートとして設定するには、最初に `rcommand` 特権 EXEC コマンドを使用して、そのクラスタ メンバー スイッチにログインします。



注意

ダイナミックアクセス ポート VLAN メンバシップはエンドステーション用、またはエンドステーションに接続されたハブ用です。他のスイッチにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。

VMPS クライアント スイッチにダイナミック アクセス ポートを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	エンド ステーションに接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 switchport mode access	ポートをアクセス モードにします。
ステップ 4 switchport access vlan dynamic	ポートをダイナミック VLAN メンバシップ適格として設定します。 ダイナミック アクセス ポートは、エンド ステーションに接続されている必要があります。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show interfaces interface-id switchport	表示された <i>Operational Mode</i> フィールドの設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスをデフォルトのスイッチポート モード (dynamic auto) に戻すには、**no switchport mode** インターフェイス コンフィギュレーション コマンドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、**no switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用します。

VLAN メンバシップの再確認

スイッチが VMPS から受信したダイナミック アクセス ポート VLAN メンバシップの割り当てを確認するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 vmmps reconfirm	ダイナミック アクセス ポート VLAN メンバシップを再確認します。
ステップ 2 show vmmps	ダイナミック VLAN の再確認ステータスを確認します。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信する VLAN メンバシップの情報を定期的に再確認します。再確認を実行する間隔は数字を使用して分単位で設定できます。

クラスタのメンバー スイッチを設定する場合、このパラメータはコマンド スイッチの再確認インターバルの設定値以上でなければなりません。メンバー スイッチにログインするには、最初に **rcommand** 特権 EXEC コマンドを使用する必要があります。

再確認インターバルを変更するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 vmmps reconfirm minutes	ダイナミック VLAN メンバシップの再確認を行う間隔 (分) を入力します。指定できる範囲は 1 ~ 120 です。デフォルト値は 60 分です。
ステップ 3 end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<code>show vmps</code>	表示された <i>Reconfirm Interval</i> フィールドのダイナミック VLAN の再確認ステータスを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチのデフォルト設定に戻すには、`no vmps reconfirm` グローバル コンフィギュレーション コマンドを使用します。

再試行回数の変更

スイッチが次のサーバにクエリーを送信する前に、VMPS との接続を試行する回数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vmps retry count</code>	再試行の回数を変更します。指定できる再試行回数の範囲は 1 ~ 10 です。デフォルトは 3 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show vmps</code>	表示された <i>Server Retry Count</i> フィールドの設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチのデフォルト設定に戻すには、`no vmps retry` グローバル コンフィギュレーション コマンドを使用します。

VMPS のモニタリング

`show vmps` 特権 EXEC コマンドを使用して、VMPS に関する情報を表示できます。スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP バージョン：VMPS との通信に使用する VQP のバージョン。スイッチは VQP バージョン 1 を使用する VMPS にクエリーを送信します。
- 再確認インターバル：スイッチが VLAN と MAC アドレスの割り当てを再確認する間隔 (分)。
- サーバ再試行回数：VQP が VMPS にクエリーを再送信する回数。この回数すべてを試行しても応答が得られない場合、スイッチはセカンダリ VMPS へのクエリーを開始します。
- VMPS ドメイン サーバ：設定されている VLAN メンバシップ ポリシー サーバの IP アドレス。スイッチは *current* と表示されているサーバにクエリーを送信します。*primary* と表示されているサーバは、プライマリ サーバです。
- VMPS 動作：最新の再確認の結果。再確認は、再確認インターバルが経過したときに自動的に行われますが、`vmps reconfirm` 特権 EXEC コマンドを入力するか、Network Assistant または SNMP で同等の操作を行うことによって、強制的に再確認することもできます。

次に、`show vmps` 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
```

```
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                   172.20.128.87

Reconfirmation status
-----
VMPS Action:          other
```

ダイナミック アクセス ポート VLAN メンバシップのトラブルシューティング

VMPS は次の状況でダイナミック アクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、なおかつホストのポートへの接続を許可しない場合。VMPS はポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- ダイナミック アクセス ポート上のアクティブ ホストが 20 を超えた場合。

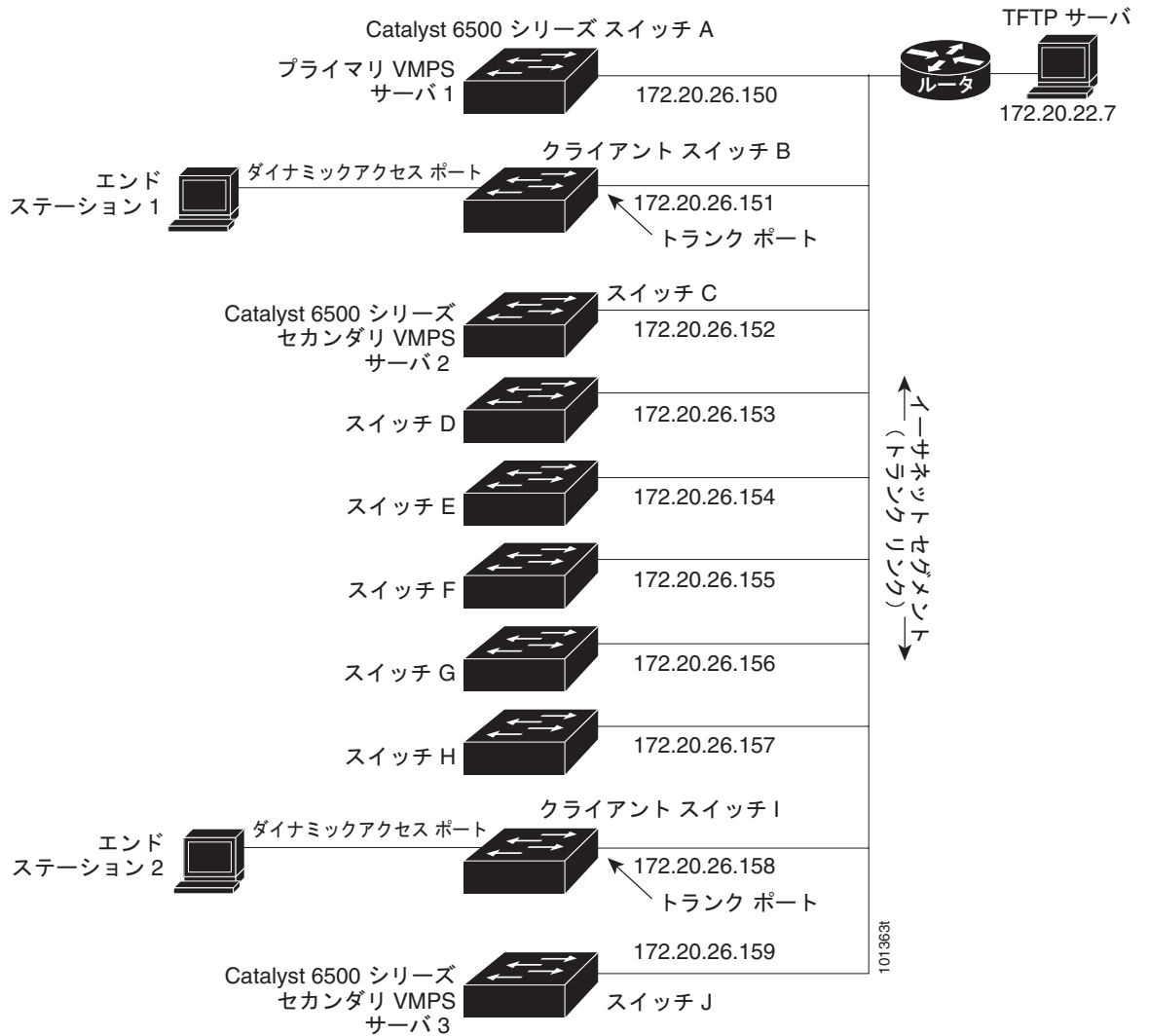
ディセーブルにされているダイナミック アクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の設定例

図 14-5 に、VMPS サーバスイッチと、ダイナミック アクセス ポートを備えた VMPS クライアントスイッチが含まれるネットワークの例を示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンドステーションはクライアント（スイッチ B、スイッチ I）に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。

図 14-5 ダイナミック ポート VLAN メンバシップの構成例





CHAPTER 15

VTP の設定

この章では、Catalyst 3750 スイッチで、VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) および VLAN データベースを使用して VLAN を管理する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

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

この章で説明する内容は、次のとおりです。

- 「VTP の概要」 (P.15-1)
- 「VTP の設定」 (P.15-8)
- 「VTP のモニタ」 (P.15-19)

VTP の概要

VTP は、レイヤ 2 のメッセージプロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN 情報を他のスイッチに送信できません。

VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

VTP 機能はスタック全体にわたってサポートされ、スタック内のすべてのスイッチがスタック マスターから継承した同一の VLAN および VTP コンフィギュレーションを維持します。スイッチが VTP メッセージを介して新たな VLAN について学習した場合、または新たな VLAN がユーザによって設定された場合は、新たな VLAN の情報がスタック内のすべてのスイッチへ通知されます。

スイッチがスタックに加入した場合、または複数のスタックがマージされた場合、新たなスイッチはスタック マスターから VTP 情報を取得します。

スイッチは 1005 の VLAN をサポートしますが、ルーテッドポート、SVI、およびその他の設定済み機能の数によって、スイッチハードウェアの使用が左右されます。VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限のハードウェアリソースをすでに使用している場合、スイッチはハードウェアリソース不足を伝えるメッセージを送信して、VLAN をシャットダウンします。show vlan ユーザ EXEC コマンドの出力に、サスペンドステートの VLAN が示されます。

VTP バージョン 1 およびバージョン 2 は、標準範囲 VLAN (VLAN ID が 1 ~ 1005) だけをサポートします。Cisco IOS Release 12.2(52)SE 以降のリリースは、VTP バージョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体 (1 ~ 4094 の VLAN) をサポートします。拡張範囲 VLAN (1006 ~ 4094 の VLAN) は、VTP バージョン 3 だけでサポートされます。ドメイン内で拡張 VLAN を設定している場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

ここでは、次の概要について説明します。

- 「VTP ドメイン」 (P.15-2)
- 「VTP モード」 (P.15-3)
- 「VTP アドバタイズ」 (P.15-4)
- 「VTP バージョン 2」 (P.15-5)
- 「VTP バージョン 3」 (P.15-5)
- 「VTP プルーニング」 (P.15-6)
- 「VTP とスイッチスタック」 (P.15-8)

VTP ドメイン

VTP ドメイン (別名 VLAN 管理ドメイン) は、1 つのスイッチ、または同じ VTP ドメイン名を共有している、同一管理下にある相互接続された複数のスイッチまたはスイッチスタックで構成されます。スイッチは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランクリンク (複数 VLAN のトラフィックを伝送するリンク) を介してドメインについてのアドバタイズを受信しないかぎり、またはユーザがドメイン名を設定しないかぎり、スイッチは VTP 非管理ドメインステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播されません。

スイッチがトランクリンクを介して VTP アドバタイズを受信すると、スイッチは管理ドメイン名および VTP コンフィギュレーションリビジョン番号を継承します。そのあとスイッチは、別のドメイン名または古いコンフィギュレーションリビジョン番号が指定されたアドバタイズについては、すべて無視します。



注意

VTP クライアントスイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーションリビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーションリビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーションリビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよび VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP コンフィギュレーションリビジョン番号の確認手順およびリセット手順については、「VTP ドメインへの VTP クライアントスイッチの追加」 (P.15-17) を参照してください。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播されます。VTP アドバタイズは、ISL (スイッチ間リンク)、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負担が大幅に軽減されます。

VTP 透過モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッチに限られます。ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレーション ファイルに保存することもできます。

ドメイン名およびパスワードの設定時の注意事項については、「[VTP 設定時の注意事項](#)」(P.15-9) を参照してください。

VTP モード

サポート対象のスイッチ スタックを、[表 15-1](#) に示す VTP モードのいずれかに設定できます。

表 15-1 VTP モード

VTP モード	説明
VTP サーバ	<p>VTP サーバモードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ (VTP バージョンなど) を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。</p> <p>VTP サーバモードがデフォルトの設定です。</p> <p>(注) VTP サーバモードでは、VLAN 設定は NVRAM に保存されます。設定を NVRAM に書き込んでいる間に障害を検出すると、スイッチはサーバモードから VTP クライアントモードに自動的に移行します。その場合、スイッチは NVRAM が機能するまで VTP サーバモードに戻ることができません。</p>
VTP クライアント	<p>VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバモードのスイッチで設定します。</p> <p>VTP バージョン 1 および 2 の場合、VTP クライアントモードでは、VLAN 設定は NVRAM に保存されません。VTP バージョン 3 の場合、VLAN 設定はクライアントモードで NVRAM に保存されます。</p>

表 15-1 VTP モード (続き)

VTP モード	説明
VTP トランスペアレント	<p>VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP 透過モードでは、スイッチ上の VLAN を作成、変更、削除できます。</p> <p>VTP バージョン 1 および 2 で拡張範囲 VLAN を設定する場合は、スイッチを VTP 透過モードにする必要があります。VTP バージョン 3 は、クライアント モードまたはサーバ モードで拡張範囲 VLAN の作成もサポートします。「拡張範囲 VLAN の設定」(P.14-11) を参照してください。</p> <p>VTP バージョン 1 およびバージョン 2 では、プライベート VLAN を作成したり、設定したりする場合に VTP モードを透過モードからクライアント モードまたはサーバ モードに変更しないでください。VTP バージョン 3 は、クライアント モードとサーバ モードでプライベート VLAN をサポートします。第 17 章「プライベート VLAN の設定」 を参照してください。</p> <p>スイッチが VTP 透過モードの場合、VTP および VLAN の設定は NVRAM に保存されますが、他のスイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。実行コンフィギュレーションと保存済みコンフィギュレーションは、スタック内のすべてのスイッチで同一です。</p>
VTP オフ	<p>VTP オフ モードのスイッチは VTP トランスペアレント スイッチと同様に機能しますが、トランク上で VTP アドバタイズを転送しません。</p>

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的送信します。このようなアドバタイズを受信した近接スイッチは、必要に応じて各自の VTP および VLAN 設定をアップデートします。



(注)

トランク ポートは VTP アドバタイズを送受信するので、スイッチ スタック上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。トランク ポートの詳細については「[VLAN トランクの設定](#)」(P.14-15) を参照してください。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP コンフィギュレーション リビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズを含む MD5 ダイジェスト VLAN コンフィギュレーション
- フレーム フォーマット

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID (ISL および IEEE 802.1Q)
- VLAN 名

- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズは、プライマリ サーバ ID、インスタンス番号、および開始インデックスも含まれます。

VTP バージョン 2

ネットワークで VTP を使用する場合は、使用する VTP のバージョンを決定する必要があります。デフォルトでは、バージョン 1 の VTP が動作します。

バージョン 2 は、VTP バージョン 1 ではサポートされない次の機能をサポートします。

- トークン リング サポート：VTP バージョン 2 は、Token Ring Bridge Relay Function (TrBRF; トークン リングブリッジリレー機能) および Token Ring Concentrator Relay Function (TrCRF; トークン リング コンセントレータリレー機能) VLAN をサポートします。トークン リング VLAN の詳細については、「標準範囲 VLAN の設定」(P.14-5) を参照してください。
- 認識不能な Type-Length-Value (TLV) のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバモードで動作している場合、NVRAM に保存されます。
- バージョン依存型透過モード：VTP バージョン 1 の場合、VTP トランスペアレントスイッチが VTP メッセージ中のドメイン名およびバージョンを検査し、バージョンおよびドメイン名が一致する場合にかぎりメッセージを転送します。VTP バージョン 2 ではドメインが 1 つしかサポートされないため、透過モードの場合はバージョンやドメイン名を検査せずに VTP メッセージを転送します。
- 整合性検査：VTP バージョン 2 の場合、CLI (コマンドライン インターフェイス)、または SNMP (簡易ネットワーク管理プロトコル) を介して新しい情報が入力された場合にかぎり、VLAN 整合性検査 (VLAN 名、値など) を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン 3

バージョン 3 は、VTP バージョン 1 またはバージョン 2 ではサポートされない次の機能をサポートします。

- 拡張認証：認証を **hidden** または **secret** として設定できます。**hidden** の場合、パスワードストリングから生成された秘密鍵は VLAN データベース ファイルには保存されますが、コンフィギュレーションにプレーンテキストで表示されません。その代わりに、パスワードに関連付けられている鍵が 16 進形式で実行コンフィギュレーションに保存されます。ドメイン内でテイクオーバーコマンドを入力した場合は、パスワードを再入力する必要があります。**secret** キーワードを入力した場合は、パスワードの秘密鍵を直接設定できます。
- 拡張範囲 VLAN (1006 ~ 4094 の VLAN) データベース伝播のサポート。VTP バージョン 1 および 2 では、VLAN 1 ~ 1005 だけが伝播されます。拡張範囲 VLAN を設定していない場合は、VTP バージョン 3 からバージョン 1 または 2 に変換できません。



(注) VTP プルーニングは、引き続き VLAN 1 ~ 1005 だけに適用されます。VLAN 1002 ~ 1005 は引き続き予約されているため、変更できません。

- プライベート VLAN のサポート。
- ドメイン内の任意のデータベースのサポート。バージョン 3 では、VTP 情報の伝播に加えて、Multiple Spanning Tree (MST) プロトコル データベース情報を伝播できます。VTP を使用するアプリケーションごとに、個別の VTP プロトコル インスタンスが実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ。VTP プライマリ サーバは、データベース情報を更新し、システムのすべてのデバイスによって採用されるアップデートを送信します。VTP セカンダリ サーバは、NVRAM で受信したプライマリ サーバからの更新済み VTP コンフィギュレーションをバックアップできるだけです。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして稼働します。vtp primary 特権 EXEC コマンドを入力してプライマリ サーバを指定できます。プライマリ サーバ ステータスは、管理者がドメイン内でテイクオーバー メッセージを発行する場合のデータベース更新のためだけに必要です。VTP ドメインは、プライマリ サーバを使用せずに動作させることができます。スイッチでパスワードを設定している場合でも、デバイスのリロードまたはドメイン パラメータの変更が行われると、プライマリ サーバ ステータスが失われます。

- トランク単位 (ポート単位) で VTP のオン/オフを切り替えるためのオプション。[no] vtp インターフェイス コンフィギュレーション コマンドを入力すると、VTP をポート単位でイネーブルまたはディセーブルにできます。トランキング ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。MST データベースに対して VTP をオフに設定した場合は、同じポート上の VLAN データベースに対して VTP をオンに設定できません。

VTP モードをグローバルにオフにすると、システムのすべてのトランキング ポートに同じ設定が適用されます。ただし、VTP インスタンス単位でオン/オフを指定することもできます。たとえば、スイッチを VLAN データベースの VTP サーバとして設定する一方で、MST データベースに対しては VTP をオフに設定することができます。

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクへのフラッドイング トラフィックが制限されるので、使用可能なネットワーク帯域幅が増えます。VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、および不明のユニキャスト トラフィックをフラッドイングします。VTP プルーニングはデフォルトでディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッドイング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、スイッチのトランク ポート上で VLAN 2 ~ 1001 がプルーニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッドイングが行われます。VTP プルーニングは、すべての VTP バージョンでサポートされています。

図 15-1 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A は、このブロードキャストをフラッドイングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク内のすべてのスイッチがこのブロードキャストを受信します。

図 15-1 VTP プルーニングを使用しない場合のフラッディング トラフィック

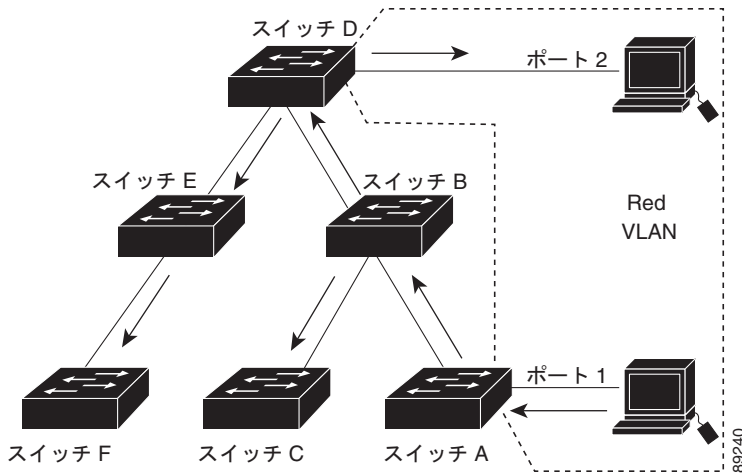
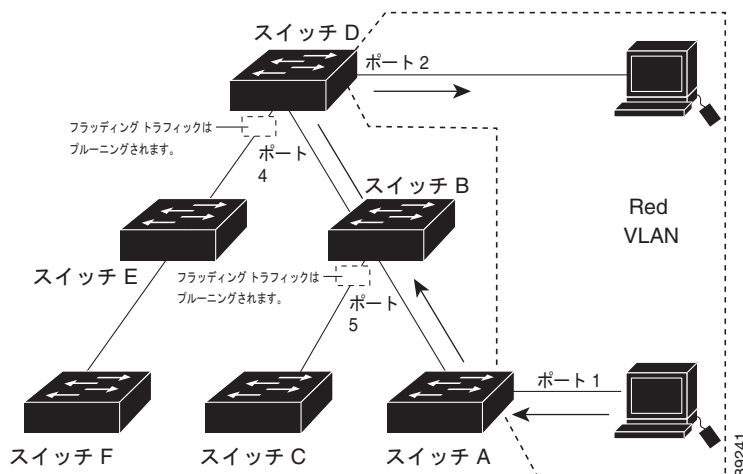


図 15-2 に、VTP プルーニングをイネーブルに設定したスイッチド ネットワークを示します。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されているリンク ポート（スイッチ B のポート 5、およびスイッチ D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。

図 15-2 VTP プルーニングによるフラッディング トラフィックの最適化



VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのリンク上の VLAN のプルーニングだけです（VTP ドメイン内のすべてのスイッチに影響するわけではありません）。

「VTP プルーニングのイネーブル化」(P.15-16) を参照してください。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 および VLAN 1002 ~ 1005 は常にプルーニング不適格です。これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN（1005 を超える VLAN ID）もプルーニング不適格です。

VTP プルーニングは VTP 透過モードでは機能しないように設計されています。ネットワーク内に VTP 透過モードのスイッチが 1 台または複数存在する場合は、次のいずれかを実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** インターフェイス コンフィギュレーション コマンドを使用します（「[プルーニング適格リストの変更](#)」(P.14-22) を参照）。VTP プルーニングは、インターフェイスがトランッキングを実行している場合に作用します。VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特定の VLAN が存在するかどうか、およびインターフェイスが現在トランッキングを実行しているかどうかにかかわらず、設定できます。

VTP とスイッチ スタック

VTP 設定は、スイッチ スタック内のすべてのメンバーで同一です。スイッチ スタックが VTP サーバモードまたは VTP クライアント モードの場合は、スタック内のすべてのスイッチが同一の VTP 設定を実行します。VTP モードが透過またはオフの場合は、スタックは VTP には加入しません。

- スイッチがスタックに加入した場合は、スタック マスターの VTP および VLAN 特性を継承します。
- すべての VTP アップデートがスタック全体にわたり搬送されます。
- スタック内のスイッチで VTP モードが変更されると、スタック内の他のスイッチも VTP モードを変更し、スイッチ VLAN データベースは一貫性を維持します。

VTP バージョン 3 は、スイッチ スタックが VTP データベースのプライマリ サーバである場合を除き、スタンドアロン スイッチであるかスタックであるかに関係なく同様に機能します。その場合は、スタック マスターの Media Access Control (MAC; メディア アクセス制御) アドレスがプライマリ サーバ ID として使用されます。マスター スイッチをリロードするか、電源を切断すると、新しいスタック マスターが選択されます。

- **stack-mac persistent timer [0 | time-value]** グローバル コンフィギュレーション コマンドを入力して固定 MAC アドレス機能を設定していない場合は、新しいマスターが選択されるときに、新しいマスターの MAC アドレスをプライマリ サーバとするテイクオーバー メッセージが送信されます。
- 固定 MAC アドレス機能が構成されている場合、新しいマスターは、構成された **stack-mac persistent timer** 値を待ちます。この期間中に前のマスター スイッチがスタックに復帰しない場合、新しいマスターはテイクオーバー メッセージを発行します。

スイッチ スタックの詳細については、[第 5 章「スイッチ スタックの管理」](#) を参照してください。

VTP の設定

ここでは、次の設定情報について説明します。

- 「[VTP のデフォルト設定](#)」(P.15-9)
- 「[VTP 設定時の注意事項](#)」(P.15-9)
- 「[VTP モードの設定](#)」(P.15-12)
- 「[VTP バージョンのイネーブル化](#)」(P.15-15)
- 「[VTP プルーニングのイネーブル化](#)」(P.15-16)

- 「ポート単位での VTP の設定」(P.15-17)
- 「VTP ドメインへの VTP クライアント スイッチの追加」(P.15-17)

VTP のデフォルト設定

表 15-2 に、VTP のデフォルト設定を示します。

表 15-2 VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード (VTP バージョン 1 およびバージョン 2)	サーバ
VTP モード (VTP バージョン 3)	バージョン 3 に変換するまでのモードは、VTP バージョン 1 または 2 のモードと同じです。
VTP バージョン	バージョン 1
MST データベース モード	透過
VTP バージョン 3 サーバタイプ	セカンダリ
VTP パスワード	なし
VTP プルーニング	ディセーブル

VTP 設定時の注意事項

VTP パスワード、バージョン、VTP ファイル名、最新の VTP 情報を提供するインターフェイス、ドメイン名、およびモードを設定する場合や、プルーニングをディセーブルまたはイネーブルに設定する場合には、**vtp** グローバル コンフィギュレーション コマンドを使用します。使用できるキーワードの詳細については、このリリースに対応するコマンドリファレンスに記載されているコマンドの説明を参照してください。VTP 情報は VTP VLAN データベースに保存されます。VTP モードが透過の場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。スイッチをリセットした場合にも、VTP モードを透過として保存するには、このコマンドを使用する必要があります。

スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視されます (クリアされます)。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

ドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内のすべてのスイッチを、同じドメイン名で設定しなければなりません。VTP 透過モードのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのスイッチについては VTP ドメイン名を設定する必要はありません。



(注)

NVRAM および DRAM のストレージが十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにする必要があります。



注意

すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しないでください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも 1 台のスイッチを VTP サーバ モードに設定してください。

パスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメイン パスワードを設定する場合は、すべてのドメイン スイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパスワードを設定する必要があります。パスワードのないスイッチ、またはパスワードが不正なスイッチは、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワードを使用して設定しないかぎり、VTP アドバタイズを受信しません。設定後、スイッチは同じパスワードおよびドメイン名を使用した VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、スイッチはドメイン名を学習します。



注意

VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメイン パスワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチが同じドメイン名を持つ必要がありますが、同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 をディセーブルに設定している場合、その VTP バージョン 2 対応スイッチは、同一 VTP ドメイン内で VTP バージョン 1 が稼動するスイッチとして動作できます (VTP バージョン 2 は、デフォルトでディセーブルに設定されています)。
- VTP バージョン 1 が稼動しているが、VTP バージョン 2 を稼動できるスイッチは、VTP バージョン 3 のアドバタイズを受信すると VTP バージョン 2 に自動的に移行します。
- VTP バージョン 3 が稼動しているスイッチを VTP バージョン 1 が稼動しているスイッチに接続すると、VTP バージョン 1 は VTP バージョン 2 に移行し、VTP バージョン 3 は、VTP バージョン 2 スイッチがそのデータベースを更新できるようにスケールダウンされたバージョンの VTP パケットを送信します。

- VTP バージョン 3 が稼動しているスイッチで拡張 VLAN を使用している場合は、バージョン 1 または 2 に移行できません。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応する場合を除いて、スイッチ上で VTP バージョン 2 をイネーブルにしないでください。あるスイッチでバージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応スイッチでバージョン 2 がイネーブルになります。バージョン 1 専用のスイッチがドメインに含まれている場合、そのスイッチはバージョン 2 対応スイッチとの間で VTP 情報を交換できません。
- VTP バージョン 1 および 2 スイッチは VTP バージョン 3 のアドバタイズを転送しないため、ネットワークのエッジに配置することを推奨します。
- 使用環境に TrBRF および TrCRF トークンリングネットワークが含まれている場合に、トークンリング VLAN スwitチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN は、各デバイスで手動で設定する必要があります。VTP バージョン 3 は、拡張範囲 VLAN をサポートします。拡張 VLAN を設定している場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- VTP バージョン 3 デバイスは、トランクポート上で VTP バージョン 2 デバイスからのメッセージを受信すると、その特定のトランク上で、VTP バージョン 2 フォーマットにスケールダウンされたバージョンの VLAN データベースを送信します。VTP バージョン 3 デバイスがトランク上で VTP バージョン 2 フォーマットの packets を送信するためには、最初にそのトランクポート上で VTP バージョン 2 packets を受信する必要があります。
- VTP バージョン 3 デバイスは、トランクポート上で VTP バージョン 2 デバイスを検出すると、VTP バージョン 2 packets に加えて VTP バージョン 3 packets の送信を続行するため、同じトランク上に 2 種類のネイバーを存在させることができます。
- VTP バージョン 3 デバイスは、VTP バージョン 2 またはバージョン 1 デバイスからの設定情報を受け入れません。
- 2 つの VTP バージョン 3 リージョンは、VTP バージョン 1 またはバージョン 2 リージョン経由でのみ、透過モードで通信できます。
- VTP バージョン 1 だけに対応したデバイスは、VTP バージョン 3 デバイスと相互運用できません。

設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズを送受信できるように、スイッチスタック上のトランクポートを設定する必要があります。

詳細については、「[VLAN トランクの設定](#)」(P.14-15) を参照してください。

クラスタメンバースイッチの VTP を VLAN に設定する場合、**rcommand** 特権 EXEC コマンドを使用して、そのメンバースイッチにログインします。コマンドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VTP バージョン 1 および 2 で拡張範囲 VLAN をスイッチに設定する場合は、スイッチを VTP 透過モードにする必要があります。VTP バージョン 3 は、クライアントモードまたはサーバモードで拡張範囲 VLAN の作成もサポートします。

VTP バージョン 1 および 2 はプライベート VLAN をサポートしていません。プライベート VLAN を設定した場合、スイッチは VTP 透過モードでなければなりません。プライベート VLAN がスイッチに設定されている場合、VTP モードを透過モードからクライアントモードやサーバモードに変更しないでください。VTP バージョン 3 はプライベート VLAN をサポートします。

VTP モードの設定

VTP モードは、次のいずれかに設定できます。

- スイッチが VTP サーバ モードの場合には、VLAN 設定を変更し、その変更をネットワーク全体に伝播できます。
- スイッチが VTP クライアント モードの場合には、そのスイッチの VLAN 設定を変更できません。クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、それに基づいて設定を変更します。
- スイッチを VTP 透過モードに設定すると、スイッチ上で VTP がディセーブルになります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 が動作している VTP トランスペアレント スイッチでは、受信した VTP アドバタイズのトランク リンクに転送します。
- VTP オフ モードは VTP 透過モードと同様に機能しますが、VTP アドバタイズは転送されません。

次の注意事項に従ってください。

- VTP バージョン 1 およびバージョン 2 では、スイッチ スタック上に拡張範囲 VLAN が設定されている場合は、VTP モードをクライアントまたはサーバに変更できません。エラー メッセージが表示され、設定が許可されません。VTP バージョン 1 およびバージョン 2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) の設定情報を伝播しません。これらの VLAN は、各デバイスで手動で設定する必要があります。



(注) VTP バージョン 1 およびバージョン 2 では、拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を作成するには、事前に **vtp mode transparent** グローバル コンフィギュレーション コマンドを使用して、VTP モードを透過に設定する必要があります。VTP 透過モードでスイッチが起動するように、この設定をスタートアップ コンフィギュレーションに保存してください。このようにしないと、スイッチのリセット時に拡張範囲 VLAN 設定が失われ、VTP サーバ モード (デフォルト) で起動します。

- VTP バージョン 3 は、拡張範囲 VLAN をサポートします。拡張範囲 VLAN を設定していない場合は、VTP バージョン 3 から VTP バージョン 2 に変換できません。
- スイッチを VTP クライアント モードに設定した場合、VLAN データベース ファイル (vlan.dat) は作成されません。そのままスイッチの電源をオフにすると、VTP 設定はデフォルトにリセットされます。スイッチが再起動されたあとも VTP 設定を VTP クライアント モードに維持するには、VTP モードを設定する前に、VTP ドメイン名を設定する必要があります。



注意

すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメイン名を設定しないでください。ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。したがって、少なくとも 1 台のスイッチを VTP サーバとして設定してください。

VTP モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp domain domain-name</code>	VTP 管理ドメイン名を設定します。1 ~ 32 文字の名前を使用できます。同一管理下にある VTP サーバ モードまたはクライアント モードのスイッチは、すべて同じドメイン名に設定する必要があります。 サーバ モード以外のモードでは、このコマンドは任意です。VTP サーバ モードでは、ドメイン名が必要です。スイッチが VTP ドメインにトランク 接続されている場合、そのスイッチはドメインの VTP サーバからドメイン名を取得します。 他の VTP パラメータを設定する前に、VTP ドメインを設定する必要があります。
ステップ 3	<code>vtp mode {client server transparent off} {vlan mst unknown}</code>	スイッチを VTP モード (クライアント、サーバ、透過、またはオフ) に設定します。 (任意) データベースを設定します。 <ul style="list-style-type: none"> • vlan : 設定されていない場合、デフォルトで VLAN データベースに設定されます。 • mst : Multiple Spanning-Tree (MST) データベース。 • unknown : データベース タイプが不明です。
ステップ 4	<code>vtp password password</code>	(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ~ 64 文字です。VTP パスワードを設定したにもかかわらず、ドメイン内の各スイッチに同じパスワードを割り当てなかった場合には、VTP ドメインが正常に動作しません。 VTP バージョン 3 で使用できるオプションについては、「 VTP バージョン 3 パスワードの設定 」(P.15-14) を参照してください。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show vtp status</code>	表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドの設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。 (注) スwitchの実行コンフィギュレーションに保存され、スタートアップ コンフィギュレーション ファイルにコピーできるのは、VTP モードおよびドメイン名だけです。

設定したドメイン名は、削除できません。別のドメインにスイッチを再び割り当てるしかありません。

他のモードのスイッチを VTP サーバ モードに戻すには、`no vtp mode` グローバル コンフィギュレーション コマンドを使用します。スイッチをパスワードがない状態に戻すには、`no vtp password` グローバル コンフィギュレーション コマンドを使用します。

次に、ドメイン名が `eng_group`、パスワードが `mypassword` という VTP サーバとしてスイッチを設定する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANs.
Switch(config)# vtp password mypassword
```

```
Setting device VLAN database password to mypassword.
Switch(config)# end
```

VTP バージョン 3 パスワードの設定

VTP バージョン 3 を使用するときのパスワードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp password password [hidden secret]</code>	(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用できる文字数は 8 ~ 64 文字です。 <ul style="list-style-type: none"> (任意) hidden : パスワード ストリングから生成された秘密鍵を <code>nvam:vlan.dat</code> ファイルに保存する場合は、hidden を入力します。VTP プライマリ サーバを設定してテイクオーバーを設定する場合は、パスワードを再入力するように求められます。 (任意) secret : パスワードを直接設定する場合は、secret を入力します。シークレットパスワードには、32 個の 16 進文字を指定する必要があります。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show vtp password</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

パスワードを消去するには、`no vtp password` グローバル コンフィギュレーション コマンドを入力します。

次に、非表示のパスワードの設定方法および表示例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP バージョン 3 プライマリ サーバの設定

テイクオーバー動作を起動する VTP プライマリ サーバ（バージョン 3 専用）として VTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>vtp primary-server [vlan mst] [force]</code>	<p>スイッチの動作ステートをセカンダリ サーバ（デフォルト）からプライマリ サーバに変更して、構成をドメインにアダプタイズします。スイッチのパスワードが hidden として設定されている場合は、パスワードを再入力するように求められます。</p> <ul style="list-style-type: none"> （任意） vlan : テイクオーバー機能として VLAN データベースを選択します。これがデフォルトです。 （任意） mst : テイクオーバー機能として Multiple Spanning Tree (MST) データベースを選択します。 （任意） force : force を入力すると、競合するサーバの設定が上書きされます。force を入力していない場合は、テイクオーバーを実行する前に確認が求められます。

次に、非表示のパスワードまたはシークレットパスワードが設定されている場合に、スイッチを VLAN データベース（デフォルト）のプライマリ サーバとして設定する例を示します。

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP domain

VTP Database Conf Switch ID      Primary Server Revision System Name
-----
VLANDB          Yes  00d0.00b8.1400=00d0.00b8.1400 1          stp7

Do you want to continue (y/n) [n]? y
```

VTP バージョンのイネーブル化

VTP バージョン 2 およびバージョン 3 は、デフォルトでディセーブルに設定されています。

- あるスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイネーブルにするには、各スイッチで手動で設定する必要があります。
- VTP バージョン 1 および 2 では、スイッチにバージョンを設定できるのは、VTP サーバモードまたは透過モードの場合に限られます。スイッチで VTP バージョン 3 が稼動しており、拡張 VLAN が存在しないか、プライベート VLAN が存在しないか、または非表示のパスワードが設定されていない場合は、クライアント モードでバージョン 2 に変更できます。



注意

同一 VTP ドメイン内のスイッチに関して、VTP バージョン 1 および VTP バージョン 2 間の相互運用はありません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正しく動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディセーブルにする必要があります。
- VTP バージョン 3 は、Cisco IOS Release 12.2(52) SE 以降のリリースが稼動するスイッチでサポートされます。

**注意**

VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのインスタンスに存在できます。

VTP バージョンを設定する場合の注意事項については、「[VTP バージョン](#)」(P.15-10) を参照してください。

VTP モードを設定するには、特権 EXEC バージョンで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp version {1 2 3}</code>	スイッチ上で VTP バージョンをイネーブルにします。デフォルトは VTP バージョン 1 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show vtp status</code>	設定した VTP バージョンがイネーブルであることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルトの VTP バージョン 1 に戻すには、`no vtp version` グローバル コンフィギュレーション コマンドを使用します。

VTP プルーニングのイネーブル化

プルーニングは、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リンクだけにフラッドングトラフィックを制限することによって、使用可能な帯域幅を増やします。VTP プルーニングをイネーブルにできるのは、スイッチが VTP サーバモードの場合だけです。

VTP ドメイン内で VTP プルーニングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp pruning</code>	VTP 管理ドメインでプルーニングをイネーブルにします。 プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバモードの 1 台のスイッチ上に限ってプルーニングをイネーブルにする必要があります。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show vtp status</code>	表示された <i>VTP Pruning Mode</i> フィールドの設定を確認します。

VTP プルーニングをディセーブルにするには、**no vtp pruning** グローバル コンフィギュレーション コマンドを使用します。

VTP バージョン 1 および 2 では、VTP サーバでプルーニングをイネーブルにすると、VTP ドメイン全体に対してイネーブルになります。VTP バージョン 3 では、ドメイン内のスイッチごとに手動でプルーニングをイネーブルにする必要があります。

プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトでは、トランク ポート上で VLAN 2 ~ 1001 がプルーニング適格です。専用の VLAN および拡張範囲 VLAN はプルーニングできません。プルーニング適格の VLAN を変更する手順については、「[プルーニング適格リストの変更](#)」(P.14-22) を参照してください。

ポート単位での VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルに設定できます。VTP は、トランク モードのポート上でのみイネーブルにできます。着信トラフィックおよび発信トラフィックはブロックされ、転送されません。

ポート上で VTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	vtp	指定したポート上で VTP をイネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface interface-id	ポートに対する変更を確認します。
ステップ 6	show vtp status	設定を確認します。

インターフェイス上で VTP をディセーブルにするには、**no vtp** インターフェイス コンフィギュレーション コマンドを使用します。

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# vtp
Switch(config-if)# end
```

VTP ドメインへの VTP クライアント スイッチの追加

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より小さいことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバ および VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、VLAN 情報は消去されません。

VTP ドメインに追加する *前に*、スイッチ上で VTP コンフィギュレーション リビジョン番号を確認およびリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show vtp status	VTP コンフィギュレーション リビジョン番号をチェックします。 番号が 0 の場合は、スイッチを VTP ドメインに追加します。 番号が 0 より大きい場合は、次の手順に従います。 a. ドメイン名を書き留めます。 b. コンフィギュレーション リビジョン番号を書き留めます。 c. 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vtp domain domain-name	ドメイン名を、ステップ 1 で表示された元の名前から新しい名前に変更します。
ステップ 4	end	スイッチの VLAN 情報が更新され、コンフィギュレーション リビジョン番号が 0 にリセットされます。特権 EXEC モードに戻ります。
ステップ 5	show vtp status	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認します。
ステップ 6	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 7	vtp domain domain-name	スイッチの元のドメイン名を入力します。
ステップ 8	end	スイッチの VLAN 情報が更新されて、特権 EXEC モードに戻ります。
ステップ 9	show vtp status	(任意) ドメイン名がステップ 1 のものと同じであり、コンフィギュレーション リビジョン番号が 0 であることを確認します。

コンフィギュレーション リビジョン番号をリセットしたあとに、スイッチを VTP ドメインに追加します。



(注)

スイッチ上で VTP をディセーブルにし、VTP ドメイン内の他のスイッチに影響を与えることなく VLAN 情報を変更するには、**vtp mode transparent** グローバル コンフィギュレーション コマンドを使用します。

VTP のモニタ

VTP の設定情報（ドメイン名、現在の VTP バージョン、VLAN 数）を表示することによって、VTP をモニタします。スイッチで送受信されたアドバタイズに関する統計情報を表示することもできます。

表 15-3 に、VTP アクティビティをモニタするための特権 EXEC コマンドを示します。

表 15-3 VTP モニタ コマンド

コマンド	目的
<code>show vtp counters</code>	送受信された VTP メッセージに関するカウンタを表示します。
<code>show vtp devices [conflict]</code>	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。競合とは、競合するプライマリ サーバを持つ VTP バージョン 3 デバイスです。スイッチが透過モードまたはオフモードである場合、 <code>show vtp devices</code> コマンドは情報を表示しません。
<code>show vtp interface [interface-id]</code>	すべてのインターフェイスまたは指定されたインターフェイスの VTP ステータスおよび設定を表示します。
<code>show vtp password</code>	VTP パスワードを表示します。表示されるパスワードの形式は、 hidden キーワードが入力されているかどうか、およびスイッチで暗号化イネーブルになっているかどうかによって異なります。
<code>show vtp status</code>	VTP スイッチの設定情報を表示します。



CHAPTER 16

音声 VLAN の設定

この章では、Catalyst 3750 スイッチに音声 VLAN 機能を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチ スタックを意味します。Catalyst 6500 ファミリー スイッチの一部のマニュアルでは、音声 VLAN を補助 VLAN と表しています。



(注)

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

この章で説明する内容は、次のとおりです。

- 「音声 VLAN の概要」 (P.16-1)
- 「音声 VLAN の設定」 (P.16-3)
- 「音声 VLAN の表示」 (P.16-8)

音声 VLAN の概要

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP precedence およびレイヤ 2 Class of Service (CoS; サービス クラス) 値を使用して、音声トラフィックを送信します。どちらの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service (QoS) をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。QoS の詳細については、第 36 章「QoS の設定」を参照してください。

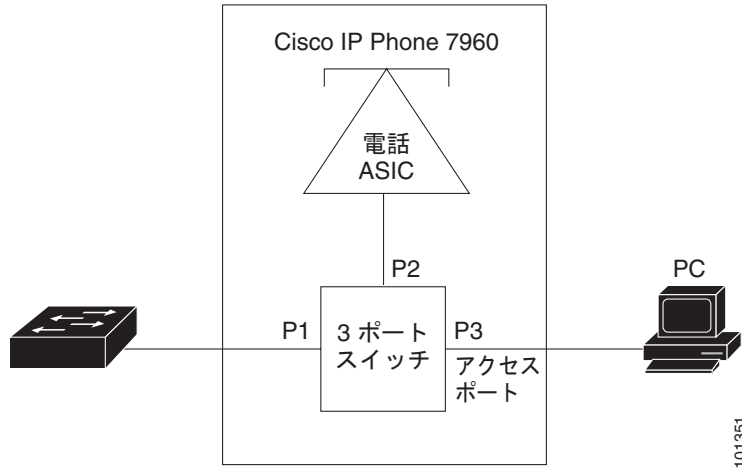
Cisco 7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

Cisco IP Phone には、3 ポートの 10/100 スイッチが統合されています。図 16-1 を参照してください。これらのポートは、次のデバイスへの接続専用です。

- ポート 1 は、スイッチまたは他の Voice over IP (VoIP) デバイスに接続します。
- ポート 2 は、IP Phone のトラフィックを伝送する内部 10/100 インターフェイスです。
- ポート 3 (アクセス ポート) は、PC または他のデバイスに接続します。

図 16-1 に、Cisco7960 IP Phone の接続方法の例を示します。

図 16-1 スイッチに接続された Cisco7960 IP Phone



Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセスポートを、1つの VLAN は音声トラフィック用に、もう1つの VLAN は Cisco IP Phone に接続しているデバイスからのデータトラフィック用に使用するように設定できます。スイッチ上のアクセスポートを設定して、Cisco Discovery Protocol (CDP) パケットを送信させることができます。CDP には、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指定します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信



(注)

いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

Cisco IP Phone のデータトラフィック

スイッチは、Cisco IP Phone のアクセスポートに接続されたデバイス（図 16-1 を参照）から送られた、タグ付きデータトラフィック（IEEE 802.1Q または IEEE 802.1p フレームタイプのトラフィック）を処理することもできます。スイッチ上のレイヤ 2 アクセスポートが、CDP パケットを送信するように設定できます。CDP は、接続する IP Phone に、次のいずれかのモードで IP Phone 上のアクセスポートを設定するように指定します。

- trusted（信頼性がある）モードでは、Cisco IP Phone のアクセスポート経由で受信したすべてのトラフィックがそのまま IP Phone を通過します。
- untrusted（信頼性がない）モードでは、Cisco IP Phone のアクセスポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与えます。デフォルトのレイヤ 2 CoS 値は 0 です。untrusted モードがデフォルトの設定です。



(注) Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの信頼状態に関係なく、そのまま IP Phone を通過します。

音声 VLAN の設定

ここでは、次の設定情報について説明します。

- 「音声 VLAN のデフォルト設定」(P.16-3)
- 「音声 VLAN 設定時の注意事項」(P.16-3)
- 「Cisco7960 IP Phone に接続するポートの設定」(P.16-5)

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN 設定時の注意事項

音声 VLAN の設定時の注意事項を次に示します。

- 音声 VLAN の設定は、スイッチ アクセス ポートでのみサポートされており、トランク ポートではサポートされていません。音声 VLAN はレイヤ 2 ポートだけで設定できます。



(注) トランク ポートは、通常の VLAN と同様に音声 VLAN をいくつでも伝送できます。音声 VLAN の設定は、トランク ポートでは必要ありません。

- IP Phone での通信が適切に行えるように、音声 VLAN はスイッチ上でアクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、**show vlan** 特権 EXEC コマンドを使用します (リストで表示されます)。VLAN がリストになかった場合、音声 VLAN の作成方法について、第 14 章「VLAN の設定」を参照してください。
- 音声 VLAN をプライベート VLAN ポートに設定しないでください。
- Power over Ethernet (PoE) スイッチは、シスコ独自規格の受電装置および IEEE 802.3af 準拠の受電装置が AC 電源から電力を供給されていない場合に、自動的に電力を供給できます。PoE インターフェイスの詳細については、「PoE ポートの電力管理モードの設定」(P.12-24) を参照してください。
- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を **trust** に設定しておくことを推奨します。Auto-QoS 機能を使用すると、これらは自動的に設定されます。詳細は、第 36 章「QoS の設定」を参照してください。

- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります (デフォルト設定では、CDP がすべてのスイッチ インターフェイスでグローバルにイネーブルです)。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上にあります。
 - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
 - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
 - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
 - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上でルーティングされないからです (ルーティングによってフレーム タイプの相違が排除されます)。
- 音声 VLAN では、スタティック セキュア MAC (メディア アクセス制御) アドレスを設定できません。
- 音声 VLAN ポートには次のポート タイプがあります。
 - ダイナミック アクセス ポート。詳細については、「[VMPS クライアント上のダイナミック アクセス ポートの設定](#)」(P.14-30) を参照してください。
 - IEEE 802.1X 認証ポート。詳細については、「[802.1X 準備チェックの設定](#)」(P.10-37) を参照してください。



(注) 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1X をイネーブルにした場合、その IP Phone のスイッチへの接続が最大 30 秒間失われます。

- 保護ポート。詳細については、「[保護ポートの設定](#)」(P.26-6) を参照してください。
- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) または Remote SPAN (RSPAN) セッションの送信元ポートまたは宛先ポート。
- セキュア ポート。詳細については、「[ポート セキュリティの設定](#)」(P.26-9) を参照してください。



(注) 音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定しなければなりません。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

Cisco7960 IP Phone に接続するポートの設定

Cisco7960 IP Phone は、PC または他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータトラフィックの伝送方法を決定できます。

ここでは、次の設定情報について説明します。

- 「Cisco IP Phone の音声トラフィックの設定」(P.16-5)
- 「着信データフレームのプライオリティ設定」(P.16-7)

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティタグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ（アクセス）VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（デフォルトは 5）を伝送します。

ポート上で音声トラフィックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>mls qos trust cos</code>	パケットの CoS 値を使用して着信するトラフィック パケットを分類するように、インターフェイスを設定します。タグなしパケットの場合、ポートのデフォルト CoS 値が使用されます。 (注) ポートの信頼状態を設定する前に、 <code>mls qos</code> グローバル コンフィギュレーション コマンドを使用することによって、QoS をグローバルでイネーブルに設定しておく必要があります。

コマンド	目的
ステップ 4 switchport voice {detect cisco-phone [full-duplex] vlan {vlan-id dot1p none untagged}}	<p>Cisco IP Phone による音声トラフィックの伝送方法を設定します。</p> <ul style="list-style-type: none"> • detect : Cisco IP Phone を検出し認識するように、インターフェイスを設定します。 • cisco-phone : switchport voice detect コマンドを最初の実装する場合、使用できるのはこのオプションだけです。デフォルトは、no switchport voice detect cisco-phone [full-duplex] です。 • full-duplex : (任意) 全二重方式の Cisco IP Phone だけを受け入れるように、スイッチを設定します。 • vlan-id : すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。有効な VLAN ID は 1 ~ 4094 です。 • dot1p : 音声トラフィックに IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN (VLAN 0) を使用してすべてのトラフィックが伝送されるように、IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。 • none : IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 • untagged : タグなしの音声トラフィックを送信するように IP Phone を設定します。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show interfaces interface-id switchport または show running-config interface interface-id	<p>音声 VLAN の設定を確認します。</p> <p>QoS および音声 VLAN の設定を確認します。</p>
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Cisco IP Phone に接続しているポートを設定する例を示します。ポートは、CoS 値を使用して着信トラフィックを分類し、音声トラフィック用に IEEE 802.1p プライオリティ タギングを使用し、デフォルトのネイティブ VLAN (VLAN 0) を使用してすべてのトラフィックを伝送するように設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport voice vlan** インターフェイス コンフィギュレーション コマンドを使用します。

次に、Cisco IP Phone で **switchport voice detect** をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport voice?
detect          detection enhancement keyword
vlan            VLAN for voice traffic
```

```
Switch(config-if)# switchport voice detect?
cisco-phone      Cisco IP Phone
Switch(config-if)# switchport voice detect cisco-phone?
full-duplex      Cisco IP Phone

Switch(config-if)# switchport voice detect cisco-phone full-duplex
full-duplex      full duplex keyword

Switch(config-if)# end
```

次に、Cisco IP Phone で **switchport voice detect** をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# no switchport voice detect cisco-phone
Switch(config-if)# no switchport voice detect cisco-phone full-duplex
```

着信データ フレームのプライオリティ設定

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラフィック (IEEE 802.1Q または IEEE 802.1p フレーム) を処理するために、スイッチが CDP パケットを送信するように設定できます。CDP は、Cisco IP Phone に、IP Phone 上のアクセス ポートに接続されたデバイスからのデータ パケットをどのように送信するかを指定します。PC は、CoS 値が割り当てられたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリティを変更しない (信頼する) または変更する (信頼しない) ように、IP Phone を設定できます。

Cisco IP Phone の非音声ポートから受信したデータ トラフィックのプライオリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport priority extend { cos value trust }	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを設定します。 <ul style="list-style-type: none"> • cos value : PC または接続しているデバイスから受信したプライオリティを指定の CoS 値に変更するように、IP Phone を設定します。値は 0 ~ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは cos 0 です。 • trust : PC または接続しているデバイスから受信したプライオリティを信頼するように IP Phone のアクセス ポートを設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id switchport	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Cisco IP Phone に接続しているポートを設定して、PC または接続しているデバイスから受信するフレームのプライオリティを変更しないようにする例を示します。

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface gigabitethernet1/0/1  
Switch(config-if)# switchport priority extend trust  
Switch(config-if)# end
```

ポートをデフォルト設定に戻すには、**no switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。

音声 VLAN の表示

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを使用します。



CHAPTER 17

プライベート VLAN の設定

この章では、Catalyst 3750 スイッチにプライベート VLAN を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



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

この章で説明する内容は、次のとおりです。

- 「プライベート VLAN の概要」(P.17-1)
- 「プライベート VLAN の設定」(P.17-6)
- 「プライベート VLAN のモニタリング」(P.17-15)



(注) プライベート VLAN を設定した場合、スイッチは VLAN Trunking Protocol (VTP; VLAN トランキン
グ プロトコル) 透過モードでなければなりません。第 15 章「VTP の設定」を参照してください。

プライベート VLAN の概要

プライベート VLAN 機能は、サービス プロバイダーが VLAN を使用している場合に直面する 2 つの問題に対処します。

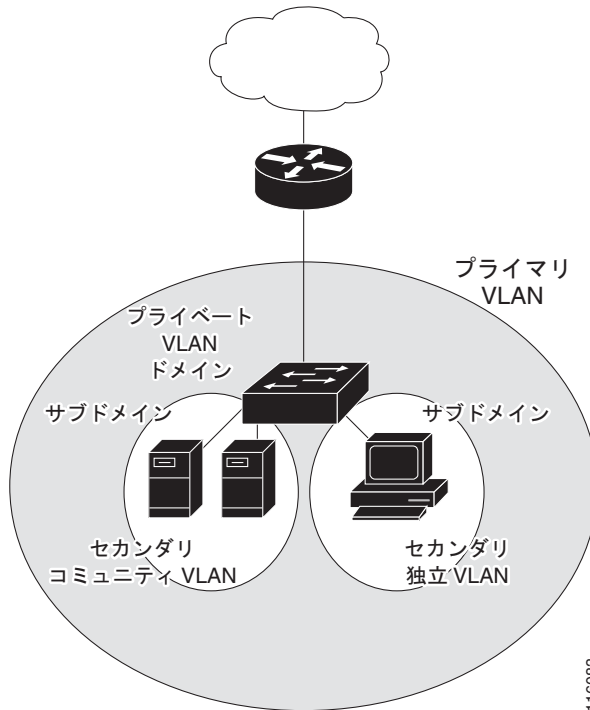
- スケーラビリティ：スイッチは最大 1005 のアクティブ VLAN をサポートします。サービス プロバイダーが 1 カスタマーあたり 1 つの VLAN を割り当てる場合、サービス プロバイダーがサポートできるカスタマー数はこれに制限されます。
- IP ルーティングをイネーブルにするには、各 VLAN にサブネット アドレス空間またはアドレス ブロックを割り当てますが、これにより、未使用の IP アドレスが無駄になり、IP アドレスの管理に問題が起きます。

プライベート VLAN を使用することでスケーラビリティの問題に対処することができ、サービス プロバイダーには IP アドレス管理の利点をもたらされ、カスタマーに対してはレイヤ 2 セキュリティを提供できます。

プライベート VLAN は、通常の VLAN ドメインをサブドメインに分割するもので、複数の VLAN ペア (各サブドメインに 1 つの VLAN) を持つことができます。サブドメインは、プライマリ VLAN およびセカンダリ VLAN という VLAN のペアで表現されます。

プライベート VLAN 内のすべての VLAN ペアは同じプライマリ VLAN を共有します。セカンダリ VLAN ID は、あるサブドメインを別のものと区別します。図 17-1 を参照してください。

図 17-1 プライベート VLAN ドメイン



セカンダリ VLAN には 2 種類あります。

- 独立 VLAN：独立 VLAN 内のポートは、レイヤ 2 レベルで互いに通信できません。
- コミュニティ VLAN：コミュニティ VLAN 内のポートは互いに通信できますが、レイヤ 2 レベルにある他のコミュニティ内のポートとは通信できません。

プライベート VLAN では、同じプライベート VLAN 内のポート間をレイヤ 2 で分離します。プライベート VLAN ポートには、次の 3 つのタイプがあります。

- 混合：混合ポートは、プライベート VLAN に属し、プライマリ VLAN と関連しているセカンダリ VLAN に属するコミュニティ ポートや独立ホスト ポートなどの、すべてのインターフェイスと通信できます。
- 独立：独立ポートは、独立セカンダリ VLAN に属するホスト ポートです。これは、混合ポートを除く、同じプライベート VLAN 内の他のポートからレイヤ 2 で完全に分離されています。プライベート VLAN では、混合ポートからのトラフィックを除く、独立ポートへのすべてのトラフィックをブロックします。独立ポートで受信されるトラフィックは、混合ポートへのみ転送されます。
- コミュニティ：コミュニティ ポートは、コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよび混合ポートと通信します。これらのインターフェイスは、他のコミュニティの他のすべてのインターフェイスおよびプライベート VLAN 内の独立ポートとレイヤ 2 で分離されます。



(注)

トランク ポートは、通常の VLAN からのトラフィックを伝送し、またプライマリ、独立、およびコミュニティ VLAN からのトラフィックも伝送します。

プライマリおよびセカンダリ VLAN には次のような特性があります。

- **プライマリ VLAN** : プライベート VLAN には、プライマリ VLAN を 1 つだけ設定できます。プライベート VLAN 内のすべてのポートは、プライマリ VLAN のメンバーです。プライマリ VLAN は、混合ポートからの単一方向トラフィックのダウンストリームを（独立およびコミュニティ）ホストポートおよび他の混合ポートへ伝送します。
- **独立 VLAN** : プライベート VLAN の独立 VLAN は 1 つだけです。独立 VLAN は、ホストからの単一方向トラフィック アップストリームを混合ポートおよびゲートウェイへ伝送するセカンダリ VLAN です。
- **コミュニティ VLAN** : コミュニティ VLAN は、コミュニティポートからのアップストリームトラフィックを混合ポートゲートウェイおよび同じコミュニティ内の他のホストポートへ伝送するセカンダリ VLAN です。複数のコミュニティ VLAN を 1 つのプライベート VLAN に設定できます。

混合ポートが扱えるのは、1 つのプライマリ VLAN、1 つの独立 VLAN、および複数のコミュニティ VLAN のみです。レイヤ 3 ゲートウェイは通常混合ポートを介してスイッチに接続されています。混合ポートを使用すると、幅広いデバイスをプライベート VLAN へのアクセスポートとして接続できます。たとえば、すべてのプライベート VLAN サーバを管理ワークステーションからモニタしたりバックアップしたりするのに、混合ポートを使用できます。

スイッチング環境では、個々のエンドステーションまたはエンドステーションの共通グループに、個別のプライベート VLAN と関連する IP サブネットを割り当てることができます。エンドステーションがデフォルトゲートウェイと対話する必要があるのは、プライベート VLAN 外部と通信する場合のみです。

プライベート VLAN を使用してエンドステーションへのアクセスを次のように制御できます。

- エンドステーションに接続されているインターフェイスを選択して独立ポートとして設定し、レイヤ 2 の通信をしないようにします。たとえば、エンドステーションがサーバの場合、この設定によりサーバ間のレイヤ 2 通信ができなくなります。
- デフォルトゲートウェイおよび選択したエンドステーション（たとえばバックアップサーバなど）に接続されたインターフェイスを混合ポートとして設定します。これにより、すべてのエンドステーションがデフォルトゲートウェイに接続できます。

プライマリ、独立、およびコミュニティ VLAN をプライベート VLAN をサポートする他のデバイスにトランッキングすることで、プライベート VLAN を複数のデバイスに拡張できます。プライベート VLAN コンフィギュレーションのセキュリティを保って VLAN の他のユーザがプライベート VLAN に設定されないようにするには、プライベート VLAN ポートのないデバイスを含む、すべての中間デバイス内にプライベート VLAN を設定します。

プライベート VLAN での IP アドレッシング方式

各カスタマーに個別の VLAN を割り当てると、次のように IP アドレッシング方式が非効率的になります。

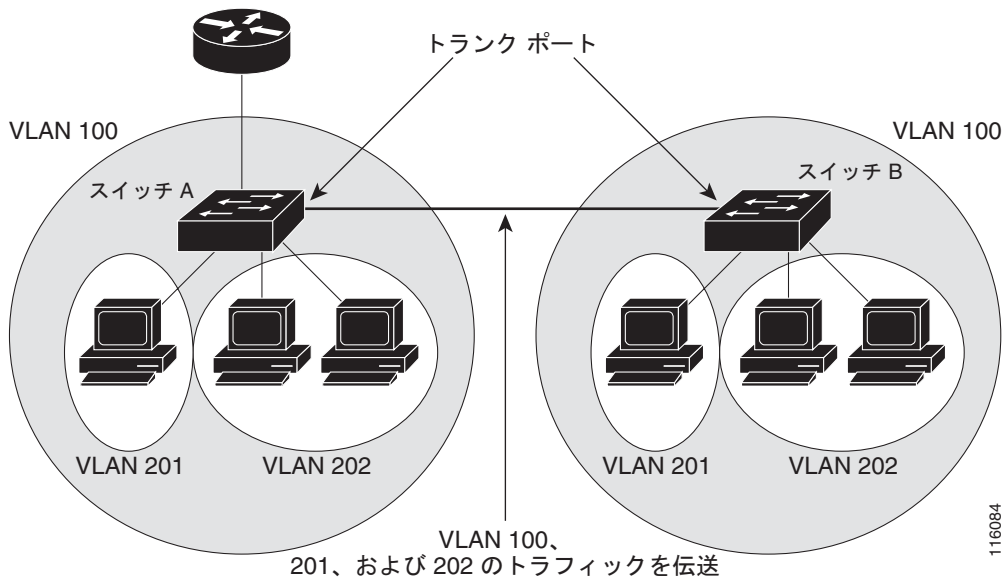
- カスタマーの VLAN にアドレスブロックを割り当てると、未使用の IP アドレスが出てきます。
- VLAN 内のデバイス数が増加した場合、それに対応するだけのアドレスを割り当てられない場合があります。

これらの問題は、プライベート VLAN を使用することで軽減できます。この場合、プライベート VLAN 内のすべてのメンバーがプライマリ VLAN に割り当てられた共通アドレス空間を共有します。ホストはセカンダリ VLAN に接続され、Dynamic Host Configuration Protocol (DHCP) サーバがプライマリ VLAN に割り当てられたアドレスブロックから IP アドレスを割り当てます。後続の IP アドレスは、同じプライマリ VLAN にある別のセカンダリ VLAN にあるカスタマーデバイスに割り当てることができます。新しいデバイスが追加されると、DHCP サーバはサブネットアドレスの大きなプールから次に使用可能なアドレスをデバイスに割り当てます。

複数のスイッチにまたがるプライベート VLAN

通常の VLAN と同様に、プライベート VLAN を複数のスイッチにまたがるように設定できます。トランクポートはプライマリ VLAN およびセカンダリ VLAN を隣接スイッチに伝送します。トランクポートはプライベート VLAN を他の VLAN として扱います。複数のスイッチにまたがるプライベート VLAN の機能の場合、スイッチ A にある独立ポートからのトラフィックはスイッチ B に到達しません。図 17-2 を参照してください。

図 17-2 複数のスイッチにまたがるプライベート VLAN



VLAN 100 = プライマリ VLAN
 VLAN 201 = セカンダリ独立 VLAN
 VLAN 202 = セカンダリ コミュニティ VLAN

VTP はプライベート VLAN をサポートしないので、レイヤ 2 ネットワーク内のすべてのスイッチにプライベート VLAN を手動で設定する必要があります。ネットワーク内の一部のスイッチにプライマリおよびセカンダリ VLAN の関連を設定しない場合、これらのスイッチのレイヤ 2 データベースは統合されません。これにより、これらのスイッチにプライベート VLAN トラフィックの不要なフラグメントが発生する可能性があります。



(注)

プライベート VLAN をスイッチに設定するときに、ユニキャストルートとレイヤ 2 エントリとの間のシステム リソースのバランスを取るために、常にデフォルトの Switch Database Management (SDM; スイッチ データベース管理) テンプレートを使用してください。別の SDM テンプレートが設定されている場合、デフォルト テンプレートを設定するのに **sdm prefer default** グローバル コンフィギュレーション コマンドを使用します。第 8 章「SDM テンプレートの設定」を参照してください。

プライベート VLAN の他機能との相互作用

プライベート VLAN には、次のように他の機能と相互作用があります。

- 「プライベート VLAN とユニキャスト、ブロードキャスト、およびマルチキャスト トラフィック」 (P.17-5)
- 「プライベート VLAN と SVI」 (P.17-5)
- 「プライベート VLAN およびスイッチ スタック」 (P.17-6)

「セカンダリおよびプライマリ VLAN の設定」 (P.17-7) の下にある「プライベート VLAN 設定時の注意事項」も参照してください。

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

通常の VLAN では、同じ VLAN にあるデバイスはレイヤ 2 レベルで互いに通信しますが、別の VLAN にあるインターフェイスに接続されたデバイスとはレイヤ 3 レベルで通信する必要があります。プライベート VLAN では、混合ポートはプライマリ VLAN のメンバーで、ホストポートはセカンダリ VLAN に属しています。セカンダリ VLAN はプライマリ VLAN に対応付けられているため、これらの VLAN のメンバーはレイヤ 2 レベルで互いに通信できます。

通常の VLAN では、ブロードキャストはその VLAN 内のすべてのポートに転送されます。プライベート VLAN ブロードキャスト転送は、次のようにブロードキャストを送信するポートに左右されます。

- 独立ポートはブロードキャストを混合ポートまたはトランクポートにだけ送信します。
- コミュニティポートは、すべての混合ポート、トランクポート、および同じコミュニティ VLAN 内のポートにブロードキャストを送信します。
- 混合ポートは、プライベート VLAN のすべてのポート（他の混合ポート、トランクポート、独立ポート、コミュニティポート）にブロードキャストを送信します。

マルチキャスト トラフィックは、プライベート VLAN 境界を越えて単一のコミュニティ VLAN 内にルーティングまたはブリッジングされます。マルチキャスト トラフィックは、同じ独立 VLAN 内のポート間で転送されず、また別のセカンダリ VLAN 内のポート間でも転送されません。

プライベート VLAN と SVI

レイヤ 3 スイッチでは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) が VLAN のレイヤ 3 インターフェイスを表します。レイヤ 3 デバイスは、セカンダリ VLAN ではなくプライマリ VLAN を介してのみプライベート VLAN と通信します。レイヤ 3 VLAN インターフェイスをプライマリ VLAN に対してのみ設定します。レイヤ 3 VLAN インターフェイスをセカンダリ VLAN 用に設定できません。セカンダリ VLAN 用の SVI は、VLAN がセカンダリ VLAN として設定されている間は非アクティブです。

- アクティブ SVI を設定した VLAN をセカンダリ VLAN として設定しようとする、SVI をディセーブルにするまで設定が許可されません。
- セカンダリ VLAN として設定されている VLAN に SVI を作成しようとしてセカンダリ VLAN がすでにレイヤ 3 にマッピングされている場合、SVI は作成されず、エラーが返されます。SVI がレイヤ 3 にマッピングされていない場合、SVI は作成されますが、自動的にシャットダウンされます。

プライマリ VLAN がセカンダリ VLAN に対応付けられていてマッピングされていると、プライマリ VLAN 上の設定はセカンダリ VLAN SVI に伝播されます。たとえば、IP サブネットをプライマリ VLAN SVI に割り当てる場合、このサブネットはプライベート VLAN 全体の IP サブネットアドレスです。

プライベート VLAN およびスイッチ スタック

プライベート VLAN はスイッチ スタック内で動作することができ、プライベート VLAN ポートはさまざまなスタック メンバーに常駐できます。ただし、スイッチ スタックを変更するとプライベート VLAN 動作に影響を与えます。

- スタックにプライベート VLAN 混合ポートのみが含まれ、このポートを含めたスタック メンバーがスタックから削除された場合、プライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- スタック内にプライベート VLAN 混合ポートが 1 つのみあるスタック マスターに障害が発生した、またはスタックを残し、新しいスタック マスターが選択された場合、古いスタック マスターに混合ポートがあるプライベート VLAN のホスト ポートとプライベート VLAN 外との接続が不能になります。
- 2 つのスタックが統合した場合、権利を獲得したスタックのプライベート VLAN は影響を受けませんが、スイッチを再起動したときに、権利を獲得しなかったスイッチのプライベート VLAN 設定が失われます。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。


プライベート VLAN の設定

ここでは、次の設定情報について説明します。

- 「プライベート VLAN の設定手順」(P.17-6)
- 「デフォルトのプライベート VLAN 設定」(P.17-7)
- 「プライベート VLAN 設定時の注意事項」(P.17-7)
- 「プライベート VLAN 内の VLAN の設定および対応付け」(P.17-10)
- 「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」(P.17-12)
- 「プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定」(P.17-13)
- 「セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング」(P.17-14)

プライベート VLAN の設定手順

プライベート VLAN を設定するには、次の手順を実行します。

- ステップ 1** VTP モードを透過に設定します。
- ステップ 2** プライマリおよびセカンダリ VLAN を作成してこれらに対応付けします。「プライベート VLAN 内の VLAN の設定および対応付け」(P.17-10) を参照してください。

(注) VLAN がまだ作成されていない場合、プライベート VLAN 設定プロセスでこれを作成します。
- ステップ 3** インターフェイスを独立ポートまたはコミュニティ ホスト ポートに設定して、ホスト ポートに VLAN メンバシップを割り当てます。「プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定」(P.17-12) を参照してください。

- ステップ 4** インターフェイスを混合ポートとして設定し、混合ポートをプライマリおよびセカンダリ VLAN のペアにマッピングします。「[プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定](#)」(P.17-13) を参照してください。
- ステップ 5** VLAN 間ルーティングを使用している場合、プライマリ SVI を設定し、セカンダリ VLAN をプライマリ SVI にマッピングします。「[セカンダリ VLAN のプライマリ VLAN レイヤ 3 VLAN インターフェイスへのマッピング](#)」(P.17-14) を参照してください。
- ステップ 6** プライマリ VLAN 設定を確認します。

デフォルトのプライベート VLAN 設定

プライベート VLAN は設定されていません。

プライベート VLAN 設定時の注意事項

プライベート VLAN 設定時の注意事項は、次のカテゴリに分けられます。

- 「[セカンダリおよびプライマリ VLAN の設定](#)」(P.17-7)
- 「[プライベート VLAN ポート設定](#)」(P.17-9)
- 「[他の機能との間の制限](#)」(P.17-9)

セカンダリおよびプライマリ VLAN の設定

プライベート VLAN の設定を行うときは、次の注意事項に従ってください。

- スイッチで VTP バージョン 1 または 2 が稼動している場合は、VTP を透過モードに設定する必要があります。プライベート VLAN の設定が終わったら、VTP モードをクライアントやサーバに変更しないでください。VTP の詳細については、[第 15 章「VTP の設定」](#)を参照してください。VTP バージョン 3 は、すべてのモードでプライベート VLAN をサポートします。
- VTP バージョン 1 または 2 では、プライベート VLAN を設定してから、**copy running-config startup config** 特権 EXEC コマンドを使用して VTP 透過モード設定およびプライベート VLAN 設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存します。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。VTP バージョン 3 はプライベート VLAN をサポートします。
- VTP バージョン 1 および 2 はプライベート VLAN 設定を伝播しません。デバイスで VTP バージョン 3 が稼動していない場合は、プライベート VLAN ポートが必要な各デバイスにプライベート VLAN を設定する必要があります。
- VLAN 1 または VLAN 1002 ~ 1005 をプライマリまたはセカンダリ VLAN に設定できません。拡張 VLAN (VLAN ID 1006 ~ 4094) はプライベート VLAN に属することができます。
- プライマリ VLAN には 1 つの独立 VLAN とこれに対応付けられた複数のコミュニティ VLAN を設定できます。独立またはコミュニティ VLAN には、これに対応付けられたプライマリ VLAN を 1 つだけ設定できます。
- プライベート VLAN には複数の VLAN が含まれますが、プライベート VLAN 全体で実行可能な Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) インスタンスは 1 つだけです。セカンダリ VLAN がプライマリ VLAN に対応付けられている場合、プライマリ VLAN の STP パラメータはセカンダリ VLAN に伝播されます。

- プライベート VLAN で DHCP スヌーピングをイネーブルにできます。プライマリ VLAN で DHCP スヌーピングをイネーブルにする場合、セカンダリ VLAN に伝播されます。セカンダリ VLAN に DHCP を設定する場合、その設定はプライマリ VLAN がすでに設定されていないと有効になりません。
 - プライベート VLAN ポートで IP ソース ガードをイネーブルにする場合は、プライマリ VLAN で DHCP スヌーピングをイネーブルにする必要があります。
 - プライベート VLAN 内でトラフィックを伝送していないデバイスのトランクからプライベート VLAN をプルーンすることを推奨します。
 - プライマリ VLAN、独立 VLAN、およびコミュニティ VLAN に別々の Quality of Service (QoS) 設定を適用できます。
 - Sticky ARP
 - Sticky ARP エントリは SVI およびレイヤ 3 インターフェイスで学習されます。これらのエントリには期限切れがありません。
 - **ip sticky-arp** グローバル コンフィギュレーション コマンドは、プライベート VLAN に属する SVI でだけサポートされます。
 - **ip sticky-arp** インターフェイス コンフィギュレーション コマンドは、次のインターフェイスでだけサポートされます。
 - レイヤ 3 インターフェイス
 - 標準 VLAN に属する SVI
 - プライベート VLAN に属する SVI
- ip sticky-arp** グローバル コンフィギュレーション コマンドおよび **ip sticky-arp** インターフェイス コンフィギュレーション コマンドの詳しい使用方法については、このリリースに対応するコマンドリファレンスを参照してください。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます（「[VLAN マップの設定](#)」(P.35-31) を参照)。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
 - フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
 - ホスト ポートから混合ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
 - 混合ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。
- プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN の両方に適用します。
- プライマリ VLAN SVI にのみルータ Access Control List (ACL; アクセス コントロール リスト) を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。
 - プライベート VLAN がレイヤ 2 でホストを分離していても、ホストはレイヤ 3 で互いに通信できます。
 - プライベート VLAN は、次の Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 機能をサポートします。
 - プライベート VLAN を SPAN 送信元ポートとして設定できます。

- VLAN-based SPAN (VSPAN) はプライマリ VLAN、独立 VLAN、およびコミュニティ VLAN で使用できます。また、出力または入力トラフィックを別々にモニタするために、1 つの VLAN でのみ SPAN を使用できます。

プライベート VLAN ポート設定

プライベート VLAN ポートの設定を行うときは、次の注意事項に従ってください。

- プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN にポートを割り当てるには、プライベート VLAN 設定コマンドのみを使用します。プライマリ VLAN、独立 VLAN、またはコミュニティ VLAN として設定した VLAN に割り当てられたレイヤ 2 アクセス ポートは、VLAN がプライベート VLAN 設定の一部の間は非アクティブになります。レイヤ 2 トランク インターフェイスは STP フォワーディング ステートのままです。
- Port Aggregation Protocol (PAgP; ポート集約プロトコル) または Link Aggregation Control Protocol (LACP) EtherChannel に属するポートをプライベート VLAN ポートとして設定しないでください。ポートがプライベート VLAN 設定の一部である間は、ポートの EtherChannel 設定は非アクティブです。
- 誤った設定による STP ループを発生させず、STP コンバージェンスを高速にするために、独立およびコミュニティ ホスト ポートで PortFast および BPDU (ブリッジプロトコルデータユニット) ガードをイネーブルにします (第 21 章「オプションのスパニング ツリー機能の設定」を参照)。イネーブルの場合、STP はすべての PortFast が設定されたレイヤ 2 LAN ポートに BPDU ガード機能を適用します。PortFast および BPDU ガードを混合ポートでイネーブルにしないでください。
- プライベート VLAN 設定で VLAN を削除した場合、VLAN に対応付けられたプライベート VLAN ポートが非アクティブになります。
- デバイスがトランクに接続されていてプライマリおよびセカンダリ VLAN がトランクから削除されていない場合、プライベート VLAN ポートを別のネットワーク デバイス上に設定できます。

他の機能との間の制限

プライベート VLAN を設定する際に、他の機能との間で次のような制限があることに留意してください。



(注)

エラー メッセージなしで設定が受け入れられていてもコマンドが機能しない場合があります。

- フォールバック ブリッジングをプライベート VLAN のスイッチに設定しないでください。
- Internet Group Management Protocol (IGMP; インターネット グループ マネージメント プロトコル) スヌーピングがスイッチ上でイネーブル (デフォルト) の場合、スイッチ スタックがサポートするプライベート VLAN ドメイン数は、20 までです。
- Remote SPAN (RSPAN; リモート SPAN) をプライベート VLAN のプライマリまたはセカンダリ VLAN として設定しないでください。

SPAN の詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。

- 次のような機能が設定されているインターフェイスにプライベート VLAN ポートを設定しないでください。
 - ダイナミック アクセス ポート VLAN メンバシップ
 - Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)
 - PAgP

- LACP
- Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション)
- 音声 VLAN
- Web Cache Communication Protocol (WCCP)
- プライベート VLAN ポートはセキュア ポートにできません。保護ポートとして設定しないでください。
- IEEE 802.1X ポートベース認証をプライベート VLAN ポートに設定できますが、IEEE 802.1X とポートセキュリティ、音声 VLAN、またはポート単位のユーザ ACL を、プライベート VLAN ポートに設定できません。
- プライベート VLAN ホストまたは混合ポートは SPAN 宛先ポートにはできません。SPAN 宛先ポートをプライベート VLAN ポートに設定した場合、ポートは非アクティブになります。
- プライマリ VLAN 内の混合ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連セカンダリ VLAN に追加する必要があります。セカンダリ VLAN 内ホスト ポートにスタティック MAC アドレスを設定した場合、同じスタティック アドレスをすべての関連プライマリ VLAN に追加する必要があります。スタティック MAC アドレスをプライベート VLAN ポートから削除する際に、設定されている MAC アドレスのすべてのインスタンスをプライベート VLAN から削除する必要があります。



(注) プライベート LAN 上にある 1 つの VLAN で学習されたダイナミック MAC アドレスは、関連 VLAN に複製されます。たとえば、セカンダリ VLAN で学習された MAC アドレスはプライマリ VLAN に複製されます。元のダイナミック MAC アドレスが削除されたり期限が切れた場合、複製アドレスは MAC アドレス テーブルから削除されます。

- レイヤ 3 VLAN インターフェイスをプライマリ VLAN に対してのみ設定します。

プライベート VLAN 内の VLAN の設定および対応付け

プライベート VLAN を設定するには、特権 EXEC モードで次の手順を行います。



(注) `private-vlan` コマンドは VLAN コンフィギュレーション モードを終了するまで機能しません。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vtp mode transparent</code>	VTP モードを透過に設定します (VTP をディセーブルにします)。
ステップ 3	<code>vlan vlan-id</code>	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 4	<code>private-vlan primary</code>	VLAN をプライマリ VLAN として指定します。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>vlan vlan-id</code>	(任意) VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 7	<code>private-vlan isolated</code>	VLAN を独立 VLAN として指定します。

	コマンド	目的
ステップ 8	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	vlan <i>vlan-id</i>	(任意) VLAN コンフィギュレーション モードを開始して、コミュニティ VLAN となる VLAN を指定するか作成します。VLAN ID の範囲は 2 ~ 1001 および 1006 ~ 4094 です。
ステップ 10	private-vlan community	VLAN をコミュニティ VLAN として指定します。
ステップ 11	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	vlan <i>vlan-id</i>	ステップ 2 で指定したプライマリ VLAN 用の VLAN コンフィギュレーション モードを開始します。
ステップ 13	private-vlan association [add remove] <i>secondary_vlan_list</i>	セカンダリ VLAN をプライマリ VLAN に関連付けます。
ステップ 14	end	特権 EXEC モードに戻ります。
ステップ 15	show vlan private-vlan [type] または show interfaces status	設定を確認します。
ステップ 16	copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。プライベート VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP 透過モード設定とプライベート VLAN 設定を保存する必要があります。保存しないと、スイッチをリセットした場合、デフォルトの VTP サーバ モードになり、プライベート VLAN をサポートしなくなります。

セカンダリ VLAN をプライマリ VLAN に関連付ける際に、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータにはスペースを含められません。項目を分けるためにカンマを複数使用できます。各項目には、単独のプライベート VLAN ID またはハイフンを使用したプライベート VLAN ID の範囲を指定できます。
- *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN を関連付けます。
- **remove** キーワードとともに *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN の関連付けを解除します。
- このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。

次に、VLAN 20 をプライマリ VLAN、VLAN 501 を独立 VLAN、VLAN 502 および 503 をコミュニティ VLAN として設定し、これらをプライベート VLAN 内で関連付けして、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
```

```
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
-----
Primary Secondary Type          Ports
-----
20      501      isolated
20      502      community
20      503      community
20      504      non-operational
```

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

レイヤ 2 インターフェイスをプライベート VLAN ホストポートとして設定し、これをプライマリおよびセカンダリ VLAN と関連付けるには、特権 EXEC モードで次の手順を実行します。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ 3	switchport mode private-vlan host	レイヤ 2 ポートをプライベート VLAN ホストポートとして設定します。
ステップ 4	switchport private-vlan host-association primary_vlan_id secondary_vlan_id	レイヤ 2 ポートをプライベート VLAN に関連付けます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces [interface-id] switchport	設定を確認します。
ステップ 7	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスをプライベート VLAN ホストポートとして設定し、これにプライベート VLAN ペアを関連付けて、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/22 switchport
Name: Gi1/0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```



```

Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)

```

<output truncated>

プライベート VLAN 混合ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN 混合ポートとして設定し、これをプライマリおよびセカンダリ VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface <i>interface-id</i>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 2 インターフェイスを指定します。
ステップ3	switchport mode private-vlan promiscuous	レイヤ 2 ポートをプライベート VLAN 混合ポートとして設定します。
ステップ4	switchport private-vlan mapping <i>primary_vlan_id</i> {add remove} <i>secondary_vlan_list</i>	プライベート VLAN 混合ポートをプライマリ VLAN と選択したセカンダリ VLAN にマッピングします。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show interfaces [<i>interface-id</i>] switchport	設定を確認します。
ステップ7	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

レイヤ 2 インターフェイスをプライベート VLAN 混合ポートとして設定した場合、構文に関して次のことに留意してください。

- *secondary_vlan_list* パラメータにはスペースを含められません。項目を分けるためにカンマを複数使用できます。各項目には、単独のプライベート VLAN ID またはハイフンを使用したプライベート VLAN ID の範囲を指定できます。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN とプライマリ VLAN をプライベート VLAN 混合ポートにマッピングします。
- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライベート VLAN 混合ポートのマッピングを解除します。

次に、インターフェイスをプライベート VLAN 混合ポートとして設定してそれをプライベート VLAN にマッピングする例を示します。インターフェイスはプライマリ VLAN 20 のメンバーで、セカンダリ VLAN 501～503 はこれにマッピングされます。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

スイッチ上のプライマリ VLAN、セカンダリ VLAN、およびプライベート VLAN ポートを表示する場合は、**show vlan private-vlan** または **show interface status** 特権 EXEC コマンドを使用します。

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

プライベート VLAN が VLAN 間ルーティングに使用される場合、SVI をプライマリ VLAN に設定してセカンダリ VLAN を SVI にマッピングできます。



(注) 独立およびコミュニティ VLAN はいずれもセカンダリ VLAN です。

セカンダリ VLAN をプライマリ VLAN の SVI にマッピングしてプライベート VLAN トラフィックのレイヤ 3 スイッチングを可能にするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface vlan primary_vlan_id	プライマリ VLAN でインターフェイス コンフィギュレーション モードを開始して VLAN を SVI として設定します。VLAN ID の範囲は 2～1001 および 1006～4094 です。
ステップ 3	private-vlan mapping [add remove] secondary_vlan_list	セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングしてプライベート VLAN 入力トラフィックのレイヤ 3 スイッチングを可能にします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interface private-vlan mapping	設定を確認します。
ステップ 6	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。



(注) **private-vlan mapping** インターフェイス コンフィギュレーション コマンドは、レイヤ 3 スイッチングされているプライベート VLAN トラフィックにのみ影響します。

セカンダリ VLAN をプライマリ VLAN のレイヤ 3 VLAN インターフェイスにマッピングする際、構文について次の点に留意してください。

- *secondary_vlan_list* パラメータにはスペースを含められません。項目を分けるためにカンマを複数使用できます。各項目には、単独のプライベート VLAN ID またはハイフンを使用したプライベート VLAN ID の範囲を指定できます。
- *secondary_vlan_list* を入力するか、または **add** キーワードを指定した *secondary_vlan_list* を使用してセカンダリ VLAN をプライマリ VLAN にマッピングします。

- **remove** キーワードを指定した *secondary_vlan_list* を使用して、セカンダリ VLAN とプライマリ VLAN のマッピングを解除します。

次に、VLAN 501 および 502 のインターフェイスを VLAN 10 にマッピングする例を示します。VLAN 10 では、プライベート VLAN 501 から 502 へのセカンダリ VLAN 入力トラフィックのルーティングが許可されます。

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan10      501          isolated
vlan10      502          community
```

プライベート VLAN のモニタリング

表 17-1 プライベート VLAN モニタリング コマンド

コマンド	目的
show interfaces status	所属する VLAN を含む、インターフェイスのステータスを表示します。
show vlan private-vlan [type]	スイッチ スタックのプライベート VLAN 情報を表示します。
show interface switchport	インターフェイス上のプライベート VLAN 設定を表示します。
show interface private-vlan mapping	VLAN SVI のプライベート VLAN マッピングに関する情報を表示します。

次に、**show vlan private-vlan** コマンドからの出力例を示します。

```
Switch(config)# show vlan private-vlan
Primary Secondary Type          Ports
-----
10      501      isolated      Fa2/0/1, Gi3/0/1, Gi3/0/3
10      502      community     Fa2/0/11, Gi3/0/1, Gi3/0/4

10      503      non-operational
```




CHAPTER 18

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

Virtual Private Network (VPN; バーチャル プライベート ネットワーク) では、多くの場合にイーサネットベースの共有インフラストラクチャである企業規模の接続に、プライベート ネットワークと同じセキュリティ、プライオリティ、信頼性、管理の容易さが提供されます。トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダー用に設計された機能です。Catalyst 3750 スイッチでは、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングがサポートされています。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「[IEEE 802.1Q トンネリングの概要](#)」 (P.18-1)
- 「[IEEE 802.1Q トンネリングの設定](#)」 (P.18-4)
- 「[レイヤ 2 プロトコル トンネリングの概要](#)」 (P.18-8)
- 「[レイヤ 2 プロトコル トンネリングの設定](#)」 (P.18-10)
- 「[トンネリング ステータスのモニタリングおよびメンテナンス](#)」 (P.18-18)

IEEE 802.1Q トンネリングの概要

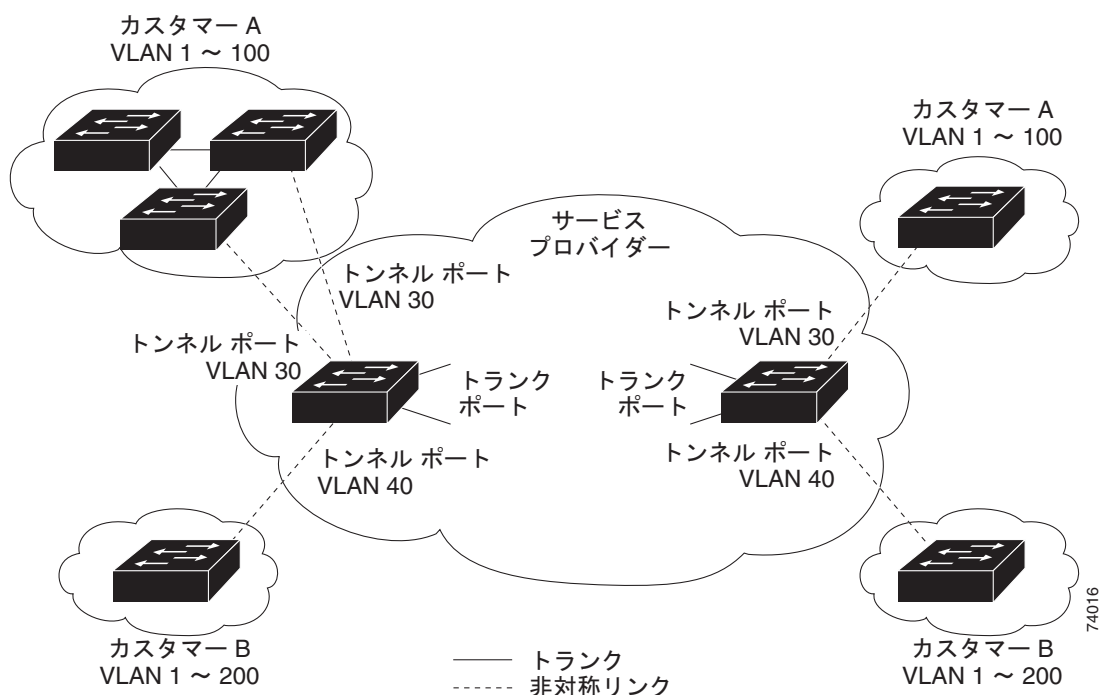
サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービス プロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混在することがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限 (4096) を簡単に越えてしまうことがあります。

サービス プロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID は、同一 VLAN に見えても保護され、さまざまなカスタマーのトラフィックは、サービス プロバイダー ネットワーク内で区別されます。IEEE 802.1Q トンネリングを使用すると、VLAN 内の VLAN 階層を使用してタグ付きパケットにタグを再び付けることで、VLAN 容量が拡大します。IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネルポートと呼ばれます。トンネリングを設定する場合は、トンネリング専用の VLAN ID にトンネルポートを割り当てます。それぞれのカスタマーには別個のサービス プロバイダー VLAN ID が必要ですが、その VLAN ID ではすべてのカスタマーの VLAN がサポートされます。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの IEEE 802.1Q トランク ポートからサービス プロバイダーのエッジスイッチのトンネルポートに発信されます。カスタマー デバイスとエッジスイッチ間のリンクは、片方が IEEE 802.1Q トランク ポートとして設定され、もう一方がトンネルポートとして設定されているので非対称です。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネルポート インターフェイスを割り当てます。

図 18-1 を参照してください。

図 18-1 サービス プロバイダー ネットワークの IEEE 802.1Q トンネルポート



カスタマーのトランク ポートからサービス プロバイダーのエッジスイッチのトンネルポートに発信されるパケットには、通常、適切な VLAN ID とともに IEEE 802.1Q タグが付いています。タグはスイッチ内でそのまま残り、タグ付きパケットがトランク ポートからサービス プロバイダー ネットワークに発信されると、カスタマーに固有の VLAN ID を含む IEEE 802.1Q タグの別のレイヤ（メトロ タグと呼ばれる）でカプセル化されます。カスタマーの元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービス プロバイダー ネットワークに入るパケットには、カスタマーのアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付いています。

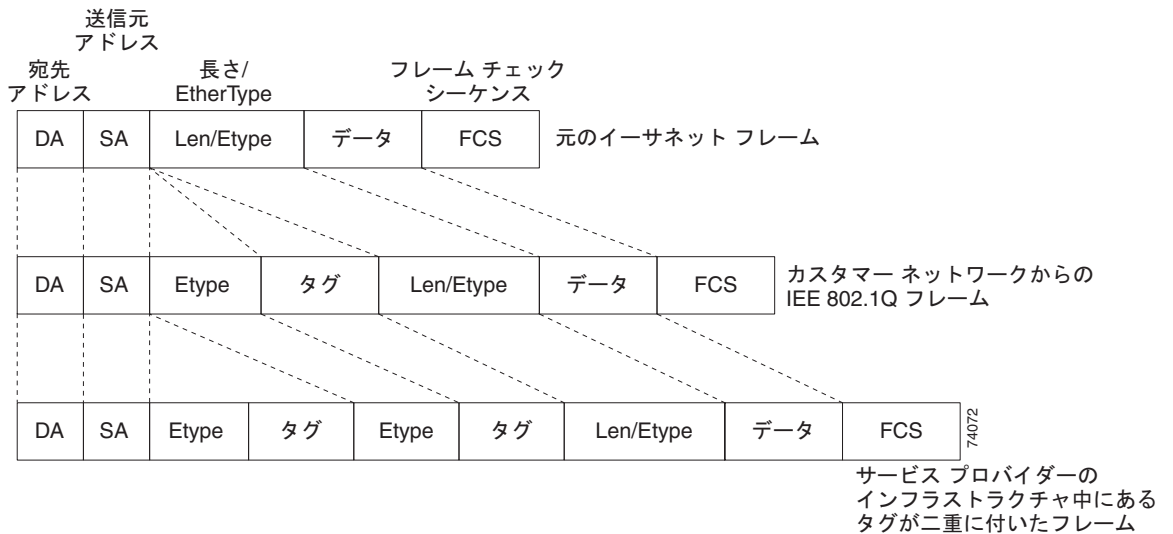
二重タグ パケットがサービス プロバイダー コア スイッチの別のトランク ポートに入ると、スイッチがパケットを処理する間に外部タグが外されます。パケットが、そのコア スイッチの別のトランク ポートを出るとき、同じメトロ タグがパケットに再び追加されます。図 18-2 は、二重タグ パケットのタグ構造です。



(注)

カプセル化された着信パケットによってそのトランク ポートが errdisable に変更されたため、トランク ポートからレイヤ 2 プロトコル設定を削除します。カプセル化された発信 VTP (CDP および STP) パケットが、そのトランクから廃棄されます。

図 18-2 元の (通常) イーサネット パケット、IEEE 802.1Q イーサネット パケット、二重タグ イーサネット パケットの形式



パケットがサービス プロバイダー 出力スイッチのトランク ポートに入ると、スイッチがパケットを内部処理する間に外部タグは再び外されます。しかしパケットがエッジ スイッチのトンネル ポートからカスタマー ネットワークに送信されるとき、メトロ タグは追加されません。パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

図 18-1 では、カスタマー A に VLAN 30 が、カスタマー B に VLAN 40 が割り当てられています。エッジ スイッチのトンネル ポートに入る、IEEE 802.1Q タグが付いたパケットには、サービス プロバイダー ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、サービス プロバイダー ネットワーク内で区別されます。それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービス プロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

発信トンネル ポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。トンネリングおよびタグ付けを複数のレベルにすることもできますが、このリリースのスイッチでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。エッジスイッチのトンネルポートを通してサービスプロバイダーネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、IEEE 802.1Q トランクポートでサービスプロバイダーネットワークを通じて送信される場合、メトロタグ VLAN ID（トンネルポートのアクセス VLAN に設定）でカプセル化されます。メトロタグのプライオリティフィールドは、トンネルポートで設定されているインターフェイス Class of Service (CoS; サービスクラス) プライオリティに設定されます（設定されていない場合、デフォルトはゼロです）。

802.1Q トンネリングはポート単位で設定されるため、スイッチがスタンドアロンであるか、またはスタックメンバーであるかは関係ありません。すべての設定は、スタックマスターで行われます。

IEEE 802.1Q トンネリングの設定

ここでは、次の設定情報について説明します。

- 「IEEE 802.1Q トンネリングのデフォルト設定」(P.18-4)
- 「IEEE 802.1Q トンネリング設定時の注意事項」(P.18-4)
- 「IEEE 802.1Q トンネリングおよびその他の機能」(P.18-6)
- 「IEEE 802.1Q トンネリングポートの設定」(P.18-7)

IEEE 802.1Q トンネリングのデフォルト設定

デフォルトの場合、デフォルトのスイッチポートモードが `dynamic auto` であるため、IEEE 802.1Q トンネルはディセーブルです。すべての IEEE 802.1Q トランクポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

IEEE 802.1Q トンネリング設定時の注意事項

IEEE 802.1Q トンネリングを設定する場合は、カスタマーデバイスおよびエッジスイッチの間で非対称リンクを常に使用する必要があります。カスタマーデバイスのポートを IEEE 802.1Q トランクポートに、エッジスイッチのポートをトンネルポートとして設定してください。

トンネリングに使用する VLAN だけにトンネルポートを割り当ててください。

ネイティブ VLAN および Maximum Transmission Unit (MTU; 最大伝送ユニット) の設定要件については、次のセクションで説明します。

ネイティブ VLAN

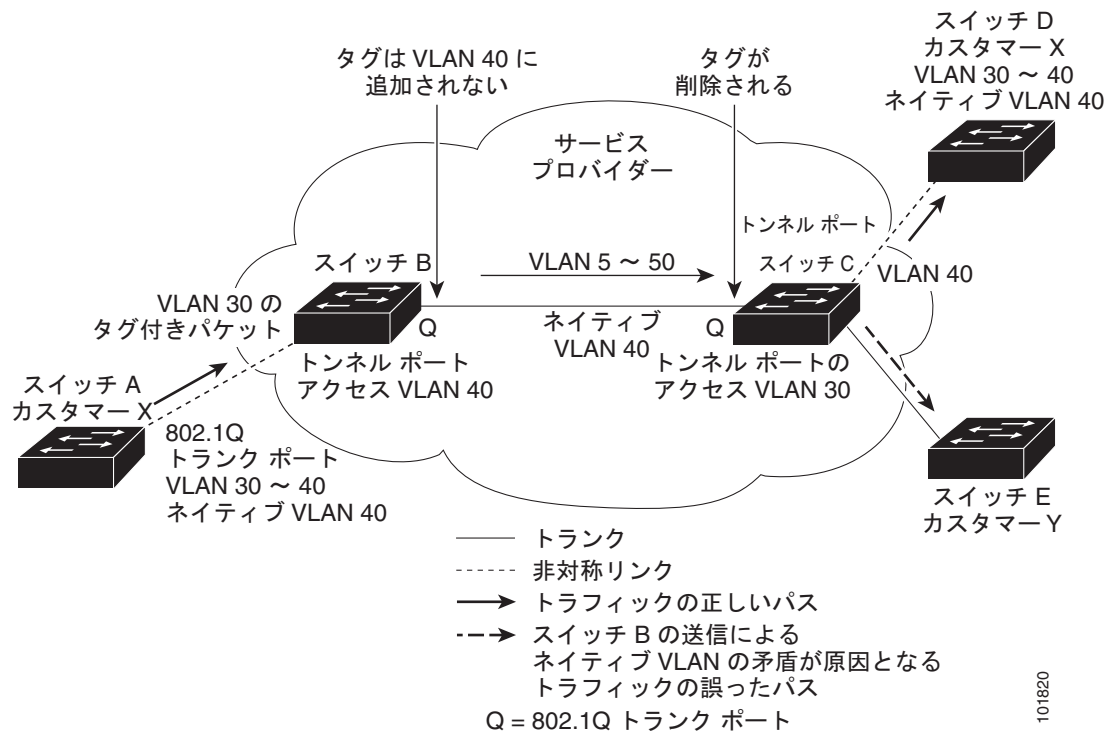
エッジスイッチで IEEE 802.1Q トンネリングを設定する場合は、サービスプロバイダーネットワークにパケットを送信するために、IEEE 802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダーネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL（スイッチ間リンク）トランク、非トランキングリンクのいずれかで送信できます。コアスイッチで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN を、同一スイッチの非トランキング（トンネリング）ポートのネイティブ VLAN と一致させることはできません。ネイティブ VLAN のトラフィックに、IEEE 802.1Q 送信トランクポートでタグが付かないためです。

図 18-3 を参照してください。VLAN 40 は、サービス プロバイダー ネットワークの入力エッジ スイッチ (スイッチ B) において、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービス プロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN (VLAN 40) は、エッジ スイッチのトランク ポートのネイティブ VLAN (VLAN 40) と同じなので、トンネル ポートから受信したタグ付きパケットにメトロタグは追加されません。パケットには VLAN 30 タグだけが付いて、サービス プロバイダー ネットワークで出力エッジ スイッチ (スイッチ C) のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

この問題の解決方法は次のとおりです。

- サービス プロバイダー ネットワークのコア スイッチ間で ISL トランクを使用します。エッジ スイッチに接続されているカスタマー インターフェイスは IEEE 802.1Q トランクとしますが、コア レイヤのスイッチの接続には ISL トランクの使用を推奨します。
- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用し、ネイティブ VLAN を含む、IEEE 802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジ スイッチを設定します。すべての IEEE 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。
- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲内でないことを確認します。たとえばトランク ポートが VLAN 100 ~ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

図 18-3 IEEE 802.1Q トンネリングおよびネイティブ VLAN に潜在する問題



101820

システム MTU

スイッチのトラフィックのデフォルト システム MTU は 1500 バイトです。 **system mtu** グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにファストイーサネット ポートを設定できます。 **system mtu jumbo** グローバル コンフィギュレーション コマンドを使用すると、1500 バイトより大きいフレームをサポートするようにギガビットイーサネット ポートを設定できます。 IEEE 802.1Q トンネリング機能では、メトロ タグが追加されると、フレーム サイズが 4 バイト増加するので、スイッチ システム MTU サイズを最低 1504 バイトに増加して最大フレームを処理できるように、サービス プロバイダー ネットワークのすべてのスイッチを設定する必要があります。ギガビットイーサネット インターフェイスの最大許容システム MTU は 9000 バイトです。ファストイーサネット インターフェイスの最大システム MTU は 1998 バイトです。

IEEE 802.1Q トンネリングおよびその他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スwitチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スwitチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。
- IEEE 802.1Q ポートを含む VLAN では IP ルーティングがサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基いて転送されます。トンネル ポートを含む Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) でルーティングがイネーブルである場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN でインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。
- フォールバック ブリッジングは、トンネル ポートでサポートされません。トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネル ポートが設定されている VLAN でフォールバック ブリッジングがイネーブルである場合、IP パケットは VLAN を越えて不適切にブリッジングされます。このため、トンネル ポートを含む VLAN ではフォールバック ブリッジングをイネーブルにしないでください。
- トンネル ポートでは IP Access Control List (ACL; アクセス コントロール リスト) がサポートされません。
- レイヤ 3 情報に関連するレイヤ 3 Quality of Service (QoS) ACL およびその他の QoS 機能は、トンネル ポートでサポートされません。MAC ベース QoS はトンネル ポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- Port Aggregation Protocol (PAgP; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、UniDirectional Link Detection (UDLD; 単一方向リンク検出) は、IEEE 802.1Q トンネリング ポートでサポートされます。
- トンネル ポートとトランク ポートで非対称リンクを手動で設定する必要があるため、Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) には IEEE 802.1Q トンネリングとの互換性がありません。
- VLAN Trunking Protocol (VTP) は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネル ポートとしてポートを設定すると、スパニング ツリー Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フィルタリングがインターフェイスで自動的にイネーブルになります。Cisco Discovery Protocol (CDP; シスコ検出プロトコル) および Layer Link Discovery Protocol (LLDP) は、インターフェイスで自動的にディセーブルになります。

IEEE 802.1Q トンネリング ポートの設定

IEEE 802.1Q トンネル ポートとしてポート設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	トンネル ポートとして設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1 ~ 48）が含まれます。
ステップ 3	switchport access vlan vlan-id	デフォルト VLAN を指定します。これは、インターフェイスがトランキングを停止した場合に使用されます。この VLAN ID は特定カスタマーに固有です。
ステップ 4	switchport mode dot1q-tunnel	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	vlan dot1q tag native	(任意) すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタグ付けをイネーブルにするようにスイッチを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show running-config show dot1q-tunnel	IEEE 802.1Q トンネリング用に設定したポートを表示します。 トンネリング モードになっているポートを表示します。
ステップ 9	show vlan dot1q tag native	IEEE 802.1Q ネイティブ VLAN タグ付けステータスを表示します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

dynamic desirable のデフォルト状態にポートを戻すには、**no switchport mode dot1q-tunnel** インターフェイス コンフィギュレーション コマンドを使用します。ネイティブ VLAN パケットのタグ付けをディセーブルにするには、**no vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用します。

以下は、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法の例です。この設定では、スタック メンバー 1 のインターフェイス Gigabit Ethernet 7 に接続するカスタマーの VLAN ID は、VLAN 22 になります。

```
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Port
-----

-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
Switch(config)# interface gigabitethernet1/0/7
Switch# show dot1q-tunnel interface gigabitethernet1/0/7
Gi1/0/1Port
```

レイヤ 2 プロトコル トンネリングの概要

サービス プロバイダー ネットワークを越えて接続されている、さまざまなサイトに散在するカスタマーは、さまざまなレイヤ 2 プロトコルを使用してトポロジをスケールし、すべてのリモート サイトおよびローカル サイトを含める必要があります。STP を適切に動作させる必要があります。サービス プロバイダー ネットワークを越えたローカル サイトおよびすべてのリモート サイトを含む、適切なスパンニング ツリーをすべての VLAN で構築する必要があります。CDP では、隣接するシスコ デバイスをローカル サイトおよびリモート サイトから検出する必要があります。VTP では、カスタマー ネットワークのすべてのサイトで矛盾しない VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルである場合、サービス プロバイダー ネットワークの着信側のエッジスイッチでは、特殊 MAC アドレスでレイヤ 2 プロトコル パケットがカプセル化され、サービス プロバイダー ネットワークを越えて送信されます。ネットワークのコアスイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、VTP のレイヤ 2 Protocol Data Unit (PDU; プロトコル データ ユニット) は、サービス プロバイダー ネットワークをまたがり、サービス プロバイダー ネットワークの発信側のカスタマー スイッチに配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信され、次のような結果になります。

- それぞれのカスタマー サイトのユーザは STP を適切に実行でき、すべての VLAN では、ローカル サイトだけではなく、すべてのサイトからのパラメータに基づいて、正しいスパンニング ツリーが構築されます。
- CDP では、サービス プロバイダー ネットワークによって接続されているその他のシスコ デバイスに関する情報が検出されて表示されます。
- VTP ではカスタマー ネットワーク全体で矛盾しない VLAN 設定が提供され、サービス プロバイダーを通してすべてのスイッチに伝播されます。



(注)

サードパーティベンダーとの相互運用性を提供するには、レイヤ 2 プロトコル トンネル バイパス機能を使用します。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。バイパス モードを実装するには、出力トランク ポートでレイヤ 2 プロトコル トンネリングをイネーブルにします。レイヤ 2 プロトコル トンネリングがトランク ポートでイネーブルの場合、カプセル化された MAC アドレスが削除されて、プロトコル パケットに通常の MAC アドレスを保有するようになります。

レイヤ 2 プロトコル トンネリングは個別に使用できます。レイヤ 2 プロトコル トンネリングでは、IEEE 802.1Q トンネリングを向上させることができます。IEEE 802.1Q トンネリング ポートでプロトコル トンネリングをイネーブルにしていない場合、サービス プロバイダー ネットワークの受信側のリモート スイッチでは PDU が受信せず、STP、CDP、VTP を適切に実行できません。プロトコル トンネリングがイネーブルである場合、それぞれのカスタマー ネットワークのレイヤ 2 プロトコルは、サービス プロバイダー ネットワーク内で動作しているものから完全に区別されます。IEEE 802.1Q トンネリングでサービス プロバイダー ネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。IEEE 802.1Q トンネリングを使用しない場合は、アクセス ポートでカスタマー スイッチに接続し、サービス プロバイダーのアクセス ポートでトンネリングをイネーブルにすることで、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば、[図 18-4](#) の場合、カスタマー X には同一 VLAN に 4 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネルされない場合、ネットワークの向こう側のスイッチでは、STP、CDP、VTP を適切に実行できません。たとえば、カスタマー X のサイト 1 内のスイッチ上の VLAN に対する STP は、サイト 2 のカスタマー X のスイッチに基づくコンバージェンス パラメータを考慮せずに、サイト 1 のスイッチ上にスパンニング ツリーを構築します。そのトポロジを[図 18-5](#) に示します。

図 18-4 レイヤ 2 プロトコル トンネリング

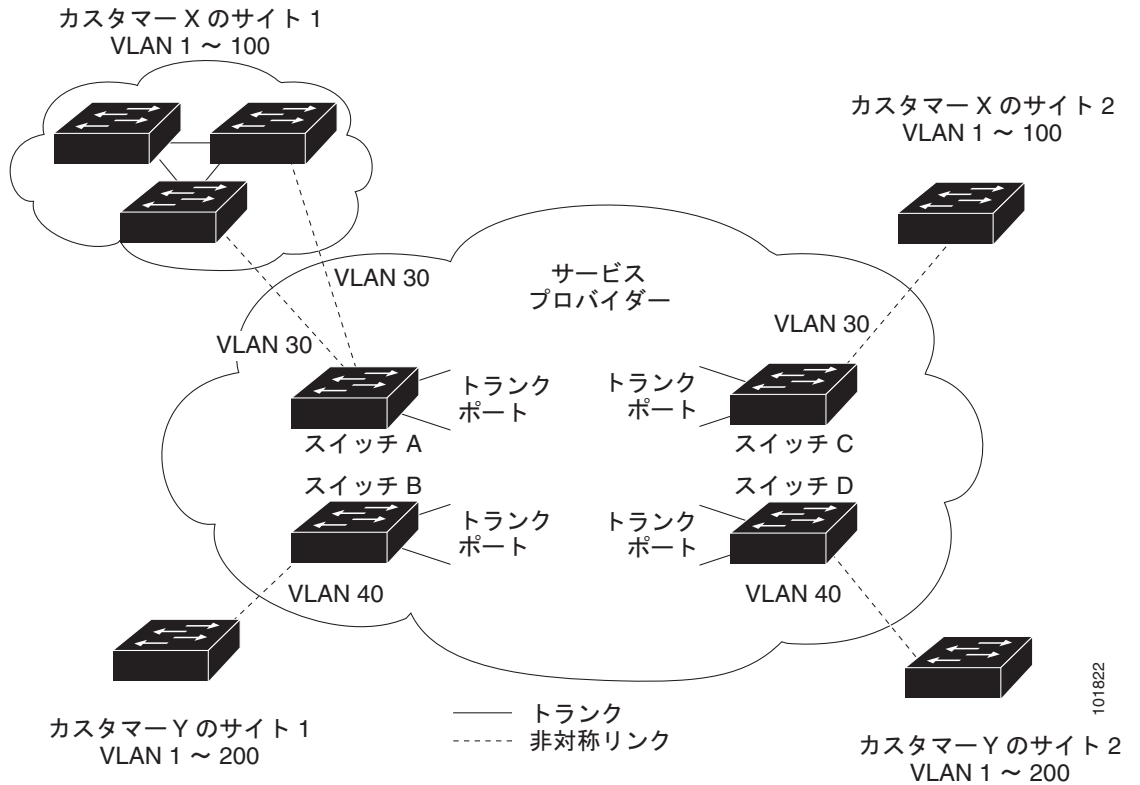
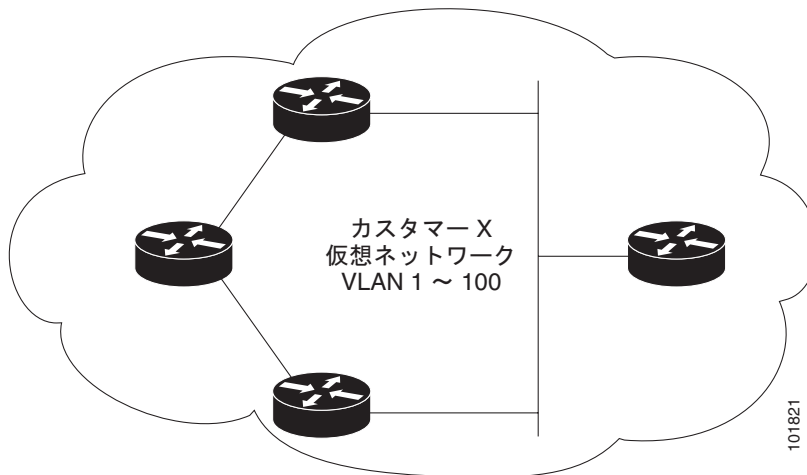


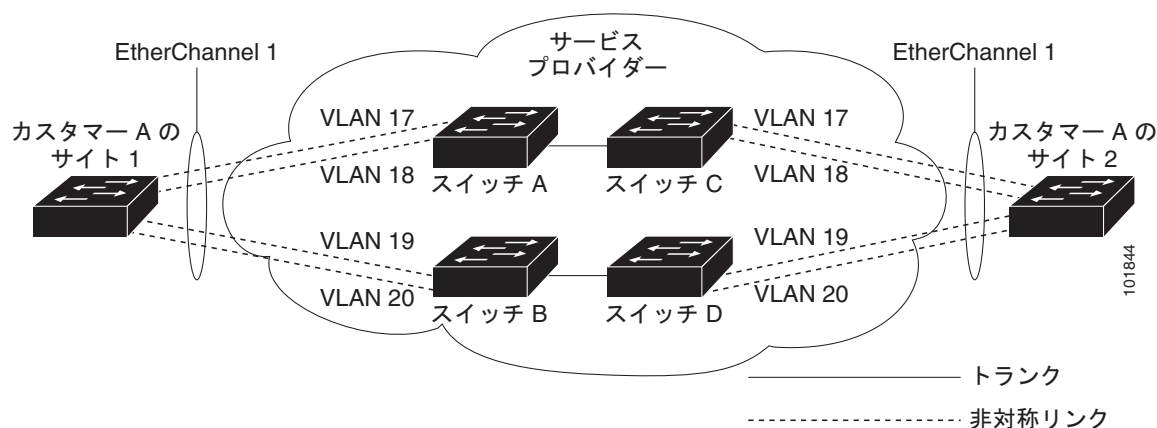
図 18-5 適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ



サービス プロバイダー ネットワークでは、レイヤ 2 プロトコル トンネリングを使用し、ポイントツウポイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を向上させることができます。サービス プロバイダー スイッチでプロトコル トンネリング (PAgP または LACP) をイネーブルにすると、リモート カスタマー スイッチでは PDU が受信され、EtherChannel の自動作成をネゴシエートできるようになります。

たとえば、図 18-6 の場合、カスタマー A には同一 VLAN に 2 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネリングされると、ネットワークの向こう側のスイッチでは、専用回線を必要とせずに、EtherChannel の自動作成をネゴシエートできます。手順については、「EtherChannel のレイヤ 2 トンネリングの設定」(P.18-15) を参照してください。

図 18-6 EtherChannel のレイヤ 2 プロトコル トンネリング



レイヤ 2 プロトコル トンネリングの設定

サービス プロバイダー ネットワークのエッジ スイッチで、カスタマーに接続されているポートにおいて、レイヤ 2 プロトコル トンネリングをプロトコルごとにイネーブルにできます。カスタマー スイッチに接続されているサービス プロバイダー エッジ スイッチでは、トンネリング処理が実行されます。エッジ スイッチ トンネル ポートは、カスタマーの IEEE 802.1Q トランク ポートに接続します。エッジ スイッチ アクセス ポートは、カスタマー アクセス ポートに接続します。カスタマー スイッチに接続されているエッジ スイッチでは、トンネリング処理が実行されます。

アクセス ポートまたはトンネル ポートのいずれかとして設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできます。スイッチポート モードが **dynamic auto** (デフォルト モード) に設定されているポートまたはスイッチポート モードが **dynamic desirable** に設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにすることができません。

スイッチでは、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングがサポートされます。ポイント ツーポイント ネットワーク トポロジのエミュレートの場合は、PAgP、LACP、UDLD のプロトコルもサポートされます。スイッチでは、LLDP のレイヤ 2 プロトコル トンネリングはサポートされません。



注意

PAgP、LACP、UDLD プロトコル トンネリングでは、ポイント ツーポイント トポロジのエミュレートだけが目的です。トンネリングされるパケットが多くのポートに送信されるエラー設定では、ネットワーク障害となることがあります。

レイヤ 2 プロトコルがイネーブルになっているポートでサービス プロバイダーの着信エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートからサービス プロバイダー ネットワークに出る場合、スイッチでは、カスタマー PDU 宛先 MAC アドレスが、周知のシスコ固有のマルチキャスト アドレス (01-00-0c-cd-cd-d0) で上書きされます。IEEE 802.1Q トンネリングがイネーブルである場合、パケットにはタグが二重に付きます。外部タグはカスタマーのメトロ タグであり、内部タグはカスタマーの VLAN タグです。コア スイッチでは内部タグが無視され、同じメトロ VLAN のすべてのトランク ポートにパケットが転送されます。発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートかアクセス ポートにパケットが転送されます。このため、レイヤ 2 PDU はそのまま残り、サービス プロバイダー インフラストラクチャを越えてカスタマー ネットワークの反対側に配信されます。

図 18-4 を参照してください。カスタマー X およびカスタマー Y が、それぞれアクセス VLAN 30 および 40 になっています。非対称リンクにより、サイト 1 のカスタマーは、サービス プロバイダー ネットワークのエッジ スイッチに接続されています。サイト 1 のカスタマー Y からスイッチ 2 に発信されたレイヤ 2 PDU (たとえば BPDU) は、周知の MAC アドレスが宛先 MAC アドレスになっている二重タグ パケットとしてインフラストラクチャに転送されます。この二重タグ パケットには、40 というメトロ VLAN タグ、および VLAN 100 などの内部 VLAN タグが付いています。二重タグ パケットがスイッチ D に入ると、外部 VLAN タグ 40 が外されて周知の MAC アドレスがそれぞれのレイヤ 2 プロトコル MAC アドレスで置き換わり、パケットは、VLAN 100 の一重タグ フレームとしてサイト 2 のカスタマー Y に送信されます。

カスタマー スイッチのアクセス ポートまたはトランク ポートに接続されているエッジ スイッチのアクセス ポートでも、レイヤ 2 プロトコル トンネリングをイネーブルにできます。この場合は、カプセル化プロセスとカプセル開放プロセスが、前の段落で説明したものと同じですが、パケットはサービス プロバイダー ネットワークで二重タグになりません。カスタマー固有のアクセス VLAN タグの一重タグになります。

レイヤ 2 プロトコル トンネリング設定は、すべてのスタック メンバー間に配信されます。ローカル ポート上で入力パケットを受信する各スタック メンバーは、パケットをカプセル化またはカプセル化解除して、該当する宛先ポートに転送します。単一のスイッチ上では、レイヤ 2 プロトコル トンネリング処理された入力トラフィックは、レイヤ 2 プロトコル トンネリングがイネーブルになっている同一 VLAN 上のすべてのローカル ポートに送信されます。スタックでは、レイヤ 2 プロトコル トンネリングの設定が行われたポートで受信したパケットを、スタック内のレイヤ 2 プロトコル トンネリングが設定され、同じ VLAN 内にあるすべてのポートに配信します。レイヤ 2 プロトコル トンネリング設定は、すべてスタック マスターにより取り扱われ、すべてのスタック メンバーに配信されます。

ここでは、次の設定情報について説明します。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」 (P.18-11)
- 「レイヤ 2 プロトコル トンネリング設定時の注意事項」 (P.18-12)
- 「レイヤ 2 プロトコル トンネリングの設定」 (P.18-13)
- 「EtherChannel のレイヤ 2 トンネリングの設定」 (P.18-15)

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 18-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 18-1 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウンしきい値	未設定。

表 18-1 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定 (続き)

機能	デフォルト設定
ドロップしきい値	未設定。
CoS 値	インターフェイスで CoS 値が設定されている場合は、その値を使用してレイヤ 2 プロトコル トンネリングの BPDU CoS 値を設定します。CoS 値がインターフェイス レベルで設定されていない場合、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 です。これはデータ トラフィックには当てはまりません。

レイヤ 2 プロトコル トンネリング設定時の注意事項

次に、レイヤ 2 プロトコル トンネリングの設定時の注意事項および動作特性を示します。

- スイッチでは、CDP、STP (Multiple STP (MSTP) を含む)、VTP のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- スイッチでは、スイッチポート モードが **dynamic auto** または **dynamic desirable** に設定されているポートにおいて、レイヤ 2 プロトコル トンネリングがサポートされません。
- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。
- サービス プロバイダー ネットワークの発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル 情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートおよびアクセス ポートにパケットが転送されます。
- サードパーティ ベンダー スイッチとの相互運用性のため、スイッチではレイヤ 2 プロトコル トンネル バイパス機能がサポートされます。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。スイッチの入力ポートでレイヤ 2 プロトコル トンネルがイネーブルである場合は、出力トランク ポートにより、トンネリングされたパケットが特殊なカプセル化で転送されます。出力トランク ポートでもレイヤ 2 プロトコル トンネリングをイネーブルにすると、この動作がバイパスされて、スイッチによって、処理や修正が行われずに制御 PDU が転送されます。
- スイッチでは、ポイントツーポイント ネットワーク トポロジのエミュレートの場合、PAgP、LACP、UDLD のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- PAgP トンネリングまたは LACP トンネリングの場合は、リンク障害検出を高速にするため、インターフェイスで UDLD もイネーブルにすることを推奨します。
- PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのレイヤ 2 プロトコル トンネリングでは、ループバック検出がサポートされません。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ 2 トンネリングがイネーブルになっているトンネル ポートまたはアクセス ポートから受信される場合、トンネル ポートは、ループを防止するためにシャットダウンされます。このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。**shutdown** コマンドに続けて **no shutdown** コマンドを入力すると、ポートを再び手動でイネーブルにできます。**errdisable recovery** がイネーブルである場合は、指定された間隔で動作が再試行されます。

- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。サービス プロバイダー ネットワーク上で動作しているスパンニング ツリー インスタンスでは、BPDU がトンネル ポートに転送されません。CDP パケットはトンネル ポートから転送されません。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのシャットダウンしきい値やポートごとのシャットダウンしきい値を設定できます。制限を越えると、ポートはシャットダウンされます。QoS ACL およびポリシー マップをトンネル ポートで使用すると、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのドロップしきい値やポートごとのドロップしきい値を設定できます。制限を越えると、ポートが PDU を受信するレートがドロップしきい値未満になるまで、ポートで PDU が廃棄されます。
- トンネリングされた PDU (特に STP BPDU) は、カスタマーの仮想ネットワークが正しく動作するためにすべてのリモート サイトに配信される必要があるため、同じトンネル ポートから受信されるデータ パケットよりも PDU のプライオリティをサービス プロバイダー ネットワーク内で高くできます。デフォルトの場合、PDU ではデータ パケットと同じ CoS 値が使用されます。

レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング用にポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、トンネル ポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスは、物理インターフェイスおよびポートチャネル論理インターフェイス (ポート チャネル 1 ~ 48) です。
ステップ 3	<code>switchport mode access</code> または <code>switchport mode dot1q-tunnel</code>	アクセス ポートまたは IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 4	<code>l2protocol-tunnel [cdp stp vtp]</code>	目的のプロトコルのプロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのレイヤ 2 プロトコルでイネーブルになります。
ステップ 5	<code>l2protocol-tunnel shutdown-threshold [cdp stp vtp] value</code>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値は、ドロップしきい値以上とする必要があります。

レイヤ 2 プロトコル トンネリングの設定

コマンド	目的
ステップ 6 l2protocol-tunnel drop-threshold [cdp stp vtp] value	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値は、シャットダウンしきい値以下である必要があります。
ステップ 7 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8 errdisable recovery cause l2ptguard	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 9 l2protocol-tunnel cos value	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 10 end	特権 EXEC モードに戻ります。
ステップ 11 show l2protocol	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 12 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel [cdp | stp | vtp]** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp]** コマンドおよび **no l2protocol-tunnel drop-threshold [cdp | stp | vtp]** コマンドを使用します。

以下は、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する方法の例です。


```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port          Protocol Shutdown Drop      Encapsulation Decapsulation Drop
              Threshold Threshold Counter      Counter      Counter
-----
Fa1/0/11     cdp          1500    1000 2288          2282          0
              stp          1500    1000 116           13            0
              vtp          1500    1000 3             67            0
              pagp         ----     ----  0             0             0
              lacp         ----     ----  0             0             0
              udld         ----     ----  0             0             0
```

EtherChannel のレイヤ 2 トンネリングの設定

レイヤ 2 ポイントツーポイント トンネリングを設定して EtherChannel の自動作成を容易にするには、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチの両方を設定する必要があります。

サービス プロバイダー エッジ スイッチの設定

EtherChannel のレイヤ 2 プロトコル トンネリング用にサービス プロバイダー エッジ スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、トンネルポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスは物理インターフェイスです。
ステップ 3	<code>switchport mode dot1q-tunnel</code>	IEEE 802.1Q トンネル ポートとしてインターフェイスを設定します。
ステップ 4	<code>l2protocol-tunnel point-to-point [pagp lacp udld]</code>	(任意) 目的のプロトコルのポイントツーポイント プロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つのすべてのプロトコルでイネーブルになります。  注意 ネットワーク障害を避けるため、ネットワークがポイントツーポイント トポロジになっていることを確認してから、PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのトンネリングをイネーブルにしてください。
ステップ 5	<code>l2protocol-tunnel shutdown-threshold [point-to-point [pagp lacp udld]] value</code>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値は、ドロップしきい値以上とする必要があります。
ステップ 6	<code>l2protocol-tunnel drop-threshold [point-to-point [pagp lacp udld]] value</code>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。 (注) このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値は、シャットダウンしきい値以下である必要があります。
ステップ 7	<code>no cdp enable</code>	インターフェイス上で CDP をディセーブルにします。
ステップ 8	<code>spanning-tree bpdudfilter enable</code>	インターフェイス上で BPDU フィルタリングをイネーブルにします。

■ レイヤ 2 プロトコル トンネリングの設定

	コマンド	目的
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	<code>errdisable recovery cause l2ptguard</code>	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。 <code>errdisable recovery</code> はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 11	<code>l2protocol-tunnel cos value</code>	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show l2protocol</code>	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには、**`no l2protocol-tunnel [point-to-point [pagp | lacp | udld]]`** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**`no l2protocol-tunnel shutdown-threshold [point-to-point [pagp | lacp | udld]]`** コマンドおよび **`no l2protocol-tunnel drop-threshold [[point-to-point [pagp | lacp | udld]]`** コマンドを使用します。

カスタマー スイッチの設定

サービス プロバイダー エッジ スイッチを設定したら、特権 EXEC モードで次の手順を実行し、EtherChannel のレイヤ 2 プロトコル トンネリング用にカスタマー スイッチを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチ ポートにする必要があります。
ステップ 3	<code>switchport trunk encapsulation dot1q</code>	トランキング カプセル化形式を IEEE 802.1Q に設定します。
ステップ 4	<code>switchport mode trunk</code>	インターフェイス上でトランキングをイネーブルにします。
ステップ 5	<code>udld enable</code>	インターフェイスの通常モードで UDLD をイネーブルにします。
ステップ 6	<code>channel-group channel-group-number mode desirable</code>	チャンネル グループにインターフェイスを割り当て、PAgP モードに <code>desirable</code> を指定します。EtherChannel の設定の詳細については、 第 37 章「EtherChannel およびリンクステート トラッキングの設定」 を参照してください。
ステップ 7	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	<code>interface port-channel port-channel number</code>	ポートチャンネル インターフェイス モードに入ります。
ステップ 9	<code>shutdown</code>	インターフェイスをシャットダウンします。
ステップ 10	<code>no shutdown</code>	インターフェイスをイネーブルにします。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 12 show l2protocol	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**no switchport mode trunk**、**no udld enable**、**no channel group channel-group-number mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel の場合は、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります (図 18-6 (P.18-10) を参照)。

次に、サービス プロバイダーのエッジ スイッチ 1 およびエッジ スイッチ 2 を設定する方法の例を示します。VLAN 17、18、19、20 はアクセス VLAN、ファストイーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、ドロップ しきい値は 1000、ファストイーサネット インターフェイス 3 はトランク ポートです。

サービス プロバイダー エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
```

Service Provider (サービス プロバイダー; SP) エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
```

次に、サイト 1 のカスタマー スイッチを設定する方法の例を示します。ファストイーサネット インターフェイス 1、2、3、4 は IEEE 802.1Q トランキンング用に設定されており、UDLD はイネーブル、EtherChannel グループ 1 はイネーブル、ポート チャネルはシャットダウンされたあとでイネーブルになって EtherChannel 設定がアクティブになります。

```

Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# uddld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# uddld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# uddld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# uddld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit

```

トンネリング ステータスのモニタリングおよびメンテナンス

表 18-2 は、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングのモニタリングとメンテナンスを行う特権 EXEC コマンドの説明です。

表 18-2 トンネリングのモニタリングおよびメンテナンスのためのコマンド

コマンド	目的
<code>clear l2protocol-tunnel counters</code>	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
<code>show dot1q-tunnel</code>	スイッチの IEEE 802.1Q トンネル ポートを表示します。
<code>show dot1q-tunnel interface interface-id</code>	特定インターフェイスがトンネル ポートであるかどうかを確認します。
<code>show l2protocol-tunnel</code>	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
<code>show errdisable recovery</code>	レイヤ 2 プロトコル トンネル エラー ディセーブル状態からの回復タイマーがイネーブルかどうかを確認します。
<code>show l2protocol-tunnel interface interface-id</code>	特定レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
<code>show l2protocol-tunnel summary</code>	レイヤ 2 プロトコルのサマリー情報だけを表示します。
<code>show vlan dot1q tag native</code>	スイッチのネイティブ VLAN タグのステータスを表示します。

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



CHAPTER 19

STP の設定

この章では、Catalyst 3750 スイッチのポートベース VLAN 上で Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) を設定する方法について説明します。このスイッチは、IEEE 802.1D 標準に準拠した Per-VLAN Spanning-Tree plus (PVST+) とシスコ独自の拡張機能の組み合わせか、もしくは IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) プロトコルのいずれかを使用できます。スイッチ スタックはネットワークの他の部分からは単一のスパニング ツリー ノードと見なされ、すべてのスタック メンバーが同じブリッジ ID を使用します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

Multiple Spanning-Tree Protocol (MSTP) および複数の VLAN を同一のスパニング ツリー インスタンスにマッピングする方法については、第 20 章「MSTP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどのその他のスパニング ツリーの機能については、第 21 章「オプションのスパニング ツリー機能の設定」を参照してください。



(注)

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

この章で説明する内容は、次のとおりです。

- 「スパニング ツリー機能の概要」(P.19-1)
- 「スパニング ツリー機能の設定」(P.19-13)
- 「スパニング ツリー ステータスの表示」(P.19-25)

スパニング ツリー機能の概要

ここでは、次の概要について説明します。

- 「STP の概要」(P.19-2)
- 「スパニング ツリー トポロジと BPDU」(P.19-3)
- 「ブリッジ ID、スイッチ プライオリティ、および拡張システム ID」(P.19-5)
- 「スパニング ツリー インターフェイス ステート」(P.19-5)
- 「スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み」(P.19-8)
- 「スパニング ツリーおよび冗長接続」(P.19-9)
- 「スパニング ツリー アドレスの管理」(P.19-9)
- 「接続を維持するためのエイジング タイムの短縮」(P.19-10)
- 「スパニング ツリー モードおよびプロトコル」(P.19-10)

- 「サポートされるスパニング ツリー インスタンス」 (P.19-11)
- 「スパニング ツリーの相互運用性と下位互換性」 (P.19-11)
- 「STP および IEEE 802.1Q トランク」 (P.19-12)
- 「VLAN ブリッジ スパニング ツリー」 (P.19-12)
- 「スパニング ツリーとスイッチ スタック」 (P.19-12)

設定手順については、「スパニング ツリー機能の設定」 (P.19-13) を参照してください。

オプションのスパニング ツリー機能については、第 21 章「オプションのスパニング ツリー機能の設定」を参照してください。

STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークを正しく動作させるには、2 つのステーション間に存在するアクティブ パスは 1 つでなければなりません。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ 2 インターフェイスのエンドステーション MAC (メディア アクセス制御) アドレスを学習する可能性があります。このような条件が発生すると、不安定なネットワークになります。スパニング ツリーの動作は透過的であり、エンドステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出できません。

STP は、スパニング ツリー アルゴリズムを使用し、スパニング ツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニング ツリー アルゴリズムは、アクティブ トポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニング ツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニング ツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルートスイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

冗長データ パスはスパニング ツリーによって、強制的にスタンバイ (ブロックされた) ステートにされます。スパニング ツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニング ツリー アルゴリズムがスパニング ツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的に Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) と呼ばれるスパニング ツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニング ツリーはこの情報を使用して、スイッチド ネットワーク用のルートスイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニング ツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニング ツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。



(注)

デフォルトでは、Small Form-Factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュールを搭載していないインターフェイス上でのみ、スイッチがキープアライブ メッセージを (接続が有効かを確認するため) 送信します。[no] keepalive インターフェイス コンフィギュレーション コマンドを使用してインターフェイスのデフォルトを変更することができます。

スパンニング ツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパンニング ツリー トポロジは、次の要素によって制御されます。

- 各スイッチのそれぞれの VLAN に対応付けられた一意のブリッジ ID (スイッチ プライオリティおよび MAC アドレス)。スイッチ スタックでは、すべてのスイッチが指定のスパンニング ツリー インスタンスに対して同じブリッジ ID を使用します。
- ルート スイッチに対するスパンニング ツリー パス コスト。
- 各レイヤ 2 インターフェイスに対応付けられたポート ID (ポート プライオリティおよび MAC アドレス)。

ネットワーク内のスイッチに電源が投入されると、それぞれがルート スイッチとして機能します。各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパンニング ツリー トポロジが計算されます。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側スイッチがルート スイッチと見なしたスイッチの一意のブリッジ ID
- ルートに対するスパンニング ツリー パス コスト
- 送信側スイッチのブリッジ ID
- メッセージの有効期間
- 送信側インターフェイス ID
- Hello タイマー、転送遅延タイマー、および最大エージング プロトコル タイマーの値

スイッチは、*優位*の情報 (より小さいブリッジ ID、より低いパス コストなど) を格納したコンフィギュレーション BPDU を受信すると、そのポートのためにこの情報を保存します。スイッチは、この BPDU をルート ポートで受信した場合は、更新されたメッセージ付きで、自身が指定スイッチであるすべての接続 LAN に対して BPDU を転送します。

そのポートに対して現在保存されているものより *下位*の情報を格納したコンフィギュレーション BPDU を受信した場合は、BPDU は廃棄されます。スイッチが、下位 BPDU の送信元の LAN の指定スイッチである場合は、そのポート用に保存された最新情報を格納した BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 台のスイッチがルート スイッチ (スイッチド ネットワークのスパンニング ツリー トポロジの論理的な中心) として選択されます。スイッチ スタックでは、1 つのスタック メンバーがスタック ルート スイッチとして選択されます。図 19-1 (P.19-4) に示すとおり、スタック ルート スイッチには出力ルート ポート (スイッチ 1) が含まれます。

各 VLAN で、スイッチのプライオリティが最も高い (プライオリティ値が数値的に最も小さい) スイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリティ (32768) で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルート スイッチになります。スイッチのプライオリティ値は、ブリッジ ID の最上位ビットを占めます (表 19-1 (P.19-5) を参照)。

- 各スイッチ（ルートスイッチを除く）に対して 1 つのルートポートが選択されます。このポートは、スイッチによってパケットがルートスイッチに転送されるときに、最適なパス（最小コスト）を提供します。

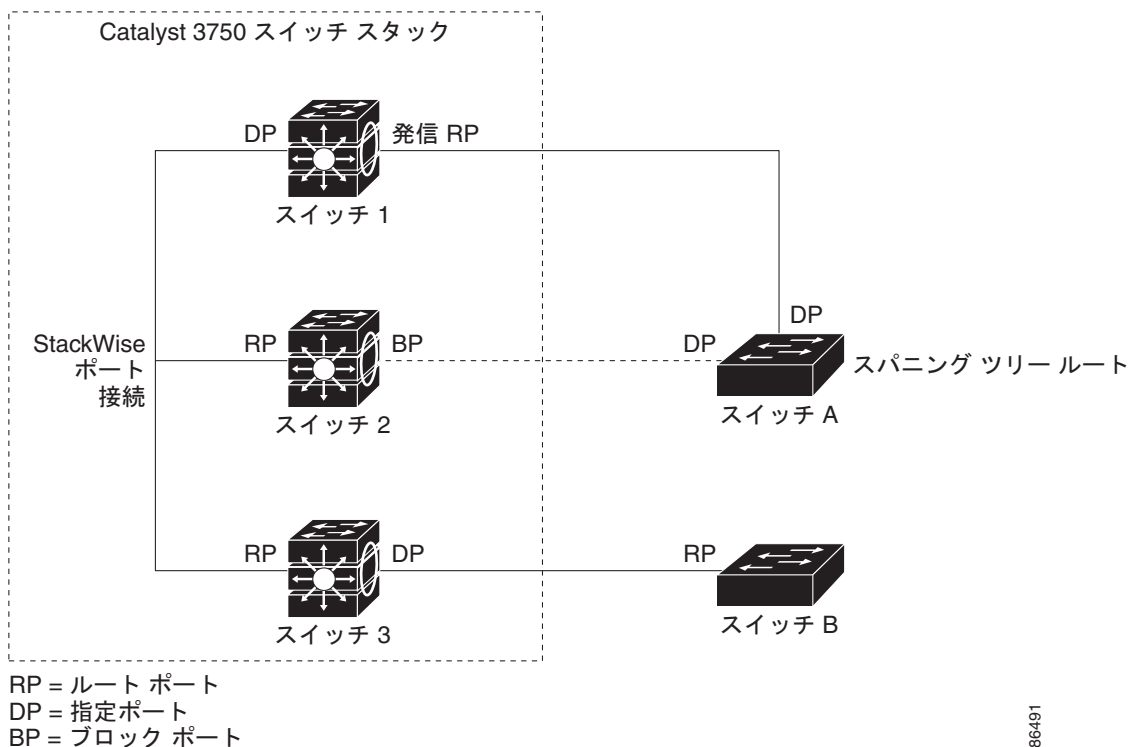
スパニング ツリーは、次の順序でスイッチ スタックのルートポートを選択します。

- 最小のルートブリッジ ID を選択します。
- ルートスイッチへのパスコストが最小のものを選択します。
- 最小の指定ブリッジ ID を選択します。
- 最小の指定パスコストを選択します。
- 最小のポート ID を選択します。

スタック ルートスイッチの 1 つの出力ポートだけが、ルートポートとして選択されます。図 19-1 (P.19-4) に示すとおり、スタック内の残りのスイッチは指定スイッチ（スイッチ 2 およびスイッチ 3）になります。

- スイッチごとに、パスコストに基づいてルートスイッチまでの最短距離が計算されます。
- 各 LAN セグメントの指定スイッチが選定されます。指定スイッチでは、LAN からルートスイッチへのパケット転送の場合、パスコストが最小となります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

図 19-1 スイッチ スタックのスパニング ツリー ポートのステート



スイッチド ネットワーク上のすべての地点からルートスイッチに到達する場合に必要なパスはすべて、スパニング ツリー ブロックモードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチに一意のブリッジ識別子（ブリッジ ID）を設定する必要があります。この ID によってルート スイッチの選択が制御されます。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のスイッチは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。スイッチ上の各 VLAN には一意の 8 バイトブリッジ ID が設定されます。上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチでは IEEE 802.1t スパンニング ツリー拡張機能がサポートされ、従来はスイッチ プライオリティに使用されていたビットの一部が VLAN ID として使用されるようになりました。その結果、スイッチに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるようになり、しかもブリッジ ID の一意性を損なうこともありません。表 19-1 に示すように、従来はスイッチ プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値（VLAN ID と同じ）に割り当てられています。

表 19-1 スイッチ プライオリティ値および拡張システム ID

スイッチ プライオリティ値				拡張システム ID (VLAN ID と同じに設定)											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパンニング ツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパンニング ツリー MAC アドレスを使用します。スイッチ スタックはネットワークの他の部分からは単一のスイッチと見なされるため、スタック内のすべてのスイッチが指定のスパンニング ツリーに対して同じブリッジ ID を使用します。スタック マスターに障害が生じると、スタック メンバーは新たなスタック メンバーの新規 MAC アドレスに基づいて、すべての実行スパンニング ツリーのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。たとえば、スイッチのプライオリティ値を変更すると、ルート スイッチとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。詳細については、「[ルート スイッチの設定](#)」(P.19-17)、「[セカンダリ ルート スイッチの設定](#)」(P.19-18)、および「[VLAN のスイッチ プライオリティの設定](#)」(P.19-22) を参照してください。

スパンニング ツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するときに、伝播遅延が生じる可能性があります。その結果、スイッチド ネットワークのさまざまな場所で、さまざまな時期に、トポロジの変更が起こる可能性があります。インターフェイスがスパンニング ツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニング ツリーを使用しているスイッチの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

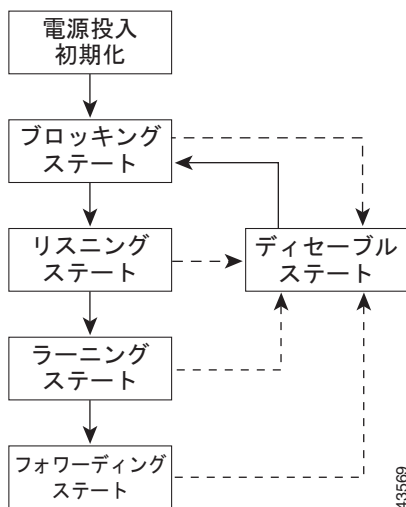
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニング ツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニング ツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニング ツリー インスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 19-2 に、インターフェイスがステートをどのように移行するかを示します。

図 19-2 スパニング ツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニング ツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニング ツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニング ツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニング ツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。

2. スパニング ツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートで、スイッチがデータベース転送のためにエンド ステーションの位置情報を学習している間、インターフェイスはフレーム転送を引き続きブロックします。
4. 転送遅延タイマーが満了すると、スパニング ツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまで、ルートとして動作します。この BPDU 交換によって、ネットワーク上のどのスイッチがルート、すなわちルート スイッチであるかが確立されます。ネットワークにスイッチが 1 台しかない場合、交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニング ステートになります。インターフェイスはスイッチの初期化後、必ずブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ 2 インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニング ツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ディセーブル ステートのレイヤ 2 インターフェイスは、フレームの転送やスパニング ツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

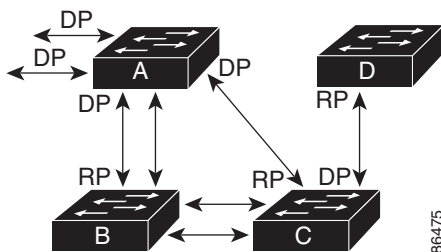
ディセーブル インターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパニング ツリー設定でイネーブルになっている場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。図 19-3 では、スイッチ A がルート スイッチとして選定されます（すべてのスイッチのスイッチ プライオリティがデフォルト (32768) に設定されており、スイッチ A の MAC アドレスが最小であるため）。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパニング ツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 19-3 スパニング ツリー トポロジ



RP = ルート ポート
DP = 指定ポート

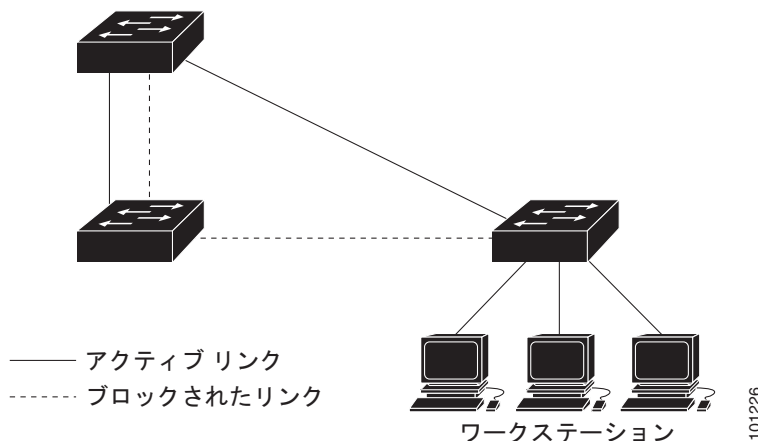
スパンニング ツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが理想です。

たとえば、スイッチ B のあるポートがギガビット イーサネット リンクで、別のポート (10/100 リンク) がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リンクに流す方が効率的です。ギガビット イーサネット ポートのスパンニング ツリー ポート プライオリティをルート ポートより高くする (数値を小さくする) と、ギガビット イーサネット ポートが新しいルート ポートになります。

スパンニング ツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の 1 台のデバイス、または 2 台の異なるデバイスに接続することにより、スパンニング ツリーを使用して冗長バックボーンを作成できます (図 19-4 を参照)。スパンニング ツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート プライオリティとポート ID が加算され、値の小さいリンクがスパンニング ツリーによってディセーブルにされます。

図 19-4 スパンニング ツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。詳細については、第 37 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

スパンニング ツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ~ 0x00180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパンニング ツリー ステートに関係なく、スタック内の各スイッチは 0x00180C2000000 ~ 0x00180C200000F のアドレス宛のバケットを受信しますが、転送は行いません。

スパニング ツリーがイネーブルな場合、スタック内の各スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛ての packets を受信します。スパニング ツリーがディセーブルな場合は、スタック内の各スイッチは、それらの packets を不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルト値です。ただし、スパニング ツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、アドレス テーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。スパニング ツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値 (**spanning-tree vlan vlan-id forward-time seconds** グローバル コンフィギュレーション コマンド) と同じです。

各 VLAN はそれぞれ独立したスパニング ツリー インスタンスなので、スイッチは VLAN 単位でエージング タイムを短縮します。ある VLAN でスパニング ツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージング タイムがそのまま適用されます。

スパニング ツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

- **PVST+** : このスパニング ツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。すべてのイーサネット ポートベースの VLAN で使用されるスパニング ツリーのデフォルト モードです。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリーパスを提供します。

PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルートスイッチがあります。このルートスイッチは、その VLAN に対応するスパニング ツリー情報を、ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネットワークに関する共通の情報を持つようになるので、ネットワーク トポロジが確実に維持されます。

- **Rapid PVST+** : このスパニング ツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージング タイムが使用されます。

Rapid PVST+ は PVST+ と同じ設定を使用しているため（特に明記する場合を除く）、必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行するのに、複雑な MSTP 設定の学習やネットワーク再設定の必要がないことです。Rapid PVST+ モードでは、各 VLAN は独自のスパニング ツリー インスタンスを最大数実行します。

- **MSTP** : このスパニング ツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパニング ツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニング ツリー インスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol (RSTP; 高速スパニング ツリー プロトコル) (IEEE 802.1w 準拠) 上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行するこ

とにより、スパンニング ツリーの高速コンバージェンスを可能にします。スイッチ スタックでは、Cross-Stack Rapid Transition (CSRT) 機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用せずに MSTP を稼動することはできません。

MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの配備です。詳細については、第 20 章「MSTP の設定」を参照してください。

サポートされるスパンニング ツリー インスタンス数については、次のセクションを参照してください。

サポートされるスパンニング ツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチ スタックは最大 128 のスパンニング ツリー インスタンスをサポートします。

MSTP モードでは、スイッチ スタックは最大 65 MST インスタンスをサポートします。特定の MST インスタンスにマッピングできる VLAN の数に制限はありません。

スパンニング ツリーと VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) の相互作用については、「スパンニング ツリー設定時の注意事項」(P.19-14) を参照してください。

スパンニング ツリーの相互運用性と下位互換性

表 19-2 に、ネットワークでサポートされるスパンニング ツリー モード間の相互運用性と下位互換性を示します。

表 19-2 PVST+、MSTP、および Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり (制限あり)	あり (PVST+ に戻る)
MSTP	あり (制限あり)	あり	あり (PVST+ に戻る)
Rapid PVST+	あり (PVST+ に戻る)	あり (PVST+ に戻る)	あり

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree (CST) のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ が稼動しているスイッチと PVST+ が稼動しているスイッチが存在する場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパンニング ツリー インスタンスにすることを推奨します。Rapid PVST+ スパンニング ツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでなければなりません。PVST+ スイッチはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが同じバージョンのスパンニング ツリーを稼動します (すべて PVST+、すべて Rapid PVST+、またはすべて MSTP)。

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニング ツリー ストラテジに一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1 つのスパニング ツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクによって接続されたシスコ製スイッチのネットワークでは、スイッチはトランク上で使用できる各 VLAN に 1 つずつ、スパニング ツリー インスタンスを維持します。

IEEE 802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続する場合、シスコ製スイッチは PVST+ を使用してスパニング ツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパニング ツリー インスタンスと他社の IEEE 802.1Q スwitchのスパニング ツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q スwitchからなるクラウドにより分離されたシスコ製スイッチによって維持されます。シスコ製スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありません。アクセス ポートおよび Inter-Switch Link (ISL; スイッチ間リンク) トランク ポートでの外部スパニング ツリーの動作は、PVST+ の影響を受けません。

IEEE 802.1Q トランクの詳細については、第 14 章「VLAN の設定」を参照してください。

VLAN ブリッジ スパニング ツリー

シスコ VLAN ブリッジ スパニング ツリーは、フォールバック ブリッジング機能 (ブリッジ グループ) で使用し、DECnet などの IP 以外のプロトコルを 2 つ以上の VLAN ブリッジ ドメインまたはルーテッド ポート間で伝送します。VLAN ブリッジ スパニング ツリーにより、ブリッジ グループは個々の VLAN スパニング ツリーの上部にスパニング ツリーを形成できるので、VLAN 間で複数の接続がある場合に、ループが形成されないようにします。また、ブリッジングされている VLAN からの個々のスパニング ツリーが単一のスパニング ツリーに縮小しないようにする働きもします。

VLAN ブリッジ スパニング ツリーをサポートするには、一部のスパニング ツリー タイマーを増やします。フォールバック ブリッジング機能を使用するには、スイッチに IP サービス イメージをインストールする必要があります。詳細については、第 48 章「フォールバック ブリッジングの設定」を参照してください。

スパニング ツリーとスイッチ スタック

次のことは、スイッチ スタックが PVST+ モードまたは Rapid PVST+ モードで稼動している場合に当てはまります。

- スイッチ スタックはネットワークの他の部分からは単一のスパニング ツリー ノードと見なされ、すべてのスタック メンバーが指定のスパニング ツリーに対して同じブリッジ ID を使用します。ブリッジ ID は、スタック マスターの MAC アドレスを基にして作成されます。
- 新たなスイッチがスタックに加入すると、そのブリッジ ID はスタック マスターのブリッジ ID に設定されます。新たに追加されたスイッチが最小の ID を持ち、すべてのスタック メンバーのルートパス コストが同一の場合は、新たに追加されたスイッチがスタック ルートになります。
- スタック メンバーがスタックを脱退すると、スタック内 (スタック外部も含まれる場合がある) でスパニング ツリーの再コンバージェンスが実行されます。残りのスタック メンバーのうち最小のスタック ポート ID を持つものがスタック ルートになります。

- スタック マスターに障害が生じたり、それがスタックから脱退したりした場合は、スタック メンバーの中から新たなスタック マスターが選択され、すべてのスタック メンバーが自分のスパンニング ツリーブリッジ ID を新たなマスターのブリッジ ID に変更します。
- スイッチ スタックがスパンニング ツリー ルートであり、スタック マスターに障害が生じたか、スタック マスターがスタックから脱退した場合は、スタック メンバーの中から新たなスタック マスターが選択され、スパンニング ツリーの再コンバージェンスが実行されます。
- スイッチ スタック外部の近接スイッチに障害が生じたか、近接スイッチの電源が切断された場合は、通常のスパンニング ツリー プロセスが実行されます。スパンニング ツリーの再コンバージェンスは、アクティブ トポロジ内でスイッチが失われた結果として実行されます。
- スイッチ スタック外部の新たなスイッチがネットワークに追加された場合は、通常のスパンニング ツリー プロセスが実行されます。スパンニング ツリーの再コンバージェンスは、ネットワーク内にスイッチが追加された結果として実行されます。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

スパンニング ツリー機能の設定

ここでは、次の設定情報について説明します。

- 「スパンニング ツリー機能のデフォルト設定」(P.19-13)
- 「スパンニング ツリー設定時の注意事項」(P.19-14)
- 「スパンニング ツリー モードの変更」(P.19-15) (必須)
- 「スパンニング ツリーのディセーブル化」(P.19-16) (任意)
- 「ルート スイッチの設定」(P.19-17) (任意)
- 「セカンダリ ルート スイッチの設定」(P.19-18) (任意)
- 「ポート プライオリティの設定」(P.19-19) (任意)
- 「パス コストの設定」(P.19-21) (任意)
- 「VLAN のスイッチ プライオリティの設定」(P.19-22) (任意)
- 「スパンニング ツリー タイマーの設定」(P.19-23) (任意)

スパンニング ツリー機能のデフォルト設定

表 19-3 に、スパンニング ツリー機能のデフォルト設定を示します。

表 19-3 スパンニング ツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル 詳細については、「サポートされるスパンニング ツリー インスタンス」(P.19-11) を参照してください。
スパンニング ツリー モード	PVST+ (Rapid PVST+ と MSTP はディセーブル)
スイッチ プライオリティ	32768
スパンニング ツリー ポート プライオリティ (インターフェイス単位で設定可能)	128

表 19-3 スパニング ツリー機能のデフォルト設定 (続き)

機能	デフォルト設定
スパニング ツリー ポート コスト (インターフェイス単位で設定可能)	1000 Mb/s : 4 100 Mb/s : 19 10 Mb/s : 100
スパニング ツリー VLAN ポート プライオリティ (VLAN 単位で設定可能)	128.
スパニング ツリー VLAN ポート コスト (VLAN 単位で設定可能)	1000 Mb/s : 4 100 Mb/s : 19 10 Mb/s : 100
スパニング ツリー タイマー	Hello タイム : 2 秒 転送遅延時間 : 15 秒 最大エージング タイム : 20 秒 転送保留カウント : 6 BPDU

スパニング ツリー設定時の注意事項

各スタック メンバーは専用のスパニング ツリーを稼動し、スタック全体はネットワークの他の部分からは単一のスイッチとして見なされます。

VTP にスパニング ツリー インスタンスよりも多くの VLAN が定義されている場合、PVST+ または Rapid PVST+ をイネーブルにできるのは、スイッチ スタックあたり 128 の VLAN に限られます。残りの VLAN は、スパニング ツリーがディセーブルの状態で作動します。ただし、MSTP を使用して複数の VLAN を同一のスパニング ツリー インスタンスにマッピングすることが可能です。詳細については、第 20 章「MSTP の設定」を参照してください。

128 のスパニング ツリー インスタンスがすでに使用されている場合、VLAN の 1 つでスパニング ツリーをディセーブルにして、STP を稼動させたい別の VLAN でイネーブルにできます。no **spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して、特定の VLAN でスパニング ツリーをディセーブルにし、**spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用して、所定の VLAN でスパニング ツリーをイネーブルにします。



注意

スパニング ツリーが稼動していないスイッチは、スパニング ツリー インスタンスが稼動している VLAN 上の他のスイッチがループを切断できるように、受信した BPDU を引き続き転送します。したがって、スパニング ツリーは、ネットワーク上のすべてのループを切断できるように十分な数のスイッチ上で稼動している必要があります。たとえば、VLAN の各ループで少なくとも 1 台のスイッチがスパニング ツリーを稼動している必要があります。VLAN 内のすべてのスイッチでスパニング ツリーを稼動させる必要はありません。ただし、最小限の数のスイッチだけでスパニング ツリーが稼動している状況では、不注意なネットワーク変更によって VLAN に別のループが発生し、ブロードキャスト ストームを引き起こす可能性があります。



(注)

スイッチ上の使用可能なスパンニング ツリー インスタンスをすべて使い切ってしまったあとに、VTP ドメイン内にさらに別の VLAN を追加すると、そのスイッチ上にスパンニング ツリーが稼動しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リストが設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパンニング ツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパンニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。ただし、ネットワークに VLAN を追加するときより多くの作業を伴うことになるので、通常、許可リストの設定は必要ありません。

VLAN スパンニング ツリー インスタンスの設定はスパンニング ツリー コマンドによって制御されます。スパンニング ツリー インスタンスは、VLAN にインターフェイスを割り当てるときに作成します。スパンニング ツリー インスタンスは最終インターフェイスが別の VLAN に移されたときに削除されます。スパンニング ツリー インスタンスの作成前に、スイッチとポートのパラメータを設定できます。設定されたパラメータは、スパンニング ツリー インスタンスを作成するときに適用されます。

スイッチは、PVST+、Rapid PVST+、および MSTP をサポートしますが、アクティブにできるバージョンは常に 1 つだけです (たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります)。すべてのスタック メンバーが同じバージョンのスパンニング ツリーを稼動します。さまざまなスパンニング ツリー モードおよび相互運用性については、「スパンニング ツリーの相互運用性と下位互換性」(P.19-11) を参照してください。

UplinkFast、BackboneFast、およびクロススタック UplinkFast 設定時の注意事項については、「オプションのスパンニング ツリー設定時の注意事項」(P.21-12) を参照してください。



注意

ループ ガードは、ポイントツーポイント リンクに限りサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

スパンニング ツリー モードの変更

スイッチは、3 つのスパンニング ツリー モード (PVST+、Rapid PVST+、MSTP) をサポートします。デフォルトで、スイッチは PVST+ プロトコルを使用します。

スパンニング ツリー モードを変更するには、特権 EXEC モードで次の手順を実行します。デフォルトモード以外のモードをイネーブルにする場合、この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mode {pvst mst rapid-pvst}</code>	スパンニング ツリー モードを設定します。すべてのスタック メンバーが同じバージョンのスパンニング ツリーを稼動します。 <ul style="list-style-type: none"> <code>pvst</code> を指定して、PVST+ をイネーブルにします (デフォルト設定)。 <code>mst</code> を指定して、MSTP (および RSTP) をイネーブルにします。設定手順の詳細については、第 20 章「MSTP の設定」を参照してください。 <code>rapid-pvst</code> を指定して、Rapid PVST+ をイネーブルにします。

コマンド	目的
ステップ 3 <code>interface interface-id</code>	(Rapid PVST+ モードの場合のみ推奨) 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポートチャネルがあります。指定できる VLAN ID 範囲は 1 ~ 4094 です。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 4 <code>spanning-tree link-type point-to-point</code>	(Rapid PVST+ モードの場合のみ推奨) このポートのリンク タイプをポイントツーポイントに指定します。 このポート (ローカル ポート) をポイントツーポイントリンクでリモート ポートと接続し、ローカル ポートが指定ポートになると、スイッチはリモート ポートとネゴシエーションし、ローカル ポートをフォワーディング ステートに高速変更します。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>clear spanning-tree detected-protocols</code>	(Rapid PVST+ モードの場合のみ推奨) スイッチ上の任意のポートが IEEE 802.1D 準拠のレガシー スイッチのポートと接続されている場合に、スイッチ全体でプロトコル移行プロセスを再開します。 このステップは、このスイッチで Rapid PVST+ が稼動していることを指定スイッチが検出する場合のオプションです。
ステップ 7 <code>show spanning-tree summary</code> および <code>show spanning-tree interface interface-id</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree mode** グローバル コンフィギュレーション コマンドを使用します。ポートをデフォルト設定に戻すには、**no spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。

スパニング ツリーのディセーブル化

スパニング ツリーはデフォルトで、VLAN 1 および「サポートされるスパニング ツリー インスタンス」(P.19-11) のスパニング ツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニング ツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。



注意

スパニング ツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

VLAN 単位でスパニング ツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>no spanning-tree vlan vlan-id</code>	<code>vlan-id</code> に指定できる範囲は、1 ~ 4094 です。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。

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

スパンニング ツリーを再びイネーブルにするには、`spanning-tree vlan vlan-id` グローバル コンフィギュレーション コマンドを使用します。

ルート スイッチの設定

スイッチは、スイッチ上で設定されているアクティブ VLAN ごとに 1 つずつ、個別のスパンニング ツリー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるブリッジ ID が対応付けられます。VLAN ごとに、ブリッジ ID が最小のスイッチがその VLAN のルート スイッチになります。

特定の VLAN でスイッチがルートになるように設定するには、`spanning-tree vlan vlan-id root` グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値 (32768) からかなり小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

指定された VLAN のルート スイッチに 24576 未満のスイッチ プライオリティが設定されている場合、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (表 19-1 (P.19-5) に示すように、4096 は 4 ビットのスイッチ プライオリティ値の最下位ビットの値です)。



(注) ルート スイッチとして設定する必要がある値が 1 未満の場合、`spanning-tree vlan vlan-id root` グローバル コンフィギュレーション コマンドは失敗します。



(注) ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼動する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。



(注) 各スパンニング ツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリビューション スイッチにする必要があります。アクセス スイッチをスパンニング ツリーのプライマリ ルートとして設定しないでください。

レイヤ 2 ネットワークの直径 (つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンド ステーション間の最大スイッチ ホップ数) を指定するには、`diameter` キーワードを指定します。ネットワークの直径を指定すると、その直径のネットワークに最適な Hello タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。自動的に算出された Hello タイムを変更するには、`hello` キーワードを使用します。



(注) ルート スイッチとして設定したあとで、**spanning-tree vlan *vlan-id* hello-time**、**spanning-tree vlan *vlan-id* forward-time**、および **spanning-tree vlan *vlan-id* max-age** グローバル コンフィギュレーション コマンドを使用して、Hello タイム、転送遅延時間、および最大エージング タイムを手動で設定することは推奨できません。

スイッチが特定の VLAN のルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan <i>vlan-id</i> root primary [<i>diameter net-diameter</i> [<i>hello-time seconds</i>]]	指定された VLAN のルートになるように、スイッチを設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 (任意) <i>diameter net-diameter</i> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。 (任意) <i>hello-time seconds</i> には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 です。デフォルトは 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree detail	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻すには、**no spanning-tree vlan *vlan-id* root** グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値 (32768) から 28672 に変更されます。したがって、プライマリ ルート スイッチで障害が発生した場合に、このスイッチが指定された VLAN のルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree vlan *vlan-id* root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および Hello タイム値を使用してください。

スイッチが特定の VLAN のセカンダリ ルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>spanning-tree vlan <i>vlan-id</i> root secondary [diameter <i>net-diameter</i> [hello-time <i>seconds</i>]]</code>	指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 <ul style="list-style-type: none"> <code>vlan-id</code> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 (任意) <code>diameter net-diameter</code> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。 (任意) <code>hello-time seconds</code> には、ルートスイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 です。デフォルトは 2 です。 プライマリ ルートスイッチを設定したときと同じネットワーク直径および Hello タイム値を使用してください。「 ルートスイッチの設定 」(P.19-17) を参照してください。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4 <code>show spanning-tree detail</code>	設定を確認します。
ステップ 5 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻すには、`no spanning-tree vlan vlan-id root` グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、Spanning Tree はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには高いプライオリティ (小さい数値) を与え、最後に選択させたいインターフェイスには低いプライオリティ (大きい数値) を与えます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、Spanning Tree はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。



(注) スイッチがスイッチ スタックのメンバーの場合は、`spanning-tree [vlan vlan-id] port-priority priority` インターフェイス コンフィギュレーション コマンドの代わりに、`spanning-tree [vlan vlan-id] cost cost` インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするインターフェイスを選択する必要があります。最初に選択させたいインターフェイスには小さいコスト値を、最後に選択させたいインターフェイスには大きいコスト値を割り当てます。詳細については、「[パス コストの設定](#)」(P.19-21) を参照してください。

インターフェイスのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス (port-channel <i>port-channel-number</i>) です。
ステップ 3	<code>spanning-tree port-priority priority</code>	インターフェイスにポート プライオリティを設定します。 <i>priority</i> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルト値は 128 です。有効な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティは高くなります。
ステップ 4	<code>spanning-tree vlan vlan-id port-priority priority</code>	VLAN にポート プライオリティを設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>priority</i> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルト値は 128 です。有効な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティは高くなります。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show spanning-tree interface interface-id</code> または <code>show spanning-tree vlan vlan-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree interface interface-id` 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能な状態にある場合に限られます。それ以外の情報については、`show running-config interface` 特権 EXEC コマンドを使用して設定を確認してください。

デフォルトの設定値に戻す場合は、`no spanning-tree [vlan vlan-id] port-priority` インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリー ポート プライオリティを使用してトランク ポートに負荷分散を設定する手順については、「[トランク ポートの負荷分散の設定](#)」(P.14-23) を参照してください。

パス コストの設定

スパンニング ツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパンニング ツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコスト値が与えられている場合、スパンニング ツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス (port-channel port-channel-number) です。
ステップ 3	<code>spanning-tree cost cost</code>	インターフェイスにコストを設定します。 ループが発生した場合、スパンニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、高速で伝送されます。 <i>cost</i> に指定できる範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度に基づきます。
ステップ 4	<code>spanning-tree vlan vlan-id cost cost</code>	VLAN にコストを設定します。 ループが発生した場合、スパンニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、高速で伝送されます。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>cost</i> に指定できる範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度に基づきます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show spanning-tree interface interface-id</code> または <code>show spanning-tree vlan vlan-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree interface interface-id` 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能な状態にある場合に限られます。それ以外の情報については、`show running-config` 特権 EXEC コマンドを使用して設定を確認してください。

デフォルトの設定値に戻す場合は、**no spanning-tree [vlan vlan-id] cost** インターフェイス コンフィギュレーション コマンドを使用します。スパニング ツリー パス コストを使用してトランク ポートに負荷分散を設定する手順については、「トランク ポートの負荷分散の設定」(P.14-23) を参照してください。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定して、スタンドアロン スイッチまたはスタック内のスイッチがルート スイッチとして選択される可能性を高めることができます。



(注) このコマンドは、十分に注意して使用してください。スイッチ プライオリティの変更には、通常は、**spanning-tree vlan vlan-id root primary** および **spanning-tree vlan vlan-id root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id priority priority	VLAN のスイッチ プライオリティを設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>priority</i> に指定できる範囲は 0 ~ 61440 で、4096 ずつ増加します。デフォルト値は 32768 です。この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 有効なプライオリティ値は、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻すには、**no spanning-tree vlan vlan-id priority** グローバル コンフィギュレーション コマンドを使用します。

スパンニング ツリー タイマーの設定

表 19-4 で、スパンニング ツリーのパフォーマンス全体を左右するタイマーについて説明します。

表 19-4 スパンニング ツリー タイマー

変数	説明
Hello タイマー	スイッチから他のスイッチへ Hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を制御します。
最大エージング タイマー	インターフェイスが受信したプロトコル情報をスイッチに保存させておく時間を制御します。
転送保留カウント	1 秒間停止する前に送信できる BPDU 数を制御します。

以下に設定手順を示します。

Hello タイムの設定

Hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を設定できます。



(注)

このコマンドは、十分に注意して使用してください。Hello タイムの変更には、通常、**spanning-tree vlan *vlan-id* root primary** および **spanning-tree vlan *vlan-id* root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN の Hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i>	VLAN の Hello タイムを設定します。Hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。 <ul style="list-style-type: none"> <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <i>seconds</i> に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan <i>vlan-id</i>	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan *vlan-id* hello-time** グローバル コンフィギュレーション コマンドを使用します。

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i></code>	VLAN の転送時間を設定します。転送遅延時間は、スパニング ツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 <ul style="list-style-type: none"> <code>vlan-id</code> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <code>seconds</code> に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree vlan <i>vlan-id</i></code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、`no spanning-tree vlan vlan-id forward-time` グローバル コンフィギュレーション コマンドを使用します。

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i></code>	VLAN の最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニング ツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 <ul style="list-style-type: none"> <code>vlan-id</code> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 <code>seconds</code> に指定できる範囲は 6 ~ 40 です。デフォルト値は 20 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree vlan <i>vlan-id</i></code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree vlan *vlan-id* max-age** グローバル コンフィギュレーション コマンドを使用します。

転送保留カウンタの設定

転送保留カウンタ値を変更することで、BPDU のバースト サイズを設定できます。



(注)

このパラメータをより高い値に変更すると、CPU の使用率が非常に大きくなります (Rapid PVST モード時に特に顕著に変化します)。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

転送保留カウンタを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree transmit hold-count <i>value</i>	1 秒間停止する前に送信できる BPDU 数を設定します。 <i>value</i> に指定できる範囲は 1 ~ 20 です。デフォルト値は 6 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree detail	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、**no spanning-tree transmit hold-count *value*** グローバル コンフィギュレーション コマンドを使用します。

スパンニング ツリー ステータスの表示

スパンニング ツリー ステータスを表示するには、表 19-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 19-5 スパンニング ツリー ステータス表示用のコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパンニング ツリー情報だけを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface <i>interface-id</i>	特定のインターフェイスのスパンニング ツリー情報を表示します。
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。または STP ステート セクションのすべての行を表示します。

clear spanning-tree [interface *interface-id*] 特権 EXEC コマンドを使用して、スパンニング ツリー カウンタをクリアできます。

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。

■ スパニング ツリー ステータスの表示



CHAPTER 20

MSTP の設定

この章では、Catalyst 3750 スイッチに IEEE 802.1s Multiple STP (MSTP) のシスコ実装を設定する方法について説明します。



(注)

Multiple Spanning-Tree (MST; スパニング ツリー) の実装は、IEEE 802.1s 標準に準拠しています。Cisco IOS Release 12.2(25)SEC 以前の Cisco IOS リリースは、先行標準に準拠しています。

MSTP は複数の VLAN を同一のスパニング ツリー インスタンスにマッピングできるようにして、多数の VLAN をサポートする場合に必要なスパニング ツリー インスタンスの数を減らします。MSTP は、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを可能にします。MSTP を使用すると、1 つのインスタンス (転送パス) で障害が発生しても他のインスタンス (転送パス) は影響を受けないので、ネットワークのフォールト トレランスが向上します。MSTP を導入する場合、最も一般的なのは、レイヤ 2 スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネットワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の Rapid Spanning-Tree Protocol (RSTP) が自動的にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定 ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニング ツリーの高速コンバージェンスを実現します。

RSTP と MSTP は、(オリジナル) IEEE 802.1D スパニング ツリー準拠デバイス、既存のシスコ独自の Multiple Instance STP (MISTP)、および既存のシスコ Per-VLAN Spanning-Tree plus (PVST+) との下位互換性を保ちながら、スパニング ツリーの動作を向上させます。PVST+ および Rapid PVST+ については、第 19 章「STP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどのその他のスパニング ツリーの機能については、第 21 章「オプションのスパニング ツリー機能の設定」を参照してください。

スイッチ スタックは、ネットワークの他の部分からは単一のスパニング ツリー ノードと見なされ、すべてのスタック メンバーが同じスイッチ ID を使用します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「MSTP の概要」(P.20-2)
- 「RSTP の概要」(P.20-10)

- 「MSTP 機能の設定」(P.20-15)
- 「MST コンフィギュレーションおよびステータスの表示」(P.20-28)

MSTP の概要

MSTP は、高速コンバージェンスが可能な RSTP を使用し、複数の VLAN を 1 つのスパニング ツリー インスタンスにまとめます。各インスタンスのスパニング ツリー トポロジは、他のスパニング ツリー インスタンスの影響を受けません。このアーキテクチャによって、データ トラフィックに複数の転送パスが提供され、ロード バランシングが可能になり、また多数の VLAN をサポートするのに必要なスパニング ツリー インスタンスの数を減らすことができます。

ここでは、MSTP の機能について説明します。

- 「MST リージョン」(P.20-2)
- 「IST、CIST、および CST」(P.20-3)
- 「ホップ カウント」(P.20-6)
- 「境界ポート」(P.20-6)
- 「IEEE 802.1s の実装」(P.20-7)
- 「MSTP とスイッチ スタック」(P.20-9)
- 「IEEE 802.1D STP との相互運用性」(P.20-9)

設定手順については、「MSTP 機能の設定」(P.20-15) を参照してください。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定しなければなりません。同じ MST コンフィギュレーションを持ち、相互接続されたスイッチの集合を MST リージョンといいます (図 20-1 (P.20-4) を参照)。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって制御されます。MST コンフィギュレーションには、リージョン名、リビジョン番号、MST の VLAN とインスタンスの割り当てマップが保存されています。スイッチにリージョンを設定するには、そのスイッチで **spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用して、MST コンフィギュレーション モードを開始します。このモードでは、**instance MST** コンフィギュレーション コマンドを使用して VLAN を MST インスタンスにマッピングし、**name MST** コンフィギュレーション コマンドを使用してリージョン名を指定し、**revision MST** コンフィギュレーション コマンドを使用してリビジョン番号を設定できます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバーが必要です。さらに、各メンバーは、RSTP Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニング ツリー インスタンスの数は 65 までです。インスタンスは 0 ~ 4094 の数字で識別されます。1 つの VLAN を同時に複数のスパニング ツリー インスタンスに割り当てることはできません。

IST、CIST、および CST

すべてのスパニング ツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の 2 種類のスパニング ツリーを確立して維持します。

- **Internal Spanning-Tree (IST)** は、1 つの MST リージョン内で稼動するスパニング ツリーです。各 MST リージョン内の MSTP は複数のスパニング ツリー インスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他の MST インスタンスはすべて 1 ~ 4094 まで番号が付けられます。

IST は、BPDU を送受信する唯一のスパニング ツリー インスタンスです。他のスパニング ツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。

MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニング ツリー インスタンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポジ パラメータ (ルート スイッチ ID、ルート パス コストなど) を持っています。デフォルトでは、すべての VLAN が IST に割り当てられています。

MST インスタンスはリージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されていても、リージョン A の MST インスタンス 1 は、リージョン B の MST インスタンス 1 から独立しています。

- **Common and Internal Spanning-Tree (CIST)** は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニング ツリーを相互接続する **Common Spanning-Tree (CST)** の集合です。

1 つのリージョン内で計算されたスパニング ツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニング ツリー アルゴリズムによって形成されます。

MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内の動作」(P.20-3) および「MST リージョン間の動作」(P.20-4) を参照してください。



(注) IEEE 802.1s 標準を実装すると、一部の MST 実装関連の用語が変更されます。これらの変更の要約については、表 19-1 (P.19-5) を参照してください。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは、図 20-1 (P.20-4) のように、CIST リージョナル ルート (IEEE 802.1s 標準が実装される以前は *IST* マスター) になります。CIST ルートに対してリージョン内で最も低いスイッチ ID とパス コストを持つスイッチがルートになります。また、リージョンがネットワーク内に 1 つしかなければ、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主張するため、CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると主張します。スイッチは、ポートに現在保存されているルート情報よりも優位の MST ルート情報 (小さいスイッチ ID、パス コストなど) を受信すると、CIST リージョナル ルートとしての主張を撤回します。

初期化中、リージョン内にそれぞれが CIST リージョナルルートである多数のサブリージョンが存在する場合があります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナルルートが含まれている新しいサブリージョンに加入します。このようにして、真の CIST リージョナルルートが含まれているサブリージョン以外のサブリージョンはすべて縮小させます。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナルルートを承認する必要があります。共通の CIST リージョナルルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

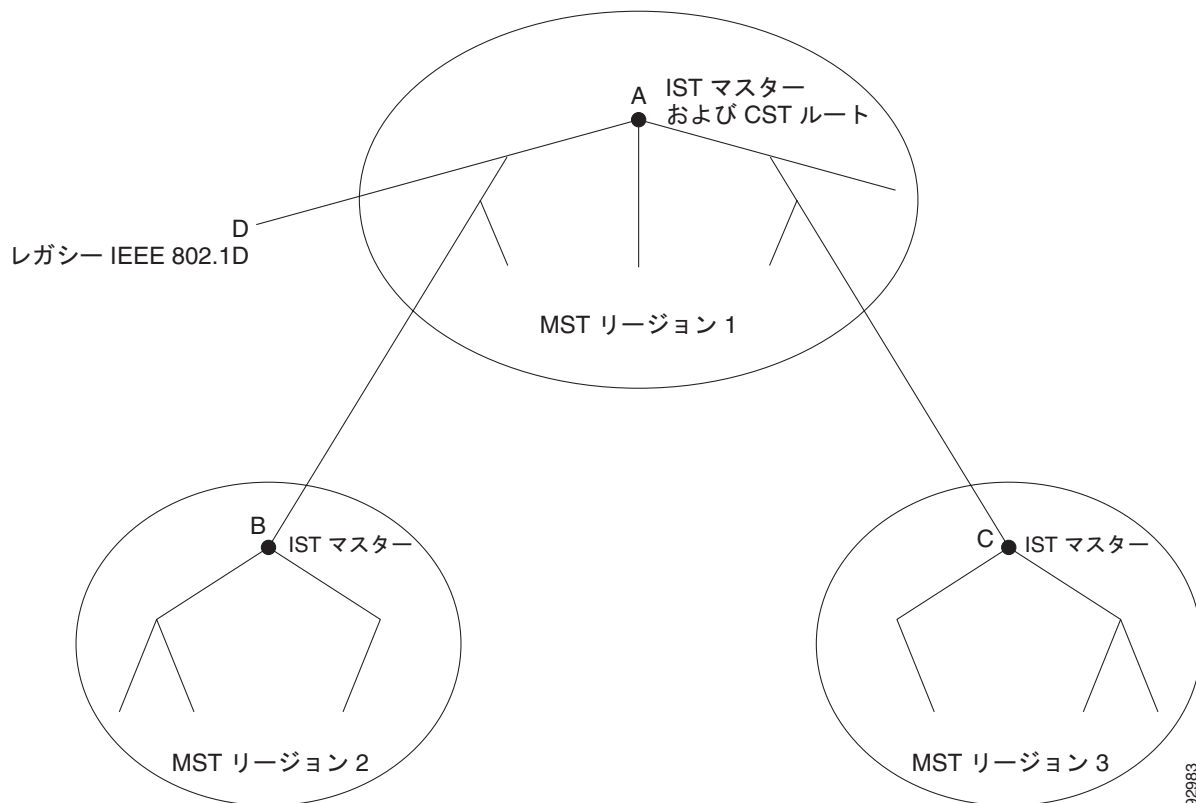
MST リージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシースイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築して維持します。MST インスタンスは、リージョンの境界で IST と結合して CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチドドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナルルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 20-1 は、3 つの MST リージョンと IEEE 802.1D 準拠のレガシースイッチ (D) からなるネットワークを示しています。リージョン 1 (A) の CIST リージョナルルートは、CIST のルートでもあります。リージョン 2 の CIST リージョナルルート (B) およびリージョン 3 の CIST リージョナルルート (C) は、CIST 内にあるそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 20-1 MST リージョン、CIST マスター、および CST ルート



92983

BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニング ツリー情報を BPDU に追加して、近接スイッチと通信し、最終的なスパニング ツリー トポロジを計算します。したがって、BPDU 伝送に関連するスパニング ツリー パラメータ (hello タイム、転送時間、最大エージング タイム、最大ホップ数など) は、CST インスタンスでのみ設定されますが、その影響はすべての MST インスタンスに及びます。スパニング ツリー トポロジに関連するパラメータ (スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど) は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、IEEE 802.1D 準拠のレガシー スイッチと通信します。MSTP スイッチ同士の通信には、MSTP BPDU が使用されます。

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体を網羅するスパニング ツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートへのコストです。このコストは MST リージョン内でも変更されずに残ります。CIST では、MST リージョンが単一のスイッチのように見えるので注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST リージョナル ルートは先行標準の実装では IST マスターと呼ばれていました。CIST ルートがリージョン内にある場合、CIST リージョナル ルートが CIST ルートになります。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナル ルートは IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、リージョン内の CIST リージョナル ルートへのコストです。このコストは IST (インスタンス 0) のみに関係します。

表 20-1 (P.20-5) に、IEEE 標準とシスコの先行標準の用語の比較を示します。

表 20-1 先行標準の用語および標準の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST および MST インスタンスは、スパニング ツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、ルートへのパス コスト、および IP Time to Live (TTL) メカニズムに似たホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST インスタンスに適用できます。ホップ カウントを設定すると、メッセージ エージング情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。インスタンスのルート スイッチは、常にコスト値が 0、ホップ カウント値が最大値に設定された BPDU（つまり M レコード）を送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼動する単一のスパニング ツリー リージョン、PVST+ または Rapid PVST+ が稼動する単一のスパニング ツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。また、境界ポートは、指定スイッチが単一のスパニング ツリー スイッチ、または異なる MST コンフィギュレーションを持つスイッチである LAN に接続されます。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートで受信可能な内部（同一リージョンからの）および外部の 2 種類のメッセージを識別します。メッセージが外部のものであれば、CIST によってのみ受信されます。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードのみを受信します。シスコ先行標準の実装では、ポートが境界ポートとして外部メッセージを受信します。つまり、ポートは内部メッセージと外部メッセージを混在させたものは受信できません。

MST リージョンには、スイッチと LAN の両方が含まれています。セグメントは、指定されたポートのリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義を利用すると、リージョン内部にある 2 つのポートのうち一方を、異なるリージョンに属するポートとしてセグメントを共有させることができます。この方法を採用すると、内部および外部の両方からポートでメッセージを受信できる場合があります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。



(注)

レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナルルート スイッチ ID フィールドが加えられたことです。一貫した送信スイッチ ID を近接スイッチに送信することで、リージョン全体で 1 つの仮想スイッチのように動作します。この例では、スイッチ A または B がそのセグメントで指定されているかどうかに関わらず、スイッチ C が、ルートの一貫した送信スイッチ ID を持つ BPDU を受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんが、境界の概念自体はシスコの実装に保持されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現状、次の 2 通りの事例が考えられます。

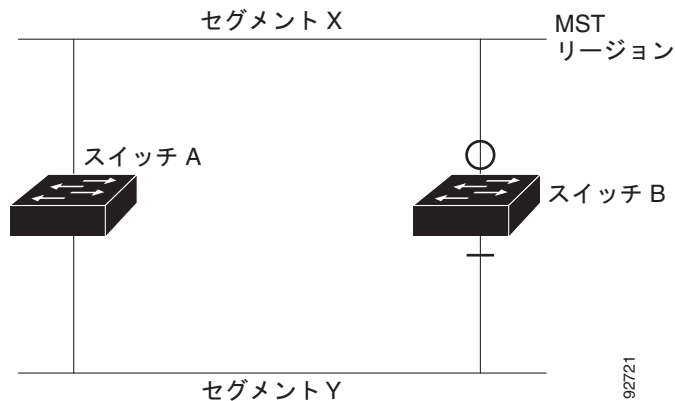
- 境界ポートが CIST リージョナルルートのルートポートである場合 - CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わったあとであれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。現在 MSTI ポートは、マスターという特別な役割を担っています。
- 境界ポートが CIST リージョナルルートのルートポートでない場合 - MSTI ポートは、CIST ポートのステートと役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU (M レコード) を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくいかもしれません。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシー スイッチと標準スイッチの相互運用

先行標準のスイッチでは先行標準のポートを自動検出できないため、インターフェイス コンフィギュレーション コマンドを使用して認識させます。標準と先行標準の間にあるリージョンは形成できませんが、CIST を使用することで相互運用できます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロード バランシングのみです。ポートが先行標準の BPDU を受信すると、CLI (コマンドライン インターフェイス) にはポートの設定に応じて異なるフラグが表示されます。また、スイッチが、先行標準の BPDU 転送の設定がされていないポートで先行標準の BPDU をはじめて受信すると、Syslog メッセージにも表示されます。

図 20-2 に例を示します。A を標準スイッチ、B を先行標準のスイッチと仮定してください。両方とも同じリージョンに設定されています。A が CIST のルートスイッチのため、B にセグメント X のルートポート (BX) とセグメント Y の代替ポート (BY) があります。セグメント Y がフラップして、先行標準の BPDU を送信する前に BY のポートが代替ポートになった場合、AY は Y に接続している先行標準のスイッチを検出できないため、標準の BPDU を送信し続けます。また、BY ポートは境界で固定されるため、AB 間でのロード バランシングができなくなります。同一の問題はセグメント X でも発生しますが、B がトポロジの変更を転送する可能性があります。

図 20-2 標準スイッチおよび先行標準のスイッチでの相互運用



(注)

標準と先行標準の MST 実装の間での干渉を少なくすることを推奨します。

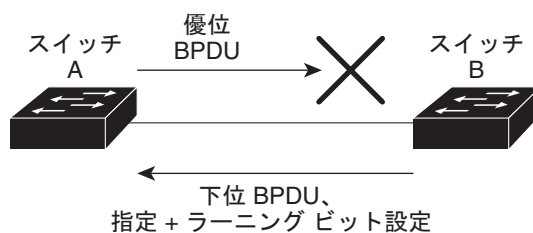
単一方向リンクの失敗の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアを使用することで、受信した BPDU からポートの役割とステートの一貫性を確認し、単一方向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

指定ポートで矛盾が検出された場合、役割には従いますが、ブリッジ処理のループを引き起こすよりは、矛盾による接続中断のほうが望ましい状態のため、廃棄ステートへ戻ります。

図 20-3 に、ブリッジ処理のループを引き起こす一般的な単一方向リンクの失敗例を示します。スイッチ A はルートスイッチです。スイッチ B へ向かうリンク上で、BPDU が紛失しています。RSTP と MST BPDU には、送信ポートの役割とステートが含まれています。この情報があれば、スイッチ A は、送信した優位 BPDU にスイッチ B が反応しないこと、さらにスイッチ B はルートスイッチではなく指定スイッチであることを検出できます。結果として、スイッチ A は自身のポートをブロックし（またはブロックを維持して）、ブリッジ処理のループを回避します。

図 20-3 単一方向リンクの失敗の検出



92722

MSTP とスイッチ スタック

スイッチ スタックはネットワークの他の部分からは単一のスパニング ツリー ノードと見なされるため、すべてのスタック メンバーが指定のスパニング ツリーに対して同じスイッチ ID を使用します。スイッチ ID は、スタック マスターの MAC アドレスを基にして作成されます。

MSTP をサポートしないスイッチが MSTP をサポートするスイッチ スタックに追加された場合、またはその逆の場合、スイッチはバージョン不一致ステートになります。可能な場合は、スイッチは自動的にスイッチ スタックで稼動しているソフトウェアと同じバージョンにアップグレードまたはダウングレードされます。

新たなスイッチがスタックに加入すると、そのスイッチ ID はスタック マスターのスイッチ ID に設定されます。新たに追加されたスイッチが最小の ID を持ち、すべてのスタック メンバーのルートパスコストが同一の場合は、新たに追加されたスイッチがスタック ルートになります。新たに追加されたスイッチが、スイッチ スタックに対してより適したルート ポート、またはスタックに接続する LAN に対してより適した指定ポートを持つ場合は、トポロジが変更されます。新たに追加されたスイッチに接続する別のスイッチが自分のルート ポートまたは指定ポートを変更した場合は、新たに追加されたスイッチによって、ネットワーク内のトポロジ変更が引き起こされます。

スタック メンバーがスタックを脱退すると、スタック内（スタック外部も含まれる場合がある）でスパニング ツリーの再コンバージェンスが実行されます。残りのスタック メンバーのうち最小のスタック ポート ID を持つものがスタック ルートになります。

スタック マスターに障害が生じたり、それがスタックから脱退したりした場合は、スタック メンバーの中から新たなスタック マスターが選択され、すべてのスタック メンバーが自分のスパニング ツリースイッチ ID を新たなマスターのスイッチ ID に変更します。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

IEEE 802.1D STP との相互運用性

MSTP が稼動しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシースイッチが指定スイッチでない場合、レガシースイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再起動する（近接スイッチとの再ネゴシエーションを強制する）には、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境界ポートは、指定スイッチがシングル スパニング ツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

RSTP の概要

RSTP は、ポイントツーポイントの配線を利用して、スパニング ツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニング ツリーを再構成できます (IEEE 802.1D スパニング ツリーのデフォルトに設定されている 50 秒とは異なります)。

ここでは、RSTP の機能について説明します。

- 「ポートの役割およびアクティブ トポロジ」 (P.20-10)
- 「高速コンバージェンス」 (P.20-11)
- 「ポートの役割の同期化」 (P.20-12)
- 「BPDU のフォーマットおよびプロセス」 (P.20-13)

設定については、「MSTP 機能の設定」 (P.20-15) を参照してください。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。「スパニング ツリー トポロジと BPDU」 (P.19-3) で説明したように、RSTP は、IEEE 802.1D STP に基づき、スイッチ プライオリティが最も高い (プライオリティの値が最も小さい) スイッチをルート スイッチに選択します。RSTP はさらに、各ポートに次のいずれか 1 つの役割を割り当てます。

- ルート ポート: スイッチからルート スイッチへパケットを転送する場合の最適パス (最も低コストなパス) を提供します。
- 指定ポート: 指定スイッチに接続します。これにより、LAN からルート スイッチへパケットを転送するときのパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。
- 代替ポート: 現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。
- バックアップ ポート: 指定ポートが提供した、スパニング ツリーのリーフに向かうパスのバックアップとして機能します。バックアップ ポートが存在できるのは、2 つのポートがポイントツーポイント リンクによってループバックで接続されている場合、または 1 つのスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合です。
- ディセーブル ポート: スパニング ツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートの役割を割り当てられたポートは、アクティブ トポロジの一部となります。代替ポートまたはバックアップ ポートの役割を割り当てられたポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルートポートおよび指定ポートがただちにフォワーディング ステートに移行し、代替ポートとバックアップポートが必ず廃棄ステート (IEEE 802.1D のブロッキング ステートと同じ) になるように保証します。フォワーディング プロセスおよびラーニング プロセスの動作はポート ステートによって制御されます。表 20-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 20-2 ポート ステートの比較

動作ステータス	STP ポート ステート (IEEE 802.1D)	RSTP ポート ステート	ポートがアクティブ トポロジに含まれているか
イネーブル	ブロッキング	廃棄	含まれていない
イネーブル	リスニング	廃棄	含まれていない
イネーブル	ラーニング	ラーニング	含まれている
イネーブル	フォワーディング	フォワーディング	含まれている
ディセーブル	ディセーブル	廃棄	含まれていない

シスコの STP 実装製品内で整合性を図るため、このマニュアルでは、ポートの廃棄ステートをブロッキングと定義しています。指定ポートは、リスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN に障害が発生しても、ただちに接続を回復できます。RSTP は、エッジポート、新しいルート ポート、およびポイントツーポイントリンクで接続されているポートに次のような高速コンバージェンスを提供します。

- エッジポート：**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、RSTP スイッチ上の 1 つのポートをエッジポートに設定すると、そのエッジポートはただちにフォワーディング ステートになります。エッジポートは PortFast 対応ポートと同じで、これをイネーブルにできるのは、単一のエンドステーションに接続されているポート上だけです。
- ルートポート：RSTP は、新しいルートポートを選択すると、古いルートポートをブロックして、新しいルートポートをただちにフォワーディングステートにします。
- ポイントツーポイントリンク：2 つのポートをポイントツーポイントリンクで接続し、ローカルポートが指定ポートになると、その指定ポートは、提案/合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します。

図 20-4 では、スイッチ A とスイッチ B はポイントツーポイントリンクを通じて接続され、すべてのポートがブロッキングステートになっています。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、スイッチ A はスイッチ B に提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDU）を送信し、スイッチ A 自身が指定スイッチになることを提案します。

スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルートポートとして選択し、すべての非エッジポートをブロッキングステートにします。さらに、新しいルートポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

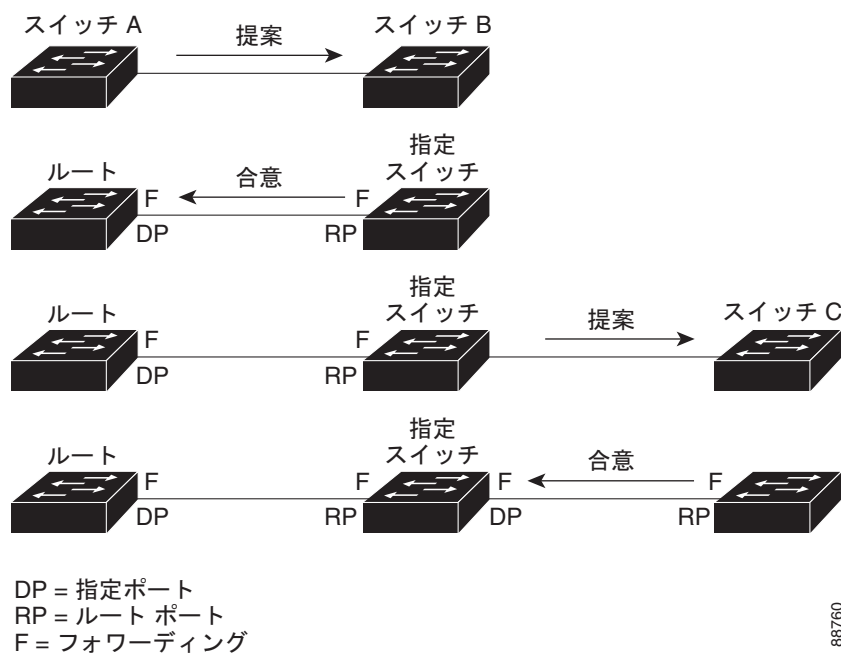
スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディングステートにします。スイッチ B はその非エッジポートをすべてブロックし、またスイッチ A とスイッチ B はポイントツーポイントリンクで接続されているので、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイクメッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルートポートとして選択し、両端のポートはただちにフォワーディングステートに移行します。アクティブトポロジにスイッチが追加されるたびに、このハンドシェイクプロセスが実行されます。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパンニングツリーのリーフへと進みます。

スイッチ スタックでは、Cross-Stack Rapid Transition (CSRT) 機能が、提案/合意ハンドシェイクの間、ポートがフォワーディング ステートになる前に、スタック メンバーが他のすべてのスタック メンバーからの確認応答を受信するように保証します。スイッチが MST モードの場合、CSRT は自動的にイネーブルになります。

スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定で制御されたデフォルトの設定値を上書きできます。

図 20-4 高速コンバージェンスの提案/合意ハンドシェイク



ポートの役割の同期化

スイッチのポートの 1 つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

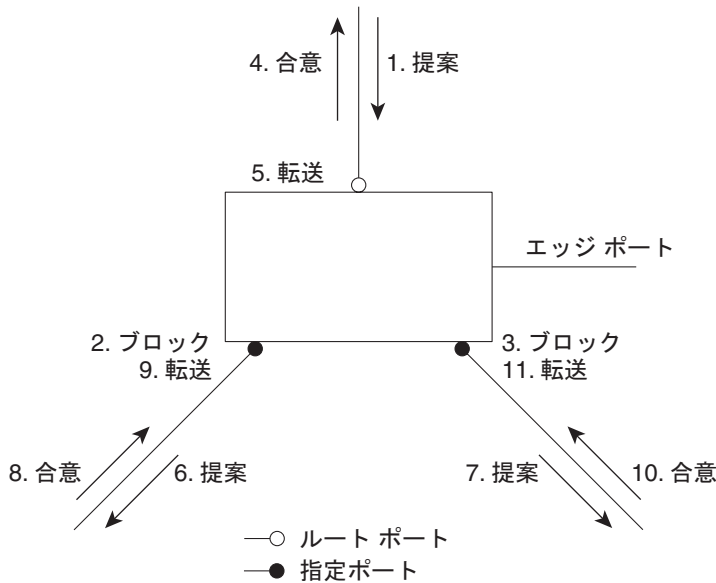
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。スイッチ上の個々のポートは次の場合に同期化された状態となります。

- ブロッキング ステートである場合
- エッジ ポートである場合 (ネットワークのエッジとして設定されているポート)

指定ポートがフォワーディング ステートであり、なおかつエッジ ポートとして設定されていない場合、RSTP によって新しいルート情報で強制的に同期化されると、その指定ポートはブロッキング ステートになります。一般的に、RSTP がポートを新しいルート情報で強制的に同期化する場合に、そのポートが上記のいずれの条件も満たしていない場合、ポートのステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルート ポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポートの役割について互いに合意すると、RSTP はポート ステートをただちにフォワーディング ステートに移行させます。図 20-5 は、この一連のイベントを示します。

図 20-5 高速コンバージェンス中の一連のイベント



88761

BPDU のフォーマットおよびプロセス

RSTP BPDU のフォーマットは、プロトコルバージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報が無いことを示しています。表 20-3 に、RSTP のフラグ フィールドを示します。

表 20-3 RSTP BPDU フラグ

ビット	機能
0	トポロジの変更 (TC)
1	提案
2-3 :	ポートの役割 :
00	不明
01	代替ポート
10	ルートポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジの変更の確認 (TCA)

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージでは、ポートの役割は常に指定ポートに設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージでは、ポートの役割は常にルートポートに設定されます。

RSTP には個別の Topology Change Notification (TCN; トポロジ変更通知) BPDU はありません。トポロジの変更を示すには、トポロジ変更 (TC) フラグが使用されます。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニングとフォワーディングのフラグは、送信ポートのステータスに応じて設定されます。

優位 BPDU 情報の処理

現在保存されているルート情報よりも優位のルート情報 (小さいスイッチ ID、低パス コストなど) をポートが受信すると、RSTP は再構成を開始します。そのポートが新しいルート ポートとして提案され、選択されると、RSTP は他のすべてのポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化したあと、合意メッセージを送信します。BPDU が IEEE 802.1D BPDU である場合、スイッチは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートはフォワーディング ステータスに移行するために 2 倍の転送遅延時間を必要とします。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる場合、RSTP はそのポートをブロッキング ステータスに設定し、合意メッセージは送信しません。指定ポートは、転送遅延タイマーが満了するまで提案フラグの設定された BPDU の送信を続けます。タイマーが満了すると、ポートはフォワーディング ステータスに移行します。

下位 BPDU 情報の処理

指定ポートの役割フラグが設定された下位 BPDU (そのポートに現在保存されている値より大きいスイッチ ID、高いパス コストなど) を指定ポートが受信した場合、その指定ポートは、ただちに現在の自身の情報を応答します。

トポロジの変更

ここでは、スパンニング ツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出 - IEEE 802.1D ではブロッキングとフォワーディング ステータス間でのすべての移行によってトポロジの変更が生じますが、RSTP ではトポロジの変更が生じるのは、ブロッキングからフォワーディングにステータスが移行する場合のみです (トポロジの変更と見なされるのは、相互接続性が向上する場合だけです)。エッジ ポートでステータスが変更されても、トポロジの変更は生じません。RSTP スイッチは、トポロジの変更を検出すると、そのスイッチのすべての非エッジ ポート (TC 通知を受信したポートを除く) で学習した情報を削除します。
- 通知 - IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- 確認 - RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー (IEEE 802.1D のトポロジ変更タイマーと同じ) がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。RSTP BPDU では、TCA ビットは設定されません。

- 伝播 - RSTP スイッチは、指定ポートまたはルートポートを介して別のスイッチから TC メッセージを受信すると、自身のすべての非エッジポート、指定ポート、およびルートポート（この TC メッセージを受信したポートを除く）に変更を伝播します。スイッチは、これらのすべてのポートの TC 時間タイマーを起動し、これらのポート上で学習した情報を削除します。
- プロトコルの移行 - IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

ポートが初期化されると、移行遅延タイマーが起動され（RSTP BPDU を送信する最小時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコルタイプを無視します。

スイッチはポートの移行遅延タイマーが満了したあとに IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了したあとに RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用を開始されます。

MSTP 機能の設定

ここでは、次の設定情報について説明します。

- 「MSTP のデフォルト設定」(P.20-16)
- 「MSTP 設定時の注意事項」(P.20-16)
- 「MST リージョンの設定および MSTP のイネーブル化」(P.20-17) (必須)
- 「ルートスイッチの設定」(P.20-19) (任意)
- 「セカンダリ ルートスイッチの設定」(P.20-20) (任意)
- 「ポートプライオリティの設定」(P.20-21) (任意)
- 「パスコストの設定」(P.20-22) (任意)
- 「スイッチプライオリティの設定」(P.20-23) (任意)
- 「Hello タイムの設定」(P.20-24) (任意)
- 「転送遅延時間の設定」(P.20-25) (任意)
- 「最大エイジングタイムの設定」(P.20-25) (任意)
- 「最大ホップカウントの設定」(P.20-26) (任意)
- 「リンクタイプの指定による高速移行の保証」(P.20-26) (任意)
- 「ネイバータイプの指定」(P.20-27) (任意)
- 「プロトコル移行プロセスの再起動」(P.20-27) (任意)

MSTP のデフォルト設定

表 20-4 に、MSTP のデフォルト設定を示します。

表 20-4 MSTP のデフォルト設定

機能	デフォルト設定
スパンニング ツリー モード	PVST+ (Rapid PVST+ と MSTP はディセーブル)
スイッチ プライオリティ (CIST ポート単位で設定可能)	32768.
スパンニング ツリー ポート プライオリティ (CIST ポート単位で設定可能)	128.
スパンニング ツリー ポート コスト (CIST ポート単位で設定可能)	1000 Mbps : 4 100 Mbps : 19 10 Mbps : 100
Hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

サポートされるスパンニング ツリー インスタンス数については、「サポートされるスパンニング ツリー インスタンス」(P.19-11) を参照してください。

MSTP 設定時の注意事項

ここでは、MSTP の設定時の注意事項を説明します。

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MST をイネーブルにすると、RSTP が自動的にイネーブルになります。
- 2 つ以上のスタック スイッチを同じ MST リージョンに設置するには、それらのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- スイッチ スタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピングできる VLAN の数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです (たとえば、すべての VLAN で PVST+ を使用するか、すべての VLAN で Rapid PVST+ を使用するか、またはすべての VLAN で MSTP を使用することになります)。詳細については、「スパンニング ツリーの相互運用性と下位互換性」(P.19-11) を参照してください。推奨するトランク ポート設定の詳細については、「他の機能との相互作用」(P.14-19) を参照してください。
- すべてのスタック メンバーが同じバージョンのスパンニング ツリーを稼働します (すべて PVST+、Rapid PVST+、または MSTP)。詳細については、「スパンニング ツリーの相互運用性と下位互換性」(P.19-11) を参照してください。

- MST コンフィギュレーションの VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) 伝播機能はサポートされません。ただし、CLI または SNMP (簡易ネットワーク管理プロトコル) サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション (リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング) を手動で設定することは可能です。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/ インスタンス マッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが 1 つのリンク上で伝送されます。パス コストを手動で設定することで、スイッチ スタック全体にわたりロード バランシングを実現できます。
- PVST+ クラウドと MST クラウドの間、または Rapid PVST+ クラウドと MST クラウドの間でロード バランシングを実現するには、すべての MST 境界ポートがフォワーディング ステートでなければなりません。そのためには、MST クラウドの IST マスターが CST のルートを兼ねている必要があります。MST クラウドが複数の MST リージョンで構成されている場合は、MST リージョンの 1 つに CST ルートが含まれており、他のすべての MST リージョンにおいて、MST クラウドに含まれているルートへのパスの方が PVST+ または Rapid PVST+ クラウド経由のパスよりも優れている必要があります。クラウド内のスイッチを手動で設定しなければならない場合もあります。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- UplinkFast、BackboneFast、およびクロススタック UplinkFast 設定時の注意事項については、「[オプションのスパニング ツリー設定時の注意事項](#)」(P.21-12) を参照してください。


MST リージョンの設定および MSTP のイネーブル化

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/ インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは RSTP BPDU を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニング ツリー インスタンスの数は 65 までです。1 つの VLAN を同時に複数のスパニング ツリー インスタンスに割り当てることはできません。

MST リージョンの設定を行い、MSTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst configuration</code>	MST コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	instance <i>instance-id</i> vlan <i>vlan-range</i>	VLAN を MST インスタンスに対応付けます。 <ul style="list-style-type: none"> <i>instance-id</i> に指定できる範囲は、0 ～ 4094 です。 vlan <i>vlan-range</i> に指定できる範囲は、1 ～ 4094 です。 MST インスタンスに VLAN をマッピングする場合、マッピングはインクリメンタルに行われ、コマンドで指定された VLAN がすでにマッピング済みの VLAN に対して追加または削除されます。 VLAN の範囲を指定するには、ハイフンを使用します。たとえば、 instance 1 vlan 1-63 と入力すると、VLAN 1 ～ 63 が MST インスタンス 1 にマッピングされます。 一連の VLAN を指定するには、カンマを使用します。たとえば、 instance 1 vlan 10, 20, 30 を入力すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。
ステップ 4	name <i>name</i>	コンフィギュレーション名を指定します。 <i>name</i> スtringの最大長は 32 文字で、大文字と小文字が区別されます。
ステップ 5	revision <i>version</i>	コンフィギュレーション リビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
ステップ 6	show pending	入力した設定を表示して、確認します。
ステップ 7	exit	変更を適用し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	spanning-tree mode mst	MSTP をイネーブルにします。RSTP もイネーブルになります。  注意 スパニング ツリー モードを変更すると、すべてのスパニング ツリー インスタンスが前のモードで停止して新しいモードで再起動されるので、トラフィックが中断する可能性があります。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show running-config	設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの MST リージョン コンフィギュレーションに戻すには、**no spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。VLAN インスタンス マッピングをデフォルトの設定に戻すには、**no instance instance-id [vlan vlan-range] MST** コンフィギュレーション コマンドを使用します。デフォルトの名前に戻すには、**no name MST** コンフィギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、**no revision MST** コンフィギュレーション コマンドを使用し、PVST+ をイネーブルに戻すには、**no spanning-tree mode** または **spanning-tree mode pvst** グローバル コンフィギュレーション コマンドを使用します。

次に、MST コンフィギュレーション モードの例を示します。まず MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、そのリージョンの名前を *region1* に設定します。次にコンフィギュレーション リビジョン番号として 1 を設定し、入力した設定を表示させて変更を適用します。そして最後にグローバル コンフィギュレーション モードに戻ります。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
```

```
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0         1-9,21-4094
1         10-20
-----

Switch(config-mst)# exit
Switch(config)#
```

ルートスイッチの設定

スイッチは、スパニング ツリー インスタンスを VLAN グループとマッピングして維持します。各インスタンスには、スイッチプライオリティとスイッチの MAC アドレスからなるスイッチ ID が対応付けられます。最小のスイッチ ID を持つスイッチがその VLAN グループのルートスイッチになります。

特定のスイッチがルートになるように設定するには、**spanning-tree mst instance-id root** グローバル コンフィギュレーション コマンドを使用して、スイッチプライオリティをデフォルト値 (32768) からきわめて小さい値に変更します。これにより、そのスイッチが指定されたスパニング ツリー インスタンスのルートスイッチになることができます。このコマンドを入力すると、スイッチは、ルートスイッチのスイッチプライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定されたインスタンスについて、自身のプライオリティを 24576 に設定します (この値によって、このスイッチが指定されたスパニング ツリー インスタンスのルートになる場合)。

指定されたインスタンスのルートスイッチに 24576 より小さいスイッチプライオリティが設定されている場合、スイッチは自身のプライオリティを最小のスイッチプライオリティより 4096 だけ小さい値に設定します (表 19-1 (P.19-5) に示すように、4096 は 4 ビットのスイッチプライオリティ値の最下位ビットの値です)。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルートスイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼動する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチプライオリティ値が増大します。

各スパニング ツリー インスタンスのルートスイッチは、バックボーンスイッチまたはディストリビューションスイッチにする必要があります。アクセススイッチをスパニング ツリーのプライマリルートとして設定しないでください。

レイヤ 2 ネットワークの直径 (つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間の最大スイッチ ホップ数) を指定するには、**diameter** キーワードを指定します (MST インスタンス 0 の場合のみ使用可)。ネットワーク直径を指定すると、スイッチは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージング タイムを自動的に設定し、これによって収束時間が大幅に短縮されます。自動的に算出された Hello タイムを変更するには、**hello** キーワードを使用します。



(注)

スイッチをルートスイッチとして設定したあとに、**spanning-tree mst hello-time**、**spanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

スイッチをルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst instance-id root primary</code> <code>[diameter net-diameter [hello-time seconds]]</code>	スイッチをルート スイッチに設定します。 <ul style="list-style-type: none"> <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 (任意) diameter net-diameter には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。このキーワードを使用できるのは MST インスタンス 0 の場合だけです。 (任意) hello-time seconds には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 秒です。デフォルトは 2 秒です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst instance-id root` グローバル コンフィギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリティはデフォルト値 (32768) から 28672 に変更されます。その結果、プライマリ ルート スイッチに障害が発生した場合に、このスイッチが、指定されたインスタンスのルート スイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree mst instance-id root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および hello タイム値を使用してください。

スイッチをセカンダリ ルート スイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst instance-id root secondary [diameter net-diameter [hello-time seconds]]	<p>スイッチをセカンダリ ルート スイッチに設定します。</p> <ul style="list-style-type: none"> <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 (任意) <i>diameter net-diameter</i> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。このキーワードを使用できるのは MST インスタンス 0 の場合だけです。 (任意) <i>hello-time seconds</i> には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は 1 ~ 10 秒です。デフォルトは 2 秒です。 <p>プライマリ ルート スイッチを設定したときと同じネットワーク直径および Hello タイム値を使用してください。「ルート スイッチの設定」(P.20-19) を参照してください。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst instance-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、**no spanning-tree mst instance-id root** グローバル コンフィギュレーション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには高いプライオリティ (小さい数値) を与え、最後に選択させたいインターフェイスには低いプライオリティ (大きい数値) を与えます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。



(注)

スイッチがスイッチ スタックのメンバーの場合は、**spanning-tree mst [instance-id] port-priority priority** インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst [instance-id] cost cost** インターフェイス コンフィギュレーション コマンドを使用して、フォワーディング ステートにするポートを選択する必要があります。最初に選択させたいポートには小さいコスト値を、最後に選択させたいポートには大きいコスト値を割り当てます。詳細については、「[パス コストの設定](#)」(P.20-22) を参照してください。

インターフェイスの MSTP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 3	<code>spanning-tree mst instance-id port-priority priority</code>	ポート プライオリティを設定します。 <ul style="list-style-type: none"> <code>instance-id</code> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 <code>priority</code> に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティは高くなります。 プライオリティ値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。それ以外の値はすべて拒否されます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree mst interface interface-id</code> または <code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) `show spanning-tree mst interface interface-id` 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。それ以外の情報については、`show running-config interface` 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、`no spanning-tree mst instance-id port-priority` インターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスの MSTP コストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 3 spanning-tree mst instance-id cost cost	コストを設定します。 ループが発生した場合、MSTP はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、高速で伝送されます。 <ul style="list-style-type: none"> • <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 • <i>cost</i> に指定できる範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度に基づきます。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show spanning-tree mst interface interface-id または show spanning-tree mst instance-id	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) **show spanning-tree mst interface interface-id** 特権 EXEC コマンドによって表示されるのは、リンク アップ動作可能状態のポートの情報だけです。それ以外の情報については、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、**no spanning-tree mst instance-id cost** インターフェイス コンフィギュレーション コマンドを使用します。

スイッチ プライオリティの設定

スイッチ プライオリティを設定して、スタンドアロン スイッチまたはスタック内のスイッチがルート スイッチとして選択される可能性を高めることができます。



(注) このコマンドは、十分に注意して使用してください。スイッチ プライオリティの変更には、通常、**spanning-tree mst instance-id root primary** および **spanning-tree mst instance-id root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

スイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst instance-id priority priority</code>	<p>スイッチ プライオリティを設定します。</p> <ul style="list-style-type: none"> <code>instance-id</code> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 <code>priority</code> に指定できる範囲は 0 ~ 61440 で、4096 ずつ増加します。デフォルト値は 32768 です。この値が低いほど、スイッチがルート スイッチとして選択される可能性が高くなります。 <p>有効なプライオリティ値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。それ以外の値はすべて拒否されます。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst instance-id</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst instance-id priority` グローバル コンフィギュレーション コマンドを使用します。

Hello タイムの設定

Hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を設定できます。

すべての MST インスタンスの hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst hello-time seconds</code>	<p>すべての MST インスタンスの hello タイムを設定します。</p> <p>Hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。</p> <p><code>seconds</code> に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst hello-time` グローバル コンフィギュレーション コマンドを使用します。

転送遅延時間の設定

すべての MST インスタンスの転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst forward-time seconds</code>	すべての MST インスタンスの転送遅延時間を設定します。転送遅延時間は、スパニング ツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 <i>seconds</i> に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst forward-time` グローバル コンフィギュレーション コマンドを使用します。

最大エージング タイムの設定

すべての MST インスタンスの最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst max-age seconds</code>	すべての MST インスタンスの最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニング ツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 <i>seconds</i> に指定できる範囲は 6 ~ 40 です。デフォルト値は 20 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst max-age` グローバル コンフィギュレーション コマンドを使用します。

最大ホップ カウントの設定

すべての MST インスタンスの最大ホップ カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree mst max-hops hop-count</code>	BPDU が廃棄され、ポートに維持されていた情報が期限切れになるまでの、リージョン内でのホップ数を指定します。 <i>hop-count</i> に指定できる範囲は 1 ~ 255 です。デフォルト値は 20 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show spanning-tree mst</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、`no spanning-tree mst max-hops` グローバル コンフィギュレーション コマンドを使用します。

リンク タイプの指定による高速移行の保証

2つのポートをポイントツーポイントリンクで接続し、ローカルポートが指定ポートになると、RSTP は提案/合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します（「[高速コンバージェンス](#)」(P.20-11)を参照）。

デフォルトでは、リンクタイプは、インターフェイスのデュプレックスモードによって制御されます。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。MSTP が稼動しているリモートスイッチ上の1つのポートと物理的にポイントツーポイントで接続されている半二重リンクが存在する場合は、リンクタイプのデフォルト設定値を変更して、フォワーディングステートへの高速移行をイネーブルにできます。

リンクタイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポートチャネル論理インターフェイスがあります。指定できる VLAN ID 範囲は 1 ~ 4094 です。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 3	<code>spanning-tree link-type point-to-point</code>	ポートのリンクタイプをポイントツーポイントに指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree mst interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、`no spanning-tree link-type` インターフェイス コンフィギュレーション コマンドを使用します。

ネイバー タイプの指定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトでは、ポートは自動的に先行標準のデバイスを検出します。ただし、ポート自体は、標準と先行標準の BPDU を両方受信できます。デバイスとネイバーの間に不一致があれば、CIST のみがインターフェイス上で動作します。

ポートを選択して、先行標準の BPDU のみ送信するように設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての `show` コマンドで表示されます。

リンク タイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	<code>spanning-tree mst pre-standard</code>	先行標準の BPDU のみ送信するようにポートを指定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree mst interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートをデフォルト設定に戻すには、`no spanning-tree mst prestandard` インターフェイス コンフィギュレーション コマンドを使用します。

プロトコル移行プロセスの再起動

MSTP が稼働しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU (プロトコルバージョンが 0 に設定されている BPDU) を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MST BPDU (バージョン 3)、または RST BPDU (バージョン 2) を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、レガシースイッチが指定スイッチでない場合、レガシースイッチがリンクから削除されているかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

スイッチでプロトコル移行プロセスを再起動する (近接スイッチとの再ネゴシエーションを強制する) には、`clear spanning-tree detected-protocols` 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再開するには、`clear spanning-tree detected-protocols interface interface-id` 特権 EXEC コマンドを使用します。

MST コンフィギュレーションおよびステータスの表示

スパニング ツリー ステータスを表示するには、表 20-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 20-5 MST ステータスを表示するコマンド

コマンド	目的
<code>show spanning-tree mst configuration</code>	MST リージョン コンフィギュレーションを表示します。
<code>show spanning-tree mst configuration digest</code>	現在の MSTCI に含まれている Message Digest 5 (MD5) ダイジェストを表示します。
<code>show spanning-tree mst instance-id</code>	特定のインスタンスの MST 情報を表示します。
<code>show spanning-tree mst interface interface-id</code>	特定のインターフェイスの MST 情報を表示します。

`show spanning-tree` 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 21

オプションのスパニング ツリー機能の設定

この章では、Catalyst 3750 スイッチにオプションのスパニング ツリー機能を設定する方法について説明します。スイッチが Per-VLAN Spanning-Tree Plus (PVST+) を実行している場合、これらのすべての機能を設定できます。スイッチ スタックが Multiple Spanning-Tree Protocol (MSTP) または Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルを稼働している場合は、明記した機能だけを設定できます。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

PVST+ および Rapid PVST+ の詳細については、[第 19 章「STP の設定」](#)を参照してください。MSTP の詳細および複数の VLAN を同スパニング ツリー インスタンスにマッピングする方法については、[第 20 章「MSTP の設定」](#)を参照してください。



(注)

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

この章で説明する内容は、次のとおりです。

- 「オプションのスパニング ツリー機能の概要」 (P.21-1)
- 「オプションのスパニング ツリー機能の設定」 (P.21-11)
- 「スパニング ツリー ステータスの表示」 (P.21-20)

オプションのスパニング ツリー機能の概要

ここでは、次の概要について説明します。

- 「PortFast の概要」 (P.21-2)
- 「BPDU ガードの概要」 (P.21-2)
- 「BPDU フィルタリングの概要」 (P.21-3)
- 「UplinkFast の概要」 (P.21-3)
- 「CSUF の概要」 (P.21-5)
- 「BackboneFast の概要」 (P.21-7)
- 「EtherChannel ガードの概要」 (P.21-10)
- 「ルート ガードの概要」 (P.21-10)
- 「ループ ガードの概要」 (P.21-11)

PortFast の概要

PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。単一のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、スパニング ツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます (図 21-1 を参照)。

1 台のワークステーションまたはサーバに接続されたインターフェイスが Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) を受信しないようにする必要があります。スイッチを再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニング ツリー ステータスの遷移をたどります。

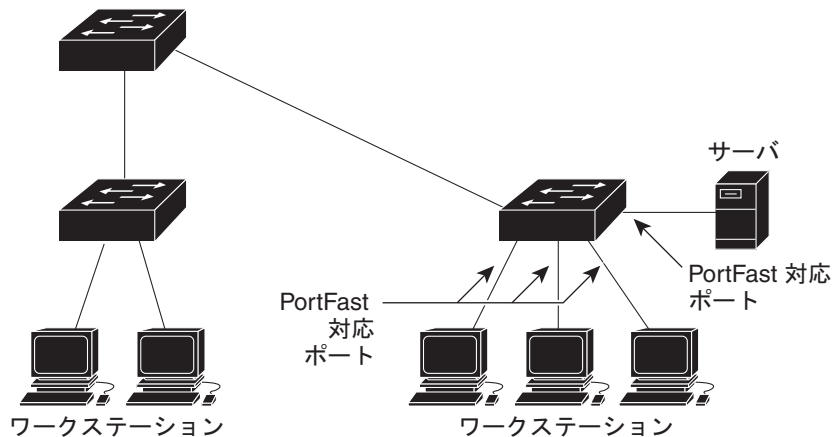


(注)

PortFast の目的は、インターフェイスがスパニング ツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はエンドステーションに接続されたインターフェイス上で使用する場合に限り有効になります。他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニング ツリーのループが生じる可能性があります。

この機能をイネーブルにするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンド、または **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。

図 21-1 PortFast 対応インターフェイス



BPDU ガードの概要

BPDU ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応ポート上で BPDU ガードをイネーブルにできます。これらのポート上で BPDU が受信されると、スパニング ツリーは、PortFast で動作しているポートをシャットダウンします。設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは **errdisable** ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

インターフェイス レベルの場合は、**PortFast 機能をイネーブルにしなくても**、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポート上で BPDU ガードをイネーブルにできます。BPDU を受信したポートは、**errdisable** ステートになります。

手動でインターフェイスを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU フィルタリングの概要

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用して、PortFast 対応インターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを使用すると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

インターフェイス レベルの場合は、**PortFast 機能をイネーブルにしなくても**、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。



注意

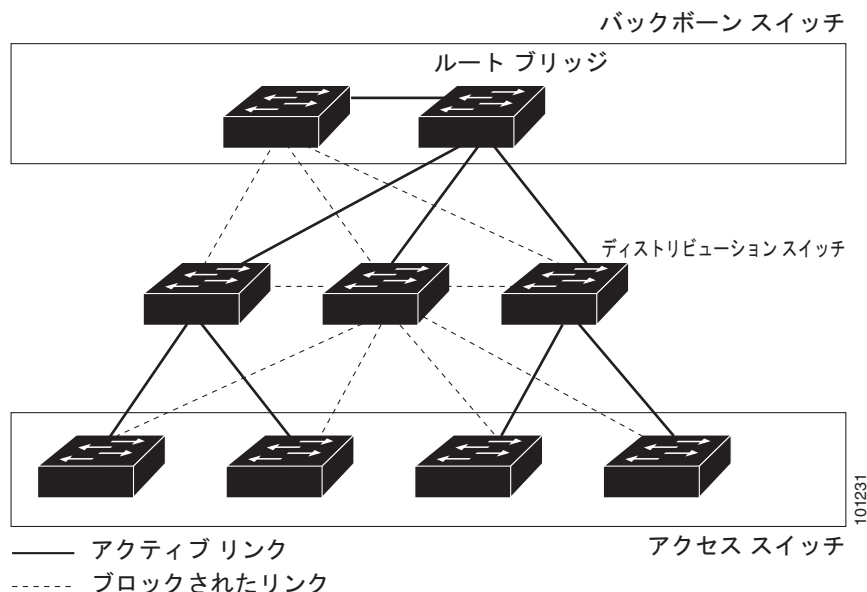
BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

スイッチ全体または 1 つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

UplinkFast の概要

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション スイッチ、およびアクセス スイッチに分類できます。図 21-2 は、ディストリビューション スイッチおよびアクセス スイッチに少なくとも 1 つの冗長リンクが確保されている複雑なネットワークの例です。冗長リンクは、ループを防止するために、スパニング ツリーによってブロックされています。

図 21-2 階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニング ツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニング ツリーが再設定された場合は、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して **UplinkFast** をイネーブルにすることにより、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニング ツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

スパニング ツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッドし、インターフェイス上で学習した各アドレスにパケットを送信します。**max-update-rate** パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます (このパラメータはデフォルトで毎秒 150 パケットです)。ただし、0 を入力すると、ステーション学習フレームが生成されないため、接続切断後スパニング ツリー トポロジがコンバージェンスする速度が遅くなります。



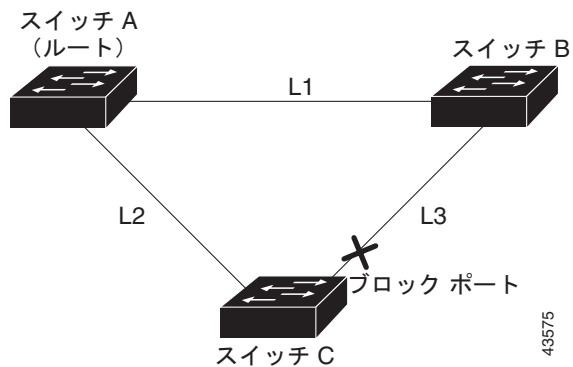
(注)

UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロード バランシングを実行します。アップリンク グループは、(VLAN ごとの) レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。具体的には、アップリンク グループは (転送を行う) ルート ポートと 1 組のブロック ポートからなります (セルフ ループ ポートは除く)。アップリンク グループは、転送中のリンクで障害が発生した場合に、代替パスを提供します。

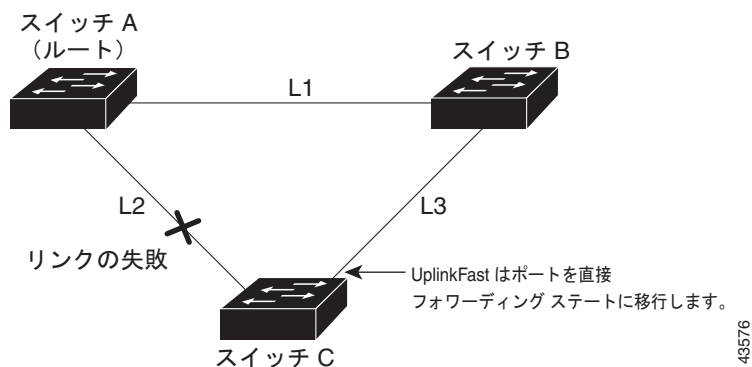
図 21-3 に、リンク障害が発生していないトポロジの例を示します。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 21-3 直接リンク障害発生前の UplinkFast の例



スイッチ C が、ルート ポートの現在アクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます（図 21-4 を参照）。この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 21-4 直接リンク障害発生後の UplinkFast の例



CSUF の概要

Catalyst 3750 スイッチでは、UplinkFast 機能は Cross-Stack UplinkFast (CSUF) 機能です。CSUF は、スイッチ スタック全体に高速スパニング ツリー トランジション（通常のネットワーク状況下では 1 秒未満の高速コンバージェンス）を提供します。高速トランジションの実行中は、スイッチ スタック上の代替冗長リンクがフォワーディング ステートになりますが、一時的にスパニング ツリー ループが発生したり、バックボーンとの接続が失われたりすることはありません。この機能を使用すると、一定の構成で、冗長性と回復性に優れたネットワークを構築できます。CSUF は、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

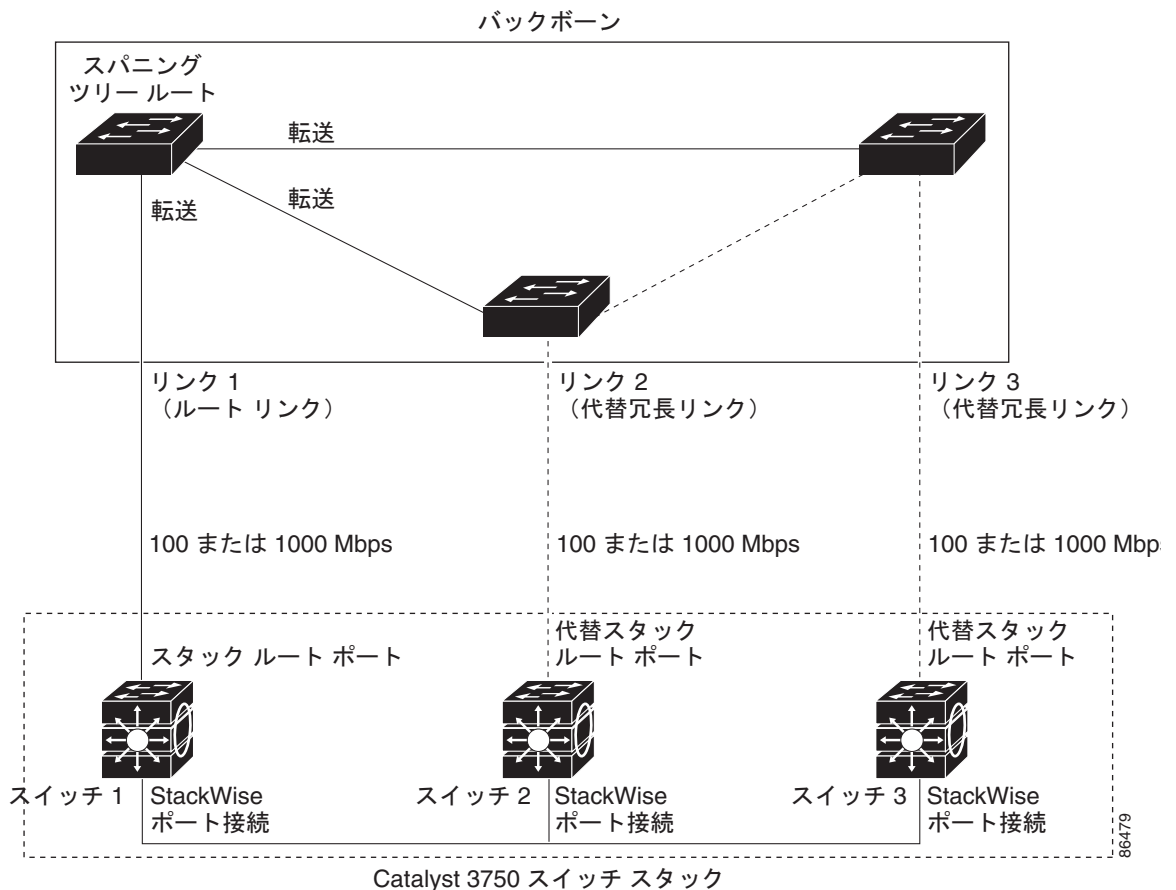
CSUF は常に高速トランジションを実現するとは限りません。場合によっては、標準スパニング ツリー トランジションが実行され、完了までに 30 ～ 40 秒かかります。詳細については、「[高速コンバージェンスを実行させるイベント](#)」(P.21-7) を参照してください。

CSUF の機能

CSUF では、スタックの 1 つのリンクが、ルートへのパスとして確実に選択されます。図 21-5 に示したように、スイッチ 1 のスタック ルート ポートがスパニング ツリーのルートへのパスを提供します。スイッチ 2 およびスイッチ 3 の代替スタック ルート ポートは、現在のスタック ルート スイッチに障害が生じた場合やスパニング ツリー ルートへのリンクに障害が生じた場合に、スパニング ツリー ルートへの代替パスを提供できます。

リンク 1 (ルート リンク) は、スパニング ツリー フォワーディング ステートです。リンク 2 およびリンク 3 は、スパニング ツリー ブロッキング ステートの代替冗長リンクです。スイッチ 1、スタック ルート ポート、あるいはリンク 1 に障害が発生すると、CSUF はスイッチ 2 またはスイッチ 3 のいずれかの代替スタック ルート ポートを選択し、1 秒未満でそのポートをフォワーディング ステートに変更します。

図 21-5 CSUF のトポロジ



何らかのリンク損失またはスパニング ツリー イベントが発生すると (「[高速コンバージェンスを実行させるイベント](#)」(P.21-7) を参照)、Fast Uplink Transition Protocol は近接リストを使用して、スタック メンバーに高速トランジション要求を送信します。

高速トランジション要求を送信するスイッチは、ルート ポートとして選択したポートを高速トランジションでフォワーディング ステートにする必要があります。また、高速トランジションを実行する前に、スタックの各スイッチから確認応答を受信する必要があります。

スタックの各スイッチは、ルート、コスト、およびブリッジ ID を比較して、送信側スイッチが自身よりもスパニング ツリー インスタンスのスタック ルートとして適しているかどうかを判別します。送信側スイッチがスタック ルートとして最適である場合、スタック内の各スイッチは確認応答を戻します。最適でない場合には、高速トランジション要求を送信します。この場合、送信側スイッチは、すべてのスタック スイッチからは確認応答を受信しないことになります。

すべてのスタック スイッチから確認応答を受信すると、送信側スイッチの **Fast Uplink Transition Protocol** は、そのスイッチの代替スタック ルート ポートをただちにフォワーディング ステートに移行させます。送信側スイッチがすべてのスタック スイッチからの確認応答を得られなかった場合、通常のスパニング ツリー トランジション（ブロッキング、リスニング、ラーニング、フォワーディング）が実行され、スパニング ツリー トポロジのコンバージェンスは標準の速度（2 × 転送遅延時間 + 最大エージング タイム）で行われます。

Fast Uplink Transition Protocol は、VLAN 単位で実装され、一度に 1 つのスパニング ツリー インスタンスだけに適用されます。

高速コンバージェンスを実行させるイベント

CSUF 高速コンバージェンスが実行されるかどうかは、ネットワークのイベントまたは障害によります。

高速コンバージェンス（通常のネットワーク状況で 1 秒未満）は、次の状況のもとで実行されます。

- スタック ルート ポートのリンクに障害が発生した場合
スタック内の 2 つのスイッチにルートへの代替パスが設定されている場合は、1 つのスイッチだけが高速トランジションを実行します。
- スタック ルートとスパニング ツリー ルートを接続しているリンクの障害が回復した場合
- ネットワークの再構築により、新しいスタック ルート スイッチが選択された場合
- ネットワークの再構築により、現在のスタック ルート スイッチの新しいポートがスタック ルートポートとして選択された場合



(注) 複数のイベントが同時に発生すると、高速トランジションが実行されないことがあります。たとえば、スタック メンバーの電源が切断され、同時に、スタック ルートからスパニング ツリー ルートへのリンク障害が回復した場合、標準のスパニング ツリー コンバージェンスが実行されます。

標準のスパニング ツリー コンバージェンス（30 ~ 40 秒）は、次の状況のもとで実行されます。

- スタック ルート スイッチの電源が切断された場合、またはソフトウェア障害が発生した場合
- スタック ルート スイッチの電源または障害が回復した場合
- スタック ルートになる可能性のある新しいスイッチが、スタックに追加された場合

BackboneFast の概要

BackboneFast は、バックボーンのコアにおける間接障害を検出します。**BackboneFast** は、**UplinkFast** 機能を補完するテクノロジーです。**UplinkFast** は、アクセス スイッチに直接接続されたリンクの障害に対応します。**BackboneFast** は、最大エージング タイマーを最適化します。最大エージング タイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDU は他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、**BackboneFast** はルートまでの別のパスを見つけようとします。

BackboneFast をイネーブルにするには、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。スイッチ上のルート ポートまたはブロック インターフェイスが指定スイッチから下位 BPDU を受信すると、BackboneFast が開始します。下位 BPDU は、ルートブリッジと指定スイッチの両方として宣言したスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルートスイッチ間の接続が切断されています）。スパニング ツリーのルールとして、**spanning-tree vlan vlan-id max-age** グローバル コンフィギュレーション コマンドによって設定された最大エージング タイムの間、スイッチは下位 BPDU を無視します。

スイッチは、ルートスイッチへの代替パスの有無を判断します。下位 BPDU がブロック インターフェイスに到達した場合、スイッチ上のルートポートおよび他のブロック インターフェイスがルートスイッチへの代替パスになります（セルフループポートは、ルートスイッチへの代替パスとは見なされません）。下位 BPDU がルートポートに到達した場合、すべてのブロック インターフェイスがルートスイッチへの代替パスになります。下位 BPDU がルートポートに到達し、しかもブロック インターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージング タイムが経過するまで待ち、通常のスパンニング ツリー ルールに従ってルートスイッチになります。

スイッチが代替パスでルートスイッチに到達できる場合、スイッチはその代替パスを使用して、**Root Link Query (RLQ)** 要求を送信します。スイッチは、スタックメンバーがルートスイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスに RLQ 要求を送信し、ネットワーク内およびスタック内の他のスイッチからの RLQ 応答を待機します。

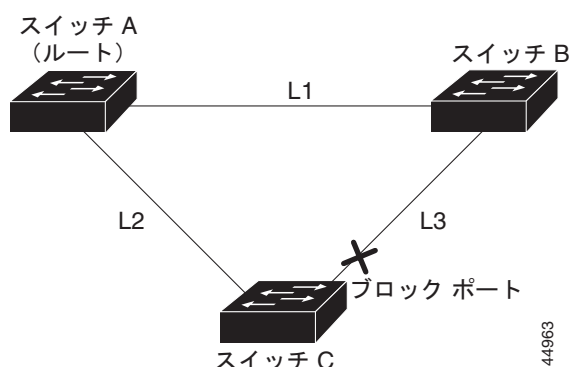
スタックメンバーは、ブロック インターフェイス上の非スタックメンバーから RLQ 応答を受け取り、その応答が別の非スタックスイッチ宛てだった場合には、スパニング ツリー インターフェイス ステートに関係なくその応答パケットを転送します。

スタックメンバーは、非スタックメンバーから RLQ 応答を受信し、その応答がスタック宛てだった場合は、他のすべてのスタックメンバーがその応答を受信できるように、それを転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェイスの最大エージング タイムが経過するまで待ちます。ルートスイッチへのすべての代替パスが、スイッチとルートスイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルートスイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイスを指定ポートにして、（ブロッキング ステートになっていた場合）ブロッキング ステートを解除し、リスニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 21-6 に、リンク障害が発生していないトポロジの例を示します。ルートスイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 21-6 間接リンク障害発生前の BackboneFast の例



44963

図 21-7 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、その障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。ルート スイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。図 21-7 では、リンク L1 で障害が発生した場合 BackboneFast がどのようにトポロジを再構成するかを示します。

図 21-7 間接リンク障害発生後の BackboneFast の例

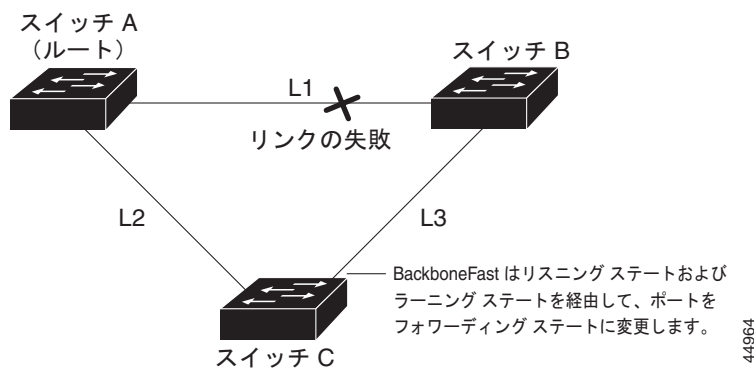
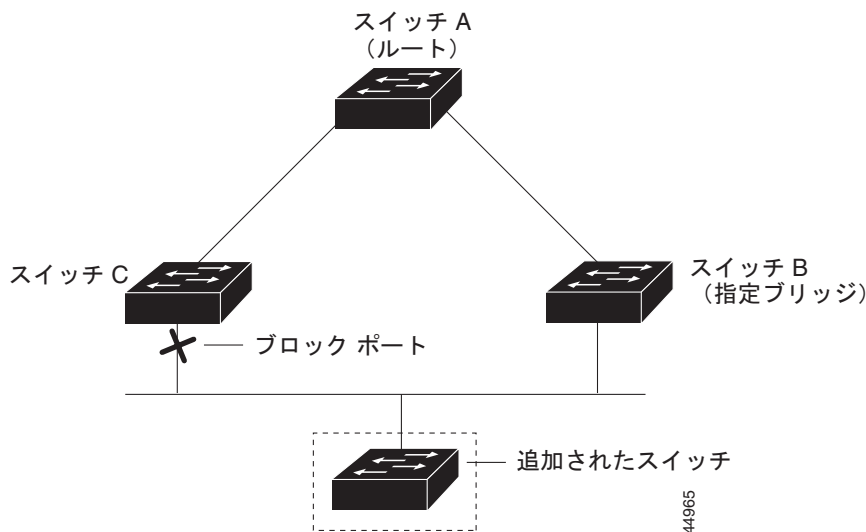


図 21-8 のように、新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ (スイッチ B) から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 21-8 メディア共有型トポロジにおけるスイッチの追加



EtherChannel ガードの概要

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャンネルのパラメータが異なる場合にも、設定の矛盾が発生します。EtherChannel 設定時の注意事項については、「[EtherChannel 設定時の注意事項](#)」(P.37-12) を参照してください。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを `errdisable` ステートにし、エラー メッセージを表示します。

spanning-tree etherchannel guard misconfig グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

ルート ガードの概要

SP (サービス プロバイダー) のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、[図 21-9](#) に示すように、スパニング ツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルート ガード機能をイネーブルに設定します。スパニング ツリーの計算によってカスタマー ネットワーク内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを `root-inconsistent` (ブロッキング) ステートにして、カスタマーのスイッチがルート スイッチにならないように、またはルートへのパスに組み込まれないようにします。

SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ (`root-inconsistent` ステートになり)、スパニング ツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはなく、ルートへのパスに組み込まれることもありません。

スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって **Internal Spanning-Tree (IST)** インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化されたあと、マッピングされます。

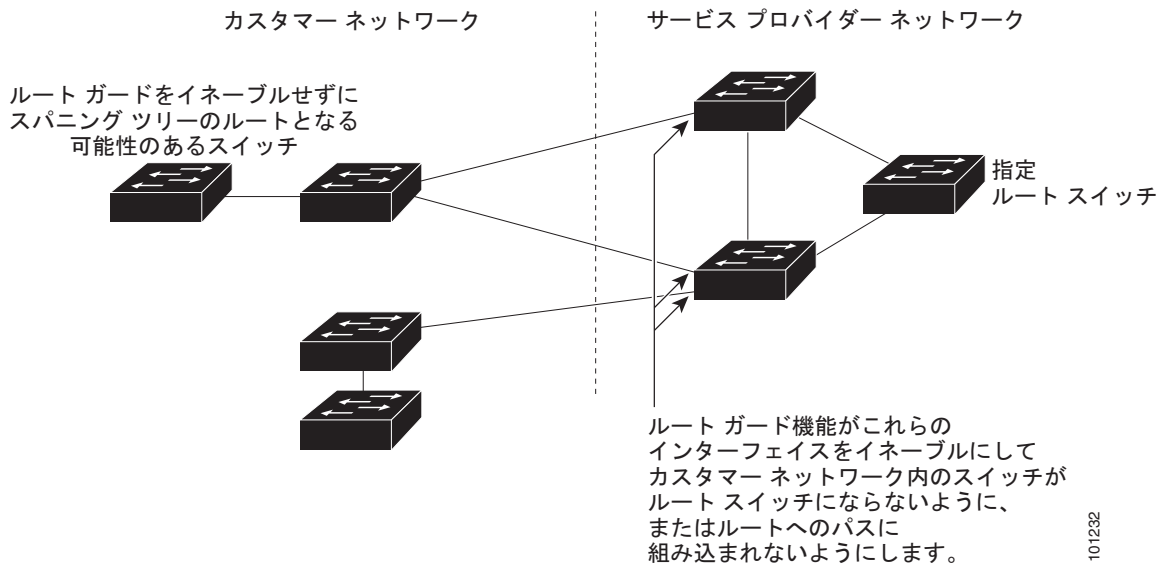
spanning-tree guard root インターフェイス コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。



注意

ルート ガード機能は使い方を誤ると、接続が切断されることがあります。

図 21-9 サービス プロバイダー ネットワークのルート ガード



ループ ガードの概要

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体でイネーブルに設定した場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニング ツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替ポートおよびルート ポートが指定ポートになることが防止され、スパニング ツリーがルート ポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされている場合に限り、非境界ポートで BPDU を送信しません。境界ポートでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

オプションのスパニング ツリー機能の設定

ここでは、次の設定情報について説明します。

- 「オプションのスパニング ツリー機能のデフォルト設定」 (P.21-12)
- 「オプションのスパニング ツリー設定時の注意事項」 (P.21-12)
- 「PortFast のイネーブル化」 (P.21-12) (任意)
- 「BPDU ガードのイネーブル化」 (P.21-13) (任意)
- 「BPDU フィルタリングのイネーブル化」 (P.21-15) (任意)
- 「冗長リンク用 UplinkFast のイネーブル化」 (P.21-16) (任意)

- ・ 「CSUF のイネーブル化」 (P.21-17) (任意)
- ・ 「BackboneFast のイネーブル化」 (P.21-17) (任意)
- ・ 「EtherChannel ガードのイネーブル化」 (P.21-17) (任意)
- ・ 「ルート ガードのイネーブル化」 (P.21-18) (任意)
- ・ 「ループ ガードのイネーブル化」 (P.21-19) (任意)

オプションのスパニング ツリー機能のデフォルト設定

表 21-1 に、オプションのスパニング ツリー機能のデフォルト設定を示します。

表 21-1 オプションのスパニング ツリー機能のデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル (インターフェイス単位で個別に設定する場合を除く)
UplinkFast	グローバルにディセーブル (Catalyst 3750 スイッチでは、UplinkFast 機能は CSUF 機能です)
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル
ルート ガード	すべてのインターフェイスでディセーブル
ループ ガード	すべてのインターフェイスでディセーブル

オプションのスパニング ツリー設定時の注意事項

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、PortFast、BPDU ガード、BPDU フィルタリング、EtherChannel ガード、ルート ガード、またはループ ガードを設定できます。

Rapid PVST+ または MSTP に対して UplinkFast、BackboneFast、またはクロススタック UplinkFast 機能を設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、この機能はディセーブル (非アクティブ) のままです。

PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニング ツリー フォワーディング ステートに移行されます。




注意

PortFast を使用するのは、単一エンド ステーションをアクセス ポートまたはトランク ポートに接続する場合に限定してください。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、スパニング ツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャスト ストームおよびアドレス学習の障害が起きる可能性があります。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。詳細は、第 16 章「音声 VLAN の設定」を参照してください。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、この機能をイネーブルにできません。

PortFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>spanning-tree portfast [trunk]</code>	<p>単一ワークステーションまたはサーバに接続されたアクセスポート上で PortFast をイネーブルにします。 trunk キーワードを指定すると、トランク ポート上で PortFast をイネーブルにできます。</p> <p>(注) トランク ポート上で PortFast 機能をイネーブルにするには、spanning-tree portfast trunk インターフェイス コンフィギュレーション コマンドを使用しなければなりません。 spanning-tree portfast コマンドは、トランク ポート上では機能しないためです。</p> <p> 注意 トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバの間にループがないことを確認してください。</p> <p>デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show spanning-tree interface interface-id portfast</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) **spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

PortFast 機能をディセーブルにするには、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用します。

BPDU ガードのイネーブル化

PortFast 対応ポート (PortFast 動作ステートのポート) で BPDU ガードをグローバルにイネーブルにしても、スパニング ツリーはポートで引き続き実行されます。ポートは BPDU を受信するまでアップのままになります。

設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは `errdisable` ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、`errdisable detect cause bpduguard shutdown vlan` グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

手動でポートを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。



注意

PortFast は、エンド ステーションに接続するポートに限って設定します。そうしないと、偶発的なトポジグループが原因でデータ パケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

PortFast 機能をイネーブルにしなくても、`spanning-tree bpduguard enable` インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、`errdisable` ステートになります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。

BPDU ガード機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>spanning-tree portfast bpduguard default</code>	BPDU ガードをグローバルにイネーブルにします。 BPDU ガードは、デフォルトではディセーブルに設定されています。
ステップ 3	<code>interface interface-id</code>	エンド ステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>spanning-tree portfast</code>	PortFast 機能をイネーブルにします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BPDU ガードをディセーブルにするには、`no spanning-tree portfast bpduguard default` グローバル コンフィギュレーション コマンドを使用します。

`no spanning-tree portfast bpduguard default` グローバル コンフィギュレーション コマンドの設定を上書きするには、`spanning-tree bpduguard enable` インターフェイス コンフィギュレーション コマンドを使用します。

BPDU フィルタリングのイネーブル化

PortFast 対応インターフェイスで BPDU フィルタリングをグローバルにイネーブルにすると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。



注意

PortFast は、エンドステーションに接続するインターフェイスに限って設定します。そうしないと、偶発的なトポロジループが原因でデータパケットループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpdudfilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネーブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できなくなります。



注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU フィルタリング機能をイネーブルにできます。

BPDU フィルタリング機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree portfast bpdudfilter default	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 3	interface interface-id	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BPDU フィルタリングをディセーブルにするには、**no spanning-tree portfast bpdudfilter default** グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpdudfilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdudfilter enable** インターフェイス コンフィギュレーション コマンドを使用します。

冗長リンク用 UplinkFast のイネーブル化

スイッチ プライオリティが設定されている VLAN 上では、UplinkFast をイネーブルにできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan *vlan-id* priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。



(注) UplinkFast をイネーブルにすると、スイッチ スタックのすべての VLAN に影響します。個々の VLAN に UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して、UplinkFast または CSUF 機能を設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、この機能はディセーブル（非アクティブ）のままです。

UplinkFast および CSUF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree uplinkfast [max-update-rate <i>pkts-per-second</i>]	UplinkFast をイネーブルにします。 (任意) <i>pkts-per-second</i> に指定できる範囲は 0 ~ 32000 パケット/秒です。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないため、接続切断後スパニング ツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上でも CSUF がイネーブルになります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されます。UplinkFast をイネーブルにする、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上に変更した場合、パス コストは変更されません)。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

アップデート パケット レートをデフォルトの設定値に戻す場合は、**no spanning-tree uplinkfast max-update-rate** グローバル コンフィギュレーション コマンドを使用します。UplinkFast をディセーブルにするには、**no spanning-tree uplinkfast** コマンドを使用します。

CSUF のイネーブル化

spanning-tree uplinkfast グローバル コンフィギュレーション コマンドを使用して UplinkFast 機能をイネーブルまたはディセーブルにすると、CSUF は自動的に非スタック ポート インターフェイス上でグローバルにイネーブルまたはディセーブルになります。

詳細については、「冗長リンク用 UplinkFast のイネーブル化」(P.21-16) を参照してください。

スイッチおよびそのすべての VLAN で UplinkFast をディセーブルにするには、**no spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用します。

BackboneFast のイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニング ツリーの再構成をより早く開始できます。



(注) BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルにしなければなりません。BackboneFast は、トークンリング VLAN 上ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

Rapid PVST+ または MSTP 用に、BackboneFast 機能を設定できます。ただし、スパニング ツリーモードを PVST+ に変更するまで、この機能はディセーブル (非アクティブ) のままです。

BackboneFast をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree backbonefast	BackboneFast をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BackboneFast 機能をディセーブルにするには、**no spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

EtherChannel ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree etherchannel guard misconfig	EtherChannel ガードをイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel ガード機能をディセーブルにするには、**no spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているスイッチ ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正したあと、誤って設定していたポート チャネル インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）ステートになり、フォワーディング ステートに移行できなくなります。



(注) ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできません。

インターフェイス上でルート ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree guard root	インターフェイスでルート ガードをイネーブルに設定します。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセーブルです。
ステップ 4	end	特権 EXEC モードに戻ります。

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

ルート ガードをディセーブルにするには、**no spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。

ループ ガードのイネーブル化

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。ループ ガードは、スパニング ツリーがポイントツーポイントと見なすインターフェイス上に限り動作します。



(注) ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、この機能をイネーブルにできません。

ループ ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	show spanning-tree active または show spanning-tree mst	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree loopguard default	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ループ ガードをグローバルにディセーブルにするには、**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用すると、**no spanning-tree loopguard default** グローバル コンフィギュレーション コマンドの設定値を上書きすることができます。

スパニング ツリー ステータスの表示

スパニング ツリー ステータスを表示するには、表 21-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 21-2 スパニング ツリー ステータスを表示するためのコマンド

コマンド	目的
<code>show spanning-tree active</code>	アクティブ インターフェイスに関するスパニング ツリー情報だけを表示します。
<code>show spanning-tree detail</code>	インターフェイス情報の詳細サマリーを表示します。
<code>show spanning-tree interface interface-id</code>	特定のインターフェイスのスパニング ツリー情報を表示します。
<code>show spanning-tree mst interface interface-id</code>	特定のインターフェイスの MST 情報を表示します。
<code>show spanning-tree summary [totals]</code>	インターフェイス ステートのサマリーを表示します。またはスパニング ツリー ステート セクションのすべての行を表示します。

`clear spanning-tree [interface interface-id]` 特権 EXEC コマンドを使用して、スパニング ツリー カウンタをクリアできます。

`show spanning-tree` 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER 22

Flex Link および MAC アドレス テーブル 移動更新機能の設定

ここでは、Catalyst 3750 スイッチ上の Flex Link を設定する方法について説明します。これは、相互にバックアップするのに使用するインターフェイス ペアです。また、MAC（メディア アクセス制御）アドレス テーブル移動更新機能の設定方法についても説明します（Flex Link の双方向高速コンバージェンス機能でも参照できます）。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチ およびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「Flex Link および MAC アドレス テーブル移動更新機能の概要」 (P.22-1)
- 「Flex Link および MAC アドレス テーブル移動更新機能の設定」 (P.22-8)
- 「Flex Link および MAC アドレス テーブル移動更新機能のモニタ」 (P.22-14)

Flex Link および MAC アドレス テーブル移動更新機能の概要

ここでは、次の情報について説明します。

- 「Flex Link」 (P.22-2)
- 「VLAN Flex Link ロード バランシングおよびサポート」 (P.22-3)
- 「Flex Link マルチキャスト高速コンバージェンス」 (P.22-3)
- 「MAC アドレス テーブル移動更新」 (P.22-6)

Flex Link

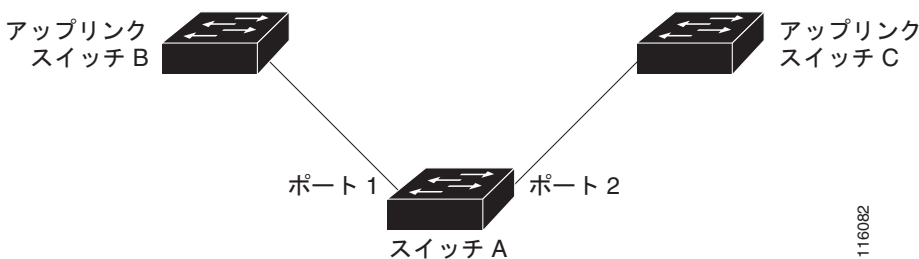
Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、一方のインターフェイスが他方のインターフェイスのバックアップとして動作するように設定されています。この機能は、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) の代替ソリューションとして役立ちます。Flex Link があれば、STP をディセーブルにしても基本的なリンクの冗長性は失われません。Flex Link は一般的に、カスタマーがスイッチで STP を稼動したくない場合に、サービス プロバイダーまたは企業ネットワークで設定されます。スイッチで STP が稼動している場合、すでに STP がリンクレベルの冗長性またはバックアップ機能を提供しているので、Flex Link を設定する必要はありません。

一方のレイヤ 2 インターフェイスを Flex Link またはバックアップ リンクとして割り当てることで、他方のレイヤ 2 インターフェイス（アクティブ リンク）に Flex Link を設定できます。Flex Link をスタック内の同じスイッチ、または別のスイッチで設定できます。一方のリンクがアップ状態でトラフィックを転送する場合、他方のリンクはスタンバイ モードになって、シャットダウンした場合にトラフィックを転送する準備をします。指定された時間に、インターフェイス 1 だけが linkup ステートになってトラフィックを転送します。プライマリ リンクがシャットダウンした場合、スタンバイ リンクがトラフィックの転送を開始します。アクティブ リンクがバックアップ状態になった場合、リンクはスタンバイ モードになって、トラフィックは転送されません。Flex Link インターフェイスでは、STP はディセーブルです。

図 22-1 では、スイッチ A のポート 1 および 2 はアップリンク スイッチ B および C と接続されています。ポートは Flex Link として設定されているので、インターフェイスのうち 1 つだけがトラフィックを転送し、残りのインターフェイスがスタンバイ モードになります。ポート 1 がアクティブ リンクの場合、ポート 1 とスイッチ B の間でトラフィックの転送を開始します。ポート 2（バックアップ リンク）とスイッチ C の間のリンクは、トラフィックを転送しません。ポート 1 がダウンした場合、ポート 2 がアップ状態になってスイッチ C へのトラフィックの転送を開始します。ポート 1 が再びバックアップ状態になった場合、ポート 1 はスタンバイ モードになってトラフィックは転送しません。ポート 2 はトラフィックを転送し続けます。

また、トラフィックの転送に優先ポートを指定して、プリエンプト メカニズムを設定するように選択できます。たとえば、図 22-1 の例では、Flex Link ペアをプリエンプト モードで設定することができます。以下のシナリオでは、ポート 1 がバックアップとなってポート 2 の帯域幅より広い場合は、ポート 1 が 60 秒後にトラフィックの転送を開始します。ポート 2 がスタンバイ ポートになります。これは、`switchport backup interface preemption mode bandwidth` および `switchport backup interface preemption delay` インターフェイス コンフィギュレーション コマンドを入力することで実行できます。

図 22-1 Flex Link の設定例

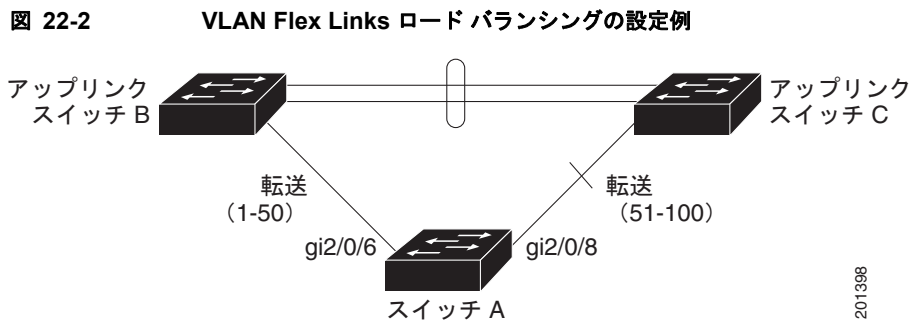


プライマリ（転送）リンクがダウンした場合、トラップはネットワーク管理ステーションに通知します。スタンバイ リンクがダウンした場合、トラップはユーザに通知します。

Flex Link はレイヤ 2 ポートおよびポート チャネルでのみサポートされ、VLAN やレイヤ 3 ポートではサポートされません。

VLAN Flex Link ロード バランシングおよびサポート

VLAN Flex Link ロード バランシングにより、相互に排他的な VLAN のトラフィックを両方のポートで同時に転送するように Flex Link ペアを設定できます。たとえば、Flex Link ポートが 1 ~ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。どちらかのポートで障害が発生した場合には、もう一方のアクティブ ポートがすべてのトラフィックを転送します。障害ポートが回復すると、優先する VLAN のトラフィックの転送を再開します。このように、Flex Link のペアは冗長性を提供するだけでなく、ロード バランシングの用途に使用できます。また、Flex Link VLAN ロード バランシングによってアップリンク スイッチが制約を受けることはありません。



Flex Link マルチキャスト高速コンバージェンス

Flex Link マルチキャスト高速コンバージェンスを使用すると、Flex Link に障害が発生したときのマルチキャスト トラフィックのコンバージェンス時間が削減されます。次のソリューションを組み合わせることでこれを実装します。

- 「他の Flex Link ポートのマルチキャスト ルータ ポートとしての学習」(P.22-3)
- 「IGMP レポートの生成」(P.22-4)
- 「IGMP レポートの送信」(P.22-4)
- 「設定例」(P.22-4)

他の Flex Link ポートのマルチキャスト ルータ ポートとしての学習

一般的なマルチキャスト ネットワークでは、各 VLAN についてクエリアが用意されています。ネットワークのエッジに配置されているスイッチには、Flex Link ポートの受信クエリーのいずれかがありません。Flex Link ポートはまた、どのようなときでも常に転送を行っています。

クエリーを受信するポートは、スイッチでマルチキャスト ルータ ポートとして追加されます。マルチキャスト ルータ ポートは、スイッチにより学習されたすべてのマルチキャスト グループに属していません。変更後、他の Flex Link ポートがクエリーを受信します。そしてまた他の Flex Link ポートがマルチキャスト ルータ ポートとして学習されます。変更後、マルチキャスト トラフィックは他の Flex Link ポートに流れます。トラフィックのコンバージェンスをさらに高速にするために、いずれかの Flex Link ポートがマルチキャスト ルータ ポートとして学習されている場合、両方の Flex Link ポートがマルチキャスト ルータ ポートとして学習されます。両方の Flex Link ポートは常に、マルチキャスト グループに属しています。

通常の操作モードでは、両方の Flex Link ポートがグループに属していますが、バックアップ ポート上のすべてのトラフィックはブロックされています。そのため、バックアップ ポートをマルチキャスト ルータ ポートとして追加しても、通常のマルチキャスト データのフローには影響がありません。変更が発生すると、バックアップ ポートのブロックが解除され、トラフィックが流れるようになります。この場合、アップストリーム マルチキャスト データは、バックアップ ポートのブロックが解除され次第流れるようになります。

IGMP レポートの生成

変更後にバックアップ リンクが起動しても、アップストリームの新しい分散スイッチはマルチキャスト データの転送を開始しません。これは、アップストリーム ルータ上のポートはブロックされている Flex Link ポートに接続していますが、どのマルチキャスト グループにも属していないためです。バックアップ リンクがブロックされているため、マルチキャスト グループのレポートはダウンストリーム スイッチによって転送されませんでした。データは、ポートがマルチキャスト グループを学習するまでこのポートを流れません。これは、ポートがレポートを受信したあとにのみ行われます。

ホストは、一般クエリーを受信するときにレポートを送信します。通常のシナリオでは、一般的なクエリーは 60 秒以内に送信されます。バックアップ リンクが転送を開始すると、マルチキャスト データのコンバージェンスをさらに高速にするために、ダウンストリーム スイッチは、一般クエリーを待たずにこのポート上で学習されたすべてのグループに関するプロキシ レポートをすぐに送信します。

IGMP レポートの送信

マルチキャスト トラフィックのコンバージェンス時の損失を最低限に抑えるには、Flex Link アクティブ リンクがダウンする前に冗長データ パスを設定する必要があります。そのためには、Flex Link バックアップ リンクに IGMP レポート パケットのみが流れるようにします。これらの送信された IGMP レポート メッセージは、アップストリームの分散ルータによって処理されます。そのため、マルチキャスト データ トラフィックはバックアップ インターフェイスに転送されます。バックアップ インターフェイスに着信したすべてのトラフィックはアクセス スイッチの入力側で廃棄され、ホストが重複マルチキャスト トラフィックを受信することはありません。Flex Link アクティブ リンクに障害が発生すると、アクセス スイッチがバックアップ リンクからのトラフィックの受信を即時に開始します。この方式の唯一の欠点は、分散スイッチ間のリンクおよび分散スイッチとアクセス スイッチ間のバックアップ リンクの帯域幅を消費することです。この機能はデフォルトでディセーブルになっています。設定するには、**switchport backup interface interface-id multicast fast-convergence** コマンドを使用します。

変更時にこの機能をイネーブルにしていると、スイッチはバックアップ ポート（今後転送ポートとなる）のプロキシ レポートを生成しません。

設定例

次に、Flex Link がギガビット イーサネット 1/0/11 およびギガビット イーサネット 1/0/12 上に設定されている場合に、その他の Flex Link ポートをマルチキャスト ルータ ポートとしてデータを流す設定例および **show interfaces switchport backup** コマンドの出力例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabithernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface gigabithernet1/0/12
Switch(config-if)# exit
Switch(config)# interface gigabithernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
```

```
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

次の出力は、クエリーがギガビット イーサネット 1/0/11 を介してスイッチに到達する場合の、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1         v2                 Gi1/0/11
401      41.41.41.1     v2                 Gi1/0/11
```

次に、VLAN 1 および 401 についての `show ip igmp snooping mrouter` コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan      ports
-----
1         Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401      Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートは学習されたグループに属しています。次の例では、ギガビット イーサネット 2/0/11 が VLAN 1 のレシーバー/ホストであり、2 つのマルチキャスト グループに関係します。

```
Switch# show ip igmp snooping groups
Vlan      Group           Type      Version      Port List
-----
1         228.1.5.1      igmp     v2           Gi1/0/11, Gi1/0/12, Gi2/0/11
1         228.1.5.2      igmp     v2           Gi1/0/11, Gi1/0/12, Gi2/0/11
```

ホストが一般クエリーに応答するときに、スイッチはすべてのマルチキャスト ルータ ポートに関するこのレポートを転送します。この例では、ホストがレポートをグループ 228.1.5.1 に送信する場合、レポートはギガビット イーサネット 1/0/11 上でだけ転送されます。これは、バックアップ ポート ギガビット イーサネット 1/0/12 がブロックされているためです。アクティブ リンク ギガビット イーサネット 1/0/11 がダウンすると、バックアップ ポート ギガビット イーサネット 1/0/12 が転送を開始します。

このポートが転送を開始するとすぐに、スイッチはホストの代わりにプロキシ レポートをグループ 228.1.5.1 および 228.1.5.2 に送信します。アップストリーム ルータはグループを学習して、マルチキャスト データの転送を開始します。これが Flex Link のデフォルトの動作です。ユーザが `switchport backup interface gigabitEthernet 1/0/12 multicast fast-convergence` コマンドを使用して高速コンバージェンスを設定すると、この動作は変わります。次に、この機能をオンにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 1/0/11
Switch(config-if)# switchport backup interface gigabitEthernet 1/0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active      Interface      Backup Interface State
-----
GigabitEthernet1/0/11 GigabitEthernet1/0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
```

```
Bandwidth : 100000 Kbit (Gi1/0/11), 100000 Kbit (Gi1/0/12)
Mac Address Move Update Vlan : auto
```

次の出力は、クエリーがギガビット イーサネット 1/0/11 を介してスイッチに到達する場合の、VLAN 1 および VLAN 401 のクエリアを示します。

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version    Port
-----
1         1.1.1.1        v2              Gi1/0/11
401      41.41.41.1     v2              Gi1/0/11
```

次に、VLAN 1 および 401 についての `show ip igmp snooping mrouter` コマンドの出力を示します。

```
Switch# show ip igmp snooping mrouter
Vlan      ports
-----
1         Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401      Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

同様に、両方の Flex Link ポートは学習されたグループに属しています。次の例では、ギガビット イーサネット 2/0/11 が VLAN 1 のレシーバー/ホストであり、2つのマルチキャスト グループに関係します。

```
Switch# show ip igmp snooping groups
Vlan      Group          Type    Version    Port List
-----
1         228.1.5.1     igmp   v2         Gi1/0/11, Gi1/0/12, Gi2/0/11
1         228.1.5.2     igmp   v2         Gi1/0/11, Gi1/0/12, Gi2/0/11
```

ホストが一般クエリーに応答するときはいつでも、スイッチはすべてのマルチキャスト ルータ ポートに関するこのレポートを転送します。コマンドライン ポートを使用してこの機能をオンにすると、レポートは、GigabitEthernet1/0/11 上のスイッチによって転送されるときにバックアップ ポート GigabitEthernet1/0/12 にも送信されます。アップストリーム ルータはグループを学習して、マルチキャスト データの転送を開始しますが、GigabitEthernet1/0/12 がブロックされているため、このマルチキャスト データは入力側で廃棄されます。アクティブ リンク ギガビット イーサネット 1/0/11 がダウンすると、バックアップ ポート ギガビット イーサネット 1/0/12 が転送を開始します。マルチキャスト データはアップストリーム ルータによってすでに転送されているため、プロキシ レポートを送信する必要はありません。レポートをバックアップ ポートに送信することで、冗長マルチキャスト パスが設定され、マルチキャスト トラフィック コンバージェンスにかかる時間が最小限で済みます。

MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能を使用すると、プライマリ (フォワーディング) リンクがダウンし、スタンバイ リンクがトラフィックの転送を開始するときに、スイッチで双方向の高速コンバージェンスを提供できます。

図 22-3 のスイッチ A はアクセス スイッチで、ポート 1 およびポート 2 は、Flex Link のペアを介してアップリンク スイッチ B および D に接続されています。ポート 1 はトラフィックを転送し、ポート 2 はバックアップ ステート状態です。PC からサーバへのトラフィック転送は、ポート 1 からポート 3 へ流れます。PC の MAC アドレスはスイッチ C のポート 3 で学習されます。サーバから PC へのトラフィック転送は、ポート 3 からポート 1 へ流れます。

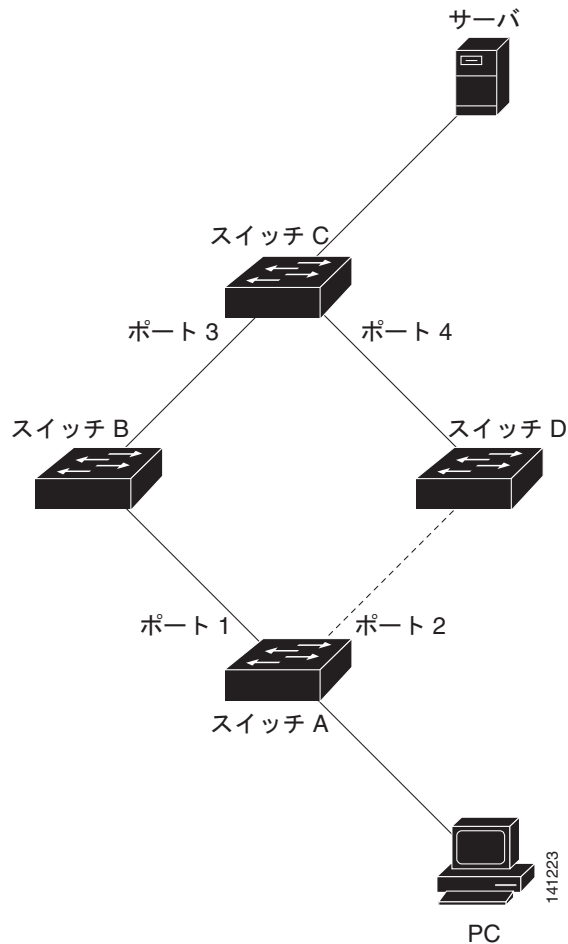
MAC アドレス テーブル移動更新機能が設定されていない状態でポート 1 がダウンすると、ポート 2 がトラフィック転送を開始します。短時間、スイッチ C はポート 3 を使用してサーバから PC へのトラフィックを転送しますが、PC はポート 1 がダウンしているため、そのトラフィックを受信しません。スイッチ C がポート 3 の PC の MAC アドレスを削除してポート 4 で再度学習すると、サーバから PC へのトラフィックを転送できます (ポート 2 を使用します)。

図 22-3 で、MAC アドレス テーブル移動更新機能を設定してスイッチ上でイネーブルにしている場合、ポート 1 がダウンしても、ポート 2 が PC からサーバへトラフィック転送を開始します。スイッチは MAC アドレス テーブル移動更新 packets をポート 2 から送信します。スイッチ C はこの packets をポート 4 で受信すると、すぐに PC のポート 4 の MAC アドレスを学習するので、コンバージェンスを繰り返す時間を短縮できます。

アクセス スイッチ (スイッチ A) を設定して MAC アドレス テーブル移動更新メッセージを送信できます。また、アップリンク スイッチ B、C、D を設定して MAC アドレス テーブル移動更新メッセージを受信し、処理することもできます。スイッチ C は MAC アドレス テーブル移動更新メッセージをスイッチ A から受信すると、PC のポート 4 の MAC アドレスを学習します。次に、スイッチ C は PC のフォワーディング テーブルのエントリを含む MAC アドレス テーブルを更新します。

スイッチ A は、MAC アドレス テーブルの更新を待機する必要はありません。スイッチがポート 1 で障害を検出し、新規転送ポートであるポート 2 からのサーバトラフィックの転送を即座に開始します。この変更は 100 ミリ秒 (ms) 以内に発生します。PC はスイッチ A に直接接続され、接続ステータスは変更されません。スイッチ A は、MAC アドレス テーブル内の PC エントリを更新する必要はありません。

図 22-3 MAC アドレス テーブル移動更新の設定例



Flex Link および MAC アドレス テーブル移動更新機能の設定

ここでは、次の情報について説明します。

- 「デフォルト設定」(P.22-8)
- 「設定時の注意事項」(P.22-8)
- 「Flex Link の設定」(P.22-9)
- 「Flex Link の VLAN ロード バランシングの設定」(P.22-11)
- 「MAC アドレス テーブル移動更新機能の設定」(P.22-12)

デフォルト設定

Flex Link は設定されていません。また、バックアップ インターフェイスも定義されていません。

プリエンブト モードはオフです。

プリエンブト遅延は 35 秒です。

MAC アドレス テーブル移動更新機能はスイッチに設定されていません。

設定時の注意事項

Flex Link を設定するときには、次の注意事項に従ってください。

- バックアップ リンクは 16 まで設定できます。
- アクティブ リンクに対し、Flex Link のバックアップ リンクを 1 つのみ設定できます。このリンクはアクティブ インターフェイスとは異なるインターフェイスである必要があります。
- インターフェイスは Flex Link ペアの 1 つにのみ、所属できます。インターフェイスは 1 つのアクティブ リンクに対してのみ、バックアップ リンクになれます。アクティブ リンクは別の Flex Link ペアに所属できません。
- どちらのリンクも EtherChannel のポートにはなれません。ただし、ポート チャネルまたは物理インターフェイスのいずれかがアクティブ リンクである場合、ポート チャネル 2 つ (EtherChannel 論理インターフェイス) を Flex Link として、またポート チャネルと物理インターフェイスを Flex Link として設定できます。
- バックアップ リンクはアクティブ リンクと同じタイプ (ファストイーサネット、ギガビットイーサネット、またはポート チャネル) にする必要はありません。ただし、スタンバイ リンクがトラフィックの転送を開始した場合に、ループや動作変更が起きないように、両方の Flex Link を類似の特性で設定する必要があります。
- Flex Link ポートでは、STP はディセーブルです。ポートの VLAN に STP が設定されていても、Flex Link ポートは STP に参加しません。STP がイネーブルでない場合、設定したトポロジでループが発生しないようにしてください。Flex Link 設定が削除されると、そのポートの STP は再びイネーブルになります。

Flex Link 機能による VLAN ロード バランシングを設定するときには、次の注意事項に従ってください。

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイス上で優先 VLAN を選択する必要があります。

- 同一 Flex Link ペアに対してプリエンプト メカニズムと VLAN ロード バランシングを設定することはできません。

MAC アドレス テーブル移動更新機能を設定するときには、次の注意事項に従ってください。

- MAC アドレス テーブル移動更新メッセージを送信する場合、この機能をアクセス スイッチに設定してイネーブルにします。
- MAC アドレス テーブル移動更新メッセージを受信する場合、この機能をアップリンク スイッチに設定してイネーブルにします。

Flex Link の設定

Flex Link のペアを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、物理レイヤ 2 インターフェイスにすることも、ポート チャネル（論理インターフェイス）にすることもできます。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ3	<code>switchport backup interface interface-id</code>	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。1 つのリンクがトラフィックを転送している場合、残りのインターフェイスはスタンバイ モードです。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ5	<code>show interfaces [interface-id] switchport backup</code>	設定を確認します。
ステップ6	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

Flex Link バックアップ インターフェイスをディセーブルにするには、**no switchport backup interface interface-id** インターフェイス コンフィギュレーション コマンドを使用します。

次に、バックアップ インターフェイスを装備し、設定を確認するようにインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2
Switch(conf-if)# end

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
GigabitEthernet1/0/1  GigabitEthernet1/0/3  Active Standby/Backup Up
Vlans Preferred on Active Interface: 1-3,5-4094
Vlans Preferred on Backup Interface: 4
```

Flex Link のペアのプリエンプト方式を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>interface interface-id</code>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、物理レイヤ 2 インターフェイスにすることも、ポートチャネル（論理インターフェイス）にすることもできます。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ3	<code>switchport backup interface interface-id</code>	物理レイヤ 2 インターフェイス（またはポートチャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。1つのリンクがトラフィックを転送している場合、残りのインターフェイスはスタンバイ モードです。
ステップ4	<code>switchport backup interface interface-id preempt mode [forced bandwidth off]</code>	Flex Link インターフェイス ペアのプリエンプト メカニズムおよび遅延を設定します。次のようにプリエンプトを設定できます。 <ul style="list-style-type: none"> • forced : アクティブ インターフェイスが常にバックアップをプリエンプトに設定します。 • bandwidth : 広帯域幅を持つインターフェイスが常にアクティブ インターフェイスとして動作します。 • off - アクティブからバックアップへのプリエンプトは発生しません。
ステップ5	<code>switchport backup interface interface-id preempt delay delay-time</code>	ポートが別のポートのプリエンプトを実行するまでの遅延時間を設定します。 (注) 遅延時間の設定は、forced および bandwidth モードでのみ機能します。
ステップ6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show interfaces [interface-id] switchport backup</code>	設定を確認します。
ステップ8	<code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

プリエンプト方式を削除するには、`no switchport backup interface interface-id preempt mode` インターフェイス コンフィギュレーション コマンドを使用します。遅延時間をデフォルトにリセットするには、`no switchport backup interface interface-id preempt delay` インターフェイス コンフィギュレーション コマンドを使用します。

次に、バックアップ インターフェイス ペアに対して *forced* としてプリエンプト モードを設定して設定を確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)#switchport backup interface gigabitethernet1/0/2 preempt mode forced
Switch(conf-if)#switchport backup interface gigabitethernet1/0/2 preempt delay 50
Switch(conf-if)# end
```

```
Switch# show interfaces switchport backup detail
Active Interface Backup Interface State
-----
GigabitEthernet1/0/21 GigabitEthernet1/0/2 Active Up/Backup Standby
Interface Pair : Gil/0/1, Gil/0/2
```

```
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi1/0/1), 100000 Kbit (Gi1/0/2)
Mac Address Move Update Vlan : auto
```

Flex Link の VLAN ロード バランシングの設定

Flex Link の VLAN ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、物理レイヤ 2 インターフェイスにすることも、ポートチャネル（論理インターフェイス）にすることもできます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ3	switchport backup interface interface-id prefer vlan vlan-id	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定し、インターフェイス上に割り当てられた VLAN を指定します。指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ4	end	特権 EXEC モードに戻ります。
ステップ5	show interfaces [interface-id] switchport backup	設定を確認します。
ステップ6	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシング機能をディセーブルにするには、**no switchport backup interface interface-id prefer vlan vlan-range** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチに VLAN 1 ～ 50、60、および 100 ～ 120 を設定する例を示します。

```
Switch(config)#interface gigabitethernet 2/0/6
Switch(config-if)#switchport backup interface gigabitethernet 2/0/8 prefer vlan 60,100-120
```

両方のインターフェイスがアップすると、Gi2/0/8 は VLAN 60 および 100 ～ 120 のトラフィックを転送し、Gi2/0/6 は VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウン（LINK_DOWN）すると、このインターフェイスの優先 VLAN は Flex Link ペアの相手側のインターフェイスに移されます。この例では、インターフェイス Gi2/0/6 がダウンすると、Gi2/0/8 が Flex Link ペアのすべての VLAN を保持します。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
```

Flex Link および MAC アドレス テーブル移動更新機能の設定

```
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up
```

```
Vlans Preferred on Active Interface: 1-50
```

```
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスの優先 VLAN は、相手側のインターフェイス上ではブロックされ、アップしたインターフェイス上でフォワーディング ステートに移行します。この例では、インターフェイス Gi2/0/6 がアップになると、このインターフェイスの優先 VLAN は、相手側のインターフェイス Gi2/0/8 ではブロックされ、Gi2/0/6 でフォワーディングされます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
```

```
Vlans Preferred on Active Interface: 1-50
```

```
Vlans Preferred on Backup Interface: 60, 100-120
```

```
Switch#show interfaces switchport backup detail
Switch Backup Interface Pairs:
```

```
Active Interface      Backup Interface      State
-----
GigabitEthernet1/0/3  GigabitEthernet1/0/4  Active Down/Backup Up
```

```
Vlans Preferred on Active Interface: 1-2,5-4094
```

```
Vlans Preferred on Backup Interface: 3-4
```

```
Preemption Mode      : off
```

```
Bandwidth : 10000 Kbit (Gi1/0/3), 100000 Kbit (Gi1/0/4)
```

```
Mac Address Move Update Vlan : auto
```

MAC アドレス テーブル移動更新機能の設定

ここでは、次の情報について説明します。

- スイッチを設定して、MAC アドレス テーブル移動更新メッセージを送信する。
- スイッチを設定して、MAC アドレス テーブル移動更新メッセージを受信する。

MAC アドレス テーブル移動更新メッセージを送信するようにアクセス スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface interface-id	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、物理レイヤ 2 インターフェイスにすることも、ポート チャネル（論理インターフェイス）にすることもできます。指定できるポートチャネルの範囲は 1 ~ 48 です。

コマンド	目的
ステップ3 <code>switchport backup interface interface-id</code> または switchport backup interface interface-id mmu primary vlan vlan-id	物理レイヤ 2 インターフェイス（またはポート チャネル）を、インターフェイスを装備した Flex Link ペアの一部として設定します。MAC アドレス テーブル移動更新の VLAN がインターフェイスで一番小さい VLAN ID です。 物理レイヤ 2 インターフェイス（またはポート チャネル）を設定し、MAC アドレステーブル移動更新の送信に使用される、インターフェイス上の VLAN ID を指定します。 1 つのリンクがトラフィックを転送している場合、残りのインターフェイスはスタンバイ モードです。
ステップ4 <code>end</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ5 <code>mac address-table move update transmit</code>	アクセス スイッチをイネーブルにして、ネットワーク内の他のスイッチに MAC アドレス テーブル移動更新メッセージを送信します（プライマリ リンクがダウンし、スイッチがスタンバイ リンクを使用してトラフィックの転送を開始する場合）。
ステップ6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ7 <code>show mac address-table move update</code>	設定を確認します。
ステップ8 <code>copy running-config startup config</code>	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、**no mac address-table move update transmit** インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移動更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次に、MAC アドレス テーブル移動更新メッセージを送信するように、アクセス スイッチを設定する例を示します。

```
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
```

Flex Link および MAC アドレス テーブル移動更新機能のモニタ

```
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

MAC アドレス テーブル移動更新メッセージを受信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2 mac address-table move update receive	スイッチをイネーブルにして MAC アドレス テーブル移動更新メッセージを受信し、その処理を実行します。
ステップ3 end	特権 EXEC モードに戻ります。
ステップ4 show mac address-table move update	設定を確認します。
ステップ5 copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、**no mac address-table move update receive** コンフィギュレーション コマンドを使用します。MAC アドレス テーブル移動更新情報を表示するには、**show mac address-table move update** 特権 EXEC コマンドを使用します。

次に、MAC アドレス テーブル移動更新メッセージを受信して、その処理を実行できるようにスイッチを設定する例を示します。

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

Flex Link および MAC アドレス テーブル移動更新機能のモニタ

表 22-1 に、Flex Link 設定および MAC アドレス テーブル移動更新情報をモニタする特権 EXEC コマンドを示します。

表 22-1 Flex Link および MAC アドレス テーブル移動更新情報のモニタ コマンド

コマンド	目的
show interfaces [interface-id] switchport backup	1つのインターフェイスに設定された Flex Link バックアップ インターフェイス、または設定した Flex Link すべてと、アクティブおよびバックアップ インターフェイスそれぞれのステート (アップまたはスタンバイ モード) を表示します。VLAN ロード バランシングがイネーブルの場合、アクティブおよびバックアップ インターフェイス上の優先 VLAN が表示されます。
show mac address-table move update	スイッチの MAC アドレス テーブル移動更新情報を表示します。



CHAPTER 23

Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定

この章では、Catalyst 3750 スイッチに、DHCP スヌーピング機能、Option 82 データ挿入機能、および DHCP サーバのポートベースのアドレス割り当て機能を設定する方法について説明します。また、IP ソース ガード機能の設定方法も説明しています。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS DHCP Command Reference, Volume 1 of 3: Multicast*』 Release 12.2 の「DHCP Commands」のセクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「DHCP スヌーピングの概要」 (P.23-1)
- 「DHCP スヌーピングの設定」 (P.23-9)
- 「DHCP スヌーピング情報の表示」 (P.23-17)
- 「IP ソース ガードの概要」 (P.23-17)
- 「IP ソース ガードの設定」 (P.23-19)
- 「IP ソース ガード情報の表示」 (P.23-27)
- 「DHCP サーバのポートベースのアドレス割り当ての概要」 (P.23-28)
- 「DHCP サーバのポートベースのアドレス割り当ての設定」 (P.23-28)
- 「DHCP サーバのポートベースのアドレス割り当ての表示」 (P.23-31)

DHCP スヌーピングの概要

DHCP は、中央集中型サーバからホスト IP アドレスを動的に割り当てるために LAN 環境で幅広く使われており、これにより IP アドレスの管理のオーバーヘッドを大幅に軽減できます。また DHCP は、制限のある IP アドレス空間を節約します。IP アドレスをホストに永続的に割り当てる必要がなく、IP アドレスを使用するのはネットワークに接続されているホストだけになるためです。

ここでは、次の情報について説明します。

- 「DHCP サーバ」 (P.23-2)
- 「DHCP リレー エージェント」 (P.23-2)
- 「DHCP スヌーピング」 (P.23-2)
- 「Option 82 データ挿入」 (P.23-4)
- 「Cisco IOS DHCP サーバ データベース」 (P.23-7)
- 「DHCP スヌーピング バインディング データベース」 (P.23-7)
- 「DHCP スヌーピングおよびスイッチ スタック」 (P.23-9)

DHCP クライアントの詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Addressing and Services」セクションにある「Configuring DHCP」セクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上にある特定のアドレス プールから IP アドレスを DHCP クライアントに割り当て、管理します。DHCP サーバが DHCP クライアントによって要求された設定パラメータを、データベースから提供できない場合、その要求は、ネットワーク管理者によって定義された 1 つまたは複数のセカンダリ DHCP サーバへ転送されます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバ間で DHCP パケットを転送するレイヤ 3 のデバイスです。各リレー エージェントは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送します。リレー エージェントの転送方法は、通常のレイヤ 2 の転送方法 (IP データグラムがネットワーク間で透過的にスイッチングされる) とは異なります。リレー エージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して出力インターフェイスから送信します。

DHCP スヌーピング

DHCP スヌーピングとは、untrusted (信頼性のない) DHCP メッセージをフィルタリングして、DHCP スヌーピング バインディング データベース (別名 DHCP スヌーピング バインディング テーブル) を作成、維持することにより、ネットワークにセキュリティを提供する DHCP セキュリティ機能です。

DHCP スヌーピングは、untrusted ホストと DHCP サーバの間でファイアウォールのような機能を果たします。DHCP スヌーピングを使用すると、エンド ユーザに接続された untrusted インターフェイスと、DHCP サーバや別のスイッチと接続された trusted インターフェイスを区別できます。



(注) DHCP スヌーピングを適切に機能させるには、すべての DHCP サーバを trusted インターフェイスを介してスイッチと接続する必要があります。

untrusted DHCP メッセージとは、ネットワークまたはファイアウォールの外部から受信したメッセージです。サービス プロバイダー環境で DHCP スヌーピングを使用すると、untrusted メッセージがサービス プロバイダー ネットワーク外のデバイス（お客様のスイッチなど）から送信されます。不明なデバイスからのメッセージは、トラフィック攻撃の原因となる可能性があるため untrusted となります。

DHCP スヌーピング バインディング データベースには、MAC（メディア アクセス制御）アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN（仮想 LAN）番号、スイッチの untrusted インターフェイスに対応したインターフェイス情報が登録されています。ただし、trusted インターフェイスに相互接続されたホストに関する情報は含まれていません。

サービス プロバイダー ネットワーク内において、trusted インターフェイスは同一ネットワーク内のデバイス上のポートに接続されています。untrusted インターフェイスは、ネットワーク内の untrusted インターフェイスまたはネットワーク外のデバイス上のインターフェイスに対して接続されています。

スイッチは untrusted インターフェイス上でパケットを受信した場合、そのインターフェイスが DHCP スヌーピングを有効にした VLAN に属していれば、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはそのパケットを転送します。アドレスが一致しなかった場合、スイッチはそのパケットを廃棄します。

次の状況が発生すると、スイッチは DHCP パケットを廃棄します。

- DHCPPOFFER、DHCPACK、DHCPNAK、または DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットを、ネットワークまたはファイアウォールの外部から受信した場合
- パケットが untrusted インターフェイスで受信され、送信元 MAC アドレスおよび DHCP クライアントハードウェア アドレスが一致しない場合
- DHCP スヌーピング バインディング データベースに MAC アドレスを持つ DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージをスイッチが受信したが、バインディング データベースのインターフェイス情報が、メッセージを受信したインターフェイスのものとは一致しない場合
- DHCP リレー エージェントが、リレーエージェント IP アドレス（0.0.0.0 以外）を含む DHCP パケットを転送する場合。またはリレー エージェントが、Option 82 情報を含むパケットを untrusted ポートへ転送する場合

スイッチが DHCP スヌーピングをサポートする集約スイッチで、DHCP Option 82 情報を挿入するエッジスイッチに接続されている場合、パケットが untrusted インターフェイスで受信されると、スイッチは Option 82 情報を持ったパケットを廃棄します。DHCP スヌーピングがイネーブルでパケットが trusted ポートで受信される場合、集約スイッチは接続されているデバイスの DHCP スヌーピング バインディングを学習しないので、完全な DHCP スヌーピング バインディング データベースを構築できません。

Cisco IOS Release 12.2(25)SEA よりも前のソフトウェア リリースでは、エッジスイッチにより Option 82 情報が挿入された場合、DHCP スヌーピング バインディング データベースが正しく読み込まれないため、集約スイッチ上で DHCP スヌーピングを設定できません。また、スタティック バインディングや Address Resolution Protocol (ARP; アドレス解決プロトコル) Access Control List (ACL; アクセス コントロール リスト) を使用しない場合、スイッチ上で IP ソースガードやダイナミック ARP インスペクションも設定できません。

untrusted インターフェイスを介して集約スイッチをエッジスイッチに接続している場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力することで、集約スイッチは Option 82 情報を持ったパケットをエッジスイッチから受信できます。集約スイッチは untrusted スイッチ インターフェイスを介して接続されたホストのバインディングを学習します。ホストが接続されている信頼できない入力インターフェイスに、Option 82 情報を含むパケットが着信する場合は、集約スイッチ上でダイナミック ARP インスペクションや IP ソース ガードなどの DHCP セキュリティ機能をイネーブルにできます。集約スイッチに接続されているエッジスイッチ上のポートは、trusted インターフェイスとして設定する必要があります。

Option 82 データ挿入

住宅地のメトロポリタンイーサネットアクセス環境では、DHCP を使用して、多数の加入者への IP アドレスの割り当てを集中管理できます。スイッチ上で DHCP Option 82 機能がイネーブルの場合、(MAC アドレスのほかにも) ネットワークに接続されたスイッチポートにより加入するデバイスを識別できます。同じアクセススイッチに接続されている加入者 LAN の複数のホストを、一意に識別できます。

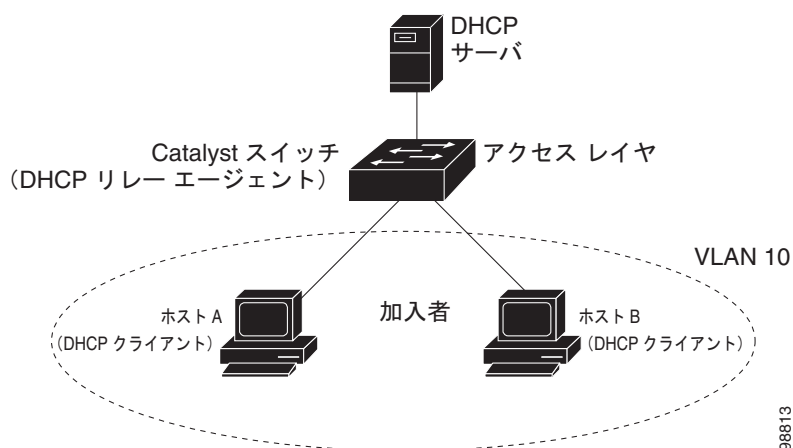


(注)

DHCP Option 82 機能は、DHCP スヌーピングがグローバルおよび VLAN 上でイネーブルで、この機能を使用している加入デバイスが VLAN に割り当てられている場合に限り、サポートされます。

図 23-1 に、アクセスレイヤでスイッチに接続されている加入者に中央集中型 DHCP サーバが IP アドレスを割り当てるメトロポリタンイーサネットネットワークの例を示します。DHCP クライアントと、それに関連付けられた DHCP サーバが、同じ IP ネットワークまたは同じサブネットに属していないため、DHCP リレーエージェント (Catalyst スイッチ) には、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間の DHCP メッセージの転送を行うヘルパーアドレスが設定されています。

図 23-1 メトロポリタンイーサネットネットワークの DHCP リレーエージェント



スイッチの DHCP スヌーピング情報 Option 82 をイネーブルにすると、次の一連のイベントが発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、ネットワークへブロードキャストします。
- スイッチは DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID (`vlan-mod-port`) です。
- リレーエージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケット内に追加します。
- スイッチは、Option 82 フィールドを格納した DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。サーバが Option 82 に対応している場合、リモート ID または回線 ID、あるいはその両方を使用して IP アドレスを割り当て、単一のリモート ID または回線 ID に割り当てる IP アドレス数を制限するなどのポリシーを実行します。その後、DHCP サーバは、DHCP の応答内に Option 82 フィールドをエコーします。

- スイッチにより要求が DHCP サーバにリレーされると、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールド、あるいは回線 ID フィールドを検査して、スイッチ自身が Option 82 データを挿入したことを確認します。スイッチは、Option 82 フィールドを削除し、そのパケットを DHCP 要求の送信元である DHCP クライアントに接続されたスイッチポートに転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、[図 23-2](#) にある次のフィールドの値は変化しません。

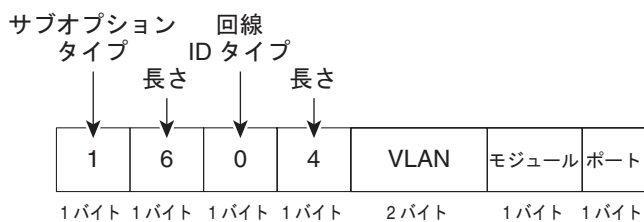
- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

回線 ID サブオプションのポートフィールドでは、ポート番号は 3 から始まります。たとえば、24 の 10/100 ポートおよび Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュールスロットを含むスイッチでは、ポート 3 がファストイーサネット x/0/1 ポート、ポート 4 がファストイーサネット x/0/2 ポートとなり、以降同様に続きます。x はスタック メンバー番号です。ポート 27 は SFP モジュール スロット x/0/1 となり、以降同様に続きます。

[図 23-2](#) に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット フォーマットを示します。回線 ID サブオプションの場合、モジュール番号がスタック内のスイッチ番号に対応します。スイッチは、DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドが入力されると、このパケット フォーマットを使用します。

図 23-2 サブオプションのパケット フォーマット

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット

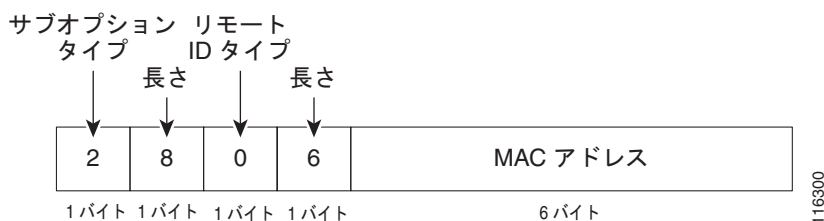


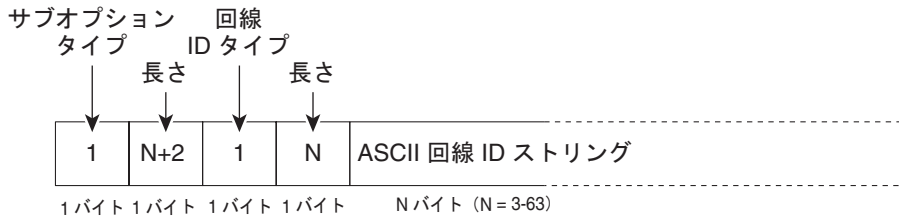
図 23-3 に、ユーザ設定のリモート ID および回線 ID サブオプションのパケット フォーマットを示します。DHCP スヌーピングがグローバルにイネーブルで **ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンドおよび **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドが入力されると、スイッチにより、パケット フォーマットが使用されます。

パケット内にあるこれらのフィールドの値は、リモート ID および 回線 ID サブオプションを設定するとデフォルト値から次のように変化します。

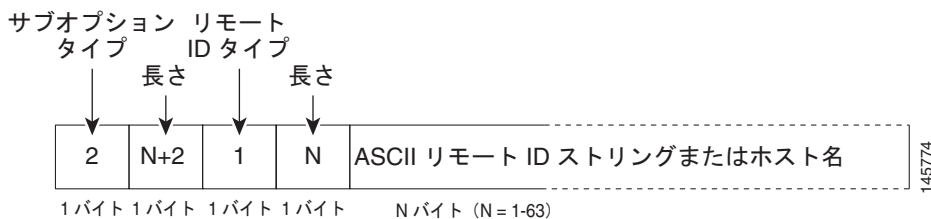
- 回線 ID サブオプション フィールド
 - 回線 ID タイプは 1 です。
 - 長さの値は変数で、設定したストリングの長さによります。
- リモート ID サブオプション フィールド
 - リモート ID タイプは 1 です。
 - 長さの値は変数で、設定したストリングの長さによります。

図 23-3 ユーザ設定サブオプション パケット フォーマット

回線 ID サブオプション フレーム フォーマット (ユーザ設定のストリング) :



リモート ID サブオプション フレーム フォーマット (ユーザ設定のストリング) :



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てることが可能で、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることができます。手動および自動アドレス バインディングの詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「Configuring DHCP」の章を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングがイネーブルの場合、スイッチは DHCP スヌーピング バインディング データベースを使用して信頼できないインターフェイスに関する情報を保存します。データベースには最大で 8192 のバインディングを保存できます。

各データベース エントリ (*binding*) には、IP アドレス、関連 MAC アドレス、およびリース時間 (16 進数表記)、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN があります。データベース エージェントは設定された場所にあるファイルにバインディングを保存します。各エントリの最後にはチェックサムがあり、ファイルの最初からエントリの終わりまでのすべてのバイト数を計上します。各エントリは 72 バイトで、そのあとにスペースとチェックサム値が続きます。

スイッチをリロードしたときにバインディングを維持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスタレーションまたは IP ソース ガードがイネーブルに設定されていて、DHCP スヌーピング バインディング データベースにダイナミック バインディングがある場合、スイッチの接続が切断されます。エージェントがディセーブルで、DHCP スヌーピングだけがイネーブルの場合、スイッチの接続は切断されませんが、DHCP スヌーピングでは DCHP スプーフィング攻撃を防止できないことがあります。

リロードしたとき、スイッチは DHCP スヌーピング バインディング データベースを構築するため、バインディング ファイルを読み込みます。データベースが変更されると、スイッチがファイルを更新します。

スイッチが新しいバインディングを学習したり、バインディングを消失したりした場合には、スイッチはデータベース内のエントリを迅速に更新します。スイッチは、バインディング ファイル内のエントリも更新します。ファイルを更新する頻度は、設定可能な遅延に基づいて更新され、更新はバッチ処理されます。指定された時間 (`write-delay` および `abort-timeout` 値によって設定) でファイルが更新されない場合、更新は中止されます。

バインディングのあるファイルのフォーマットは次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

ファイル内の各エントリはチェックサム値でタグ付けされていて、スイッチはファイルの読み取り時にこの値を使用してエントリを確認します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連したエントリを、前のファイル更新に関連したエントリと区別するものです。

バインディング ファイルの例は次のとおりです。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0
END
```

スイッチが開始されて計算されたチェックサム値が保存されているチェックサム値と等しい場合、スイッチはバインディング ファイルからエントリを読み取ってバインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合にスイッチはエントリを無視します。

- スwitchがエントリを読み取って計算されたチェックサム値が保存されているチェックサム値と異なる場合。エントリとその後続のものが無視されます。
- エントリがリース時間を超過した場合 (リース時間が超過してもスイッチはバインディング エントリを削除しない場合があります)
- エントリ内のインターフェイスがシステムに存在しない場合
- インターフェイスがルーテッド インターフェイスか DHCP スヌーピング信頼インターフェイスの場合

DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、スタック マスターで管理されます。新しいスイッチがスタックに参加すると、スイッチはスタック マスターから DHCP スヌーピング設定を受信します。メンバーがスタックから脱退した場合は、スイッチに関連付けられたすべての DHCP スヌーピング アドレス バインディングが無効になります。

すべてのスヌーピング統計情報は、スタック マスターで生成されます。新しいスタック マスターが選出されると、統計情報カウンタはリセットされます。

スタック マージが発生し、スタック マスターがもはやスタック マスターでなくなると、そのスタック マスター内のすべての DHCP スヌーピング バインディング（スタック マスターは除く）が失われます。スタック 分割により、既存のスタック マスターは変更されませんが、分割されたスイッチに所属するバインディングは、無効になります。分割されたスタックの新しいマスターは、新たに着信する DHCP パケットの処理を開始します。スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

DHCP スヌーピングの設定

ここでは、次の設定情報について説明します。

- 「DHCP スヌーピングのデフォルト設定」(P.23-9)
- 「DHCP スヌーピング設定時の注意事項」(P.23-10)
- 「DHCP リレー エージェントの設定」(P.23-12)
- 「パケット転送アドレスの指定」(P.23-12)
- 「DHCP リレー エージェントの設定」(P.23-12)
- 「パケット転送アドレスの指定」(P.23-12)
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」(P.23-13)
- 「プライベート VLAN での DHCP スヌーピングのイネーブル化」(P.23-15)
- 「Cisco IOS DHCP サーバ データベースのイネーブル化」(P.23-15)
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」(P.23-16)

DHCP スヌーピングのデフォルト設定

表 23-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 23-1 DHCP スヌーピングのデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアでイネーブルです（設定が必要）。 ¹
DHCP リレー エージェント	イネーブル ²
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄されます）。 ²
DHCP リレー エージェントの転送ポリシー	既存のリレー エージェント情報を置き換えます。 ²
DHCP スヌーピングをグローバルでイネーブルにする	ディセーブル

表 23-1 DHCP スヌーピングのデフォルト設定 (続き)

機能	デフォルト設定
DHCP スヌーピング情報オプション	イネーブル
untrusted 入力インターフェイスの packets を受信する DHCP スヌーピング オプション ³	ディセーブル
DHCP スヌーピングの制限レート	未設定
DHCP スヌーピングの信頼性	untrusted
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブルです (設定が必要)。 (注) スイッチは、DHCP サーバとして設定されているデバイスだけから、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブルです (設定が必要)。宛先が設定されている場合に限り、この機能は有効です。

1. スイッチは、DHCP サーバとして設定されている場合に限り、DHCP 要求に応答します。
2. DHCP サーバの IP アドレスが、DHCP クライアントの Switched Virtual Interface (SVI) 上で設定されている場合に限り、スイッチは DHCP パケットをリレーします。
3. スイッチが、エッジスイッチから Option 82 情報を持ったパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

ここでは、DHCP スヌーピングの設定時の注意事項について説明します。

- スイッチの DHCP スヌーピングはグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN 上で DHCP スヌーピングがイネーブルになるまでアクティブになりません。
- DHCP スヌーピングをスイッチ上でグローバルにイネーブルにする前に、DHCP サーバとして動作するデバイスおよび DHCP リレー エージェントが設定されてイネーブルであることを確認してください。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにすると、スヌーピングをディセーブルにするまで Cisco IOS コマンドは使用できません。次のコマンドを入力しても、スイッチからはエラー メッセージが返され、設定は適用されません。
 - **ip dhcp relay information check** グローバル コンフィギュレーション コマンド
 - **ip dhcp relay information policy** グローバル コンフィギュレーション コマンド
 - **ip dhcp relay information trust-all** グローバル コンフィギュレーション コマンド
 - **ip dhcp relay information trusted** インターフェイス コンフィギュレーション コマンド
- DHCP スヌーピング情報オプションをスイッチ上で設定する前に、DHCP サーバとして機能させるデバイスを設定してください。たとえば、DHCP サーバによる割り当てまたは除外の対象にする IP アドレスの指定、およびデバイスの DHCP オプションの設定が必要です。
- スイッチに数多くの回線 ID を設定する際は、NVRAM またはフラッシュ メモリ上の冗長な文字列の影響を考慮してください。他のデータと組み合わせて回線 ID を設定する場合、NVRAM またはフラッシュ メモリの容量を超過すると、エラー メッセージが表示されます。

- スイッチに DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスが設定されていることを確認します。たとえば、DHCP サーバが割り当てたり排除したりすることができる IP アドレスを指定するか、デバイスに DHCP オプションを設定するか、または DHCP データベース エージェントを設定する必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルの場合、DHCP Option 82 データ挿入機能はサポートされません。
- スイッチのポートが DHCP サーバに接続されている場合、**ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを **trusted** として設定してください。
- スイッチのポートが DHCP クライアントに接続されている場合、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを **untrusted** として設定してください。
- DHCP スヌーピング バインディング データベースを設定する場合に次の注意事項に従ってください。
 - NVRAM (不揮発性 RAM) およびフラッシュ メモリのストレージ容量に制限があるので、バインディング ファイルは Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバに保存することを推奨します。
 - ネットワーク ベース URL (TFTP や FTP (ファイル転送プロトコル) など) の場合、スイッチが設定した URL のバインディング ファイルにバインディングを書き込む前に、その URL で空のファイルを作成しておく必要があります。先にサーバで空のファイルを作成する必要があるかどうかを判断するには、TFTP サーバのマニュアルを参照してください。一部の TFTP サーバはこの方法では設定することができません。
 - データベースのリース時間を正確にするには、Network Time Protocol (NTP) をイネーブルにして設定することを推奨します。詳細については、「[NTP の設定](#)」(P.7-4) を参照してください。
 - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期している場合に限り、スイッチはバインディング変更をバインディング ファイルに書き込みます。
- **untrusted** デバイスが接続されている集約スイッチに **ip dhcp snooping information option allow-untrusted** コマンドを入力しないでください。このコマンドを入力すると、**untrusted** デバイスは Option 82 情報をスプーフィングします。
- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力すると DHCP スヌーピングの統計情報を表示でき、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力するとスヌーピング統計情報カウンタをクリアできます。



(注) RSPAN VLAN 上で DHCP スヌーピングをイネーブルにしないでください。RSPAN VLAN 上で DHCP スヌーピングをイネーブルにすると、DHCP パケットが RSPAN 宛先ポートに到達しないことがあります。

DHCP リレー エージェントの設定

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>service dhcp</code>	スイッチ上で DHCP サーバおよびリレー エージェントをイネーブルにします。デフォルトで、この機能はイネーブルに設定されています。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP サーバとリレー エージェントをディセーブルにするには、`no service dhcp` グローバル コンフィギュレーション コマンドを使用します。

これらの手順については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Addressing and Services」セクションにある「Configuring DHCP」セクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

- リレー エージェント情報の確認 (検証)
- リレー エージェントの転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを `ip helper-address address` インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的な規則は、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。`ip helper-address` コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワーク セグメントにある場合はネットワーク アドレスにできます。ネットワーク アドレスを使用することでどの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface vlan vlan-id</code>	VLAN ID を入力してスイッチの仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip address ip-address subnet-mask</code>	インターフェイスに IP アドレスおよび IP サブネットを設定します。

	コマンド	目的
ステップ 4	<code>ip helper-address address</code>	DHCP パケット転送アドレスを指定します。 ヘルパー アドレスは特定の DHCP サーバアドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにできます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>interface range port-range</code> または <code>interface interface-id</code>	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス レンジ コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<code>switchport mode access</code>	ポートの VLAN メンバシップ モードを定義します。
ステップ 8	<code>switchport access vlan vlan-id</code>	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show running-config</code>	設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP パケット転送アドレスを削除するには、`no ip helper-address address` インターフェイス コンフィギュレーション コマンドを使用します。

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dhcp snooping</code>	DHCP スヌーピングをグローバルでイネーブルにします。
ステップ 3	<code>ip dhcp snooping vlan vlan-range</code>	VLAN または VLAN 範囲で DHCP スヌーピングをイネーブルにします。指定できる範囲は 1 ~ 4094 です。 VLAN ID には、VLAN ID 番号で識別される 1 つの VLAN ID、カンマで区切られた一連の VLAN ID、ハイフンで区切られた VLAN ID の範囲、開始 VLAN ID と終了 VLAN ID をスペースで区切った VLAN ID の範囲を入力できます。

	コマンド	目的
ステップ 4	<code>ip dhcp snooping information option</code>	スイッチで、DHCP サーバ宛に転送される要求メッセージ内の DHCP リレー情報 (Option 82 フィールド) の挿入および削除をイネーブルにします。これがデフォルトの設定です。
ステップ 5	<code>ip dhcp snooping information option format remote-id [string ASCII-string hostname]</code>	(任意) リモート ID サブオプションを設定します。 次のようにリモート ID を設定できます。 <ul style="list-style-type: none"> 63 文字までの ASCII 文字列 (スペースなし) スイッチに設定されたホスト名 (注) ホスト名が 64 文字以上の場合、リモート ID 設定で 63 文字に切り捨てられます。 デフォルトのリモート ID はスイッチ MAC アドレスです。
ステップ 6	<code>ip dhcp snooping information option allow-untrusted</code>	(任意) スイッチがエッジスイッチに接続された集約スイッチである場合、エッジスイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを受信できるようスイッチをイネーブルにします。 デフォルトではディセーブルに設定されています。 (注) このコマンドは trusted デバイスに接続された集約スイッチ上でだけ入力してください。
ステップ 7	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	<code>ip dhcp snooping vlan vlan information option format-type circuit-id [override] string ASCII-string</code>	(任意) 指定したインターフェイスで回線 ID サブオプションを設定します。 1 ~ 4094 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID はポート ID で、フォーマットは vlan-mod-port です。 回線 ID を 3 ~ 63 の ASCII 文字 (スペースなし) を設定できます。 (任意) 登録情報を定義する TLV フォーマットに回線 ID サブオプションを挿入しない場合は override キーワードを使用します。
ステップ 9	<code>ip dhcp snooping trust</code>	(任意) インターフェイスを trusted または untrusted のいずれかに設定します。untrusted クライアントからのメッセージをインターフェイスが受信できるようにするには、 no キーワードを使用します。デフォルトでは untrusted に設定されています。
ステップ 10	<code>ip dhcp snooping limit rate rate</code>	(任意) インターフェイスが受信できる DHCP パケット数/秒の上限を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトでは無制限に設定されています。 (注) untrusted レート制限は、100 パケット/秒以下にすることを推奨します。trusted インターフェイスにレート制限を設定する場合、ポートが複数の DHCP スヌーピングを行う VLAN に割り当てられているトランク ポートであれば、レート制限を増やさなければなりません。
ステップ 11	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	<code>ip dhcp snooping verify mac-address</code>	(任意) untrusted ポート上で受信した DHCP パケットにある送信元 MAC アドレスが、パケット内のクライアントのハードウェアアドレスと一致するかどうかを確認するように、スイッチを設定します。デフォルトでは、パケット内の送信元 MAC アドレスとクライアントのハードウェアアドレスの一致を確認するように設定されています。

	コマンド	目的
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show running-config</code>	設定を確認します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピングをディセーブルにするには、`no ip dhcp snooping` グローバル コンフィギュレーション コマンドを使用します。VLAN または VLAN 範囲で DHCP スヌーピングをディセーブルにするには、`no ip dhcp snooping vlan vlan-range` グローバル コンフィギュレーション コマンドを使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、`no ip dhcp snooping information option` グローバル コンフィギュレーション コマンドを使用します。エッジ スイッチからの Option 82 情報を持った着信 DHCP スヌーピング パケットを廃棄するよう集約スイッチを設定するには、`no ip dhcp snooping information option allow-untrusted` グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 10 上で DHCP スヌーピングをグローバルでイネーブルにし、ポート上でレート制限を 100 パケット/秒に設定する例を示します。

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```

プライベート VLAN での DHCP スヌーピングのイネーブル化

プライベート VLAN で DHCP スヌーピングをイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN および関連付けられているセカンダリ VLAN の両方に伝播します。DHCP スヌーピングがプライマリ VLAN でイネーブルの場合、セカンダリ VLAN でもイネーブルに設定されています。

DHCP スヌーピングがすでにプライマリ VLAN に設定されていて DHCP スヌーピングをセカンダリ VLAN とは異なるように設定した場合、セカンダリ VLAN の設定は有効になりません。プライマリ VLAN に DHCP スヌーピングを設定する必要があります。プライマリ VLAN に DHCP スヌーピングが設定されていない場合は、VLAN 200 などのセカンダリ VLAN に DHCP スヌーピングを設定するときに、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take effect on secondary vlan 200.DHCP Snooping configuration on secondary vlan is derived from its primary vlan.
```

`show ip dhcp snooping` 特権 EXEC コマンド出力では、DHCP スヌーピングがイネーブルであるプライマリおよびセカンダリ プライベート VLAN を含む、すべての VLAN を表示します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順の詳細については、『*Cisco IOS IP Configuration Guide*』 Release 12.2 の「Configuring DHCP」の章にある「DHCP Configuration Task List」セクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dhcp snooping database {flash[number]:filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}{/directory} /image-name.tar rcp://user@host/filename} tftp://host/filename</code>	次の形式のいずれかを使用して、データベース エージェントまたはバインディング ファイル用の URL を指定します。 <ul style="list-style-type: none"> <code>flash[number]:filename</code> (任意) スタック マスターのスタック メンバー番号を指定するには、<code>number</code> パラメータを使用します。<code>number</code> の指定できる範囲は 1 ~ 9 です。 <code>ftp://user:password@host/filename</code> <code>http://[[username:password]@]{hostname host-ip}{/directory}/image-name.tar</code> <code>rcp://user@host/filename</code> <code>tftp://host/filename</code>
ステップ 3	<code>ip dhcp snooping database timeout seconds</code>	データベース転送処理を停止するまでに待機する時間 (秒) を指定します。 デフォルト値は 300 秒です。指定できる範囲は 0 ~ 86400 です。時間を無制限に定義するには 0 を使用します。これは、転送の試行を無制限に継続することを意味します。
ステップ 4	<code>ip dhcp snooping database write-delay seconds</code>	バインディング データベースが変更されたあとの伝送が遅延する期間を指定します。指定できる範囲は 15 ~ 86400 秒です。デフォルトは 300 秒 (5 分) です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</code>	(任意) DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。 <code>vlan-id</code> の範囲は 1 ~ 4904 です。 <code>seconds</code> の範囲は 1 ~ 4294967295 秒です。 追加する各エントリにこのコマンドを入力します。 (注) スイッチのテストやデバッグを行うとき、このコマンドを使用します。
ステップ 7	<code>show ip dhcp snooping database [detail]</code>	DHCP スヌーピング バインディング データベース エージェントのステータスと統計情報を表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を止めるには、`no ip dhcp snooping database` グローバル コンフィギュレーション コマンドを使用します。タイムアウト値または遅延値をリセットするには、`ip dhcp snooping database timeout seconds` または `ip dhcp snooping database write-delay seconds` グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報を消去するには、**clear ip dhcp snooping database statistics** 特権 EXEC コマンドを使用します。データベースを更新するには、**renew ip dhcp snooping database** 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからエントリを削除するには、**no ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id** 特権 EXEC コマンドを使用します。削除する各エントリにこのコマンドを入力します。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 23-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-2 DHCP 情報を表示するためのコマンド

コマンド	目的
show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース (バインディング テーブル) で動的に設定されたバインディングだけを表示します。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示します。
show ip source binding	ダイナミックおよびスタティックに設定されたバインディングを表示します。



(注)

DHCP スヌーピングがイネーブルで、インターフェイスがダウン ステートに変わった場合、スイッチは静的に設定されたバインディングを削除しません。

IP ソース ガードの概要

IPSG は、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングすることで、実現しています。IP ソース ガードを使用することで、ホストがネイバーの IP アドレスを使用しようとする場合のトラフィック攻撃を回避できます。

DHCP スヌーピングが信頼できないインターフェイスでイネーブルの場合に IP ソース ガードをイネーブルにできます。IPSG がインターフェイスでイネーブルになったあと、スイッチは、DHCP スヌーピングで許可された DHCP パケットを除く、インターフェイスで受信されたすべての IP トラフィックをブロックします。ポート Access Control List (ACL) はインターフェイスに適用されます。ポート ACL により、IP 送信元バインディング テーブル内の送信元 IP アドレスの IP トラフィックだけを許可し、他のトラフィックを拒否できます。



(注)

ポート ACL は、同じインターフェイスに影響するルータ ACL や VLAN マップに優先します。

IP ソース バインディング テーブルのバインディングは、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）です。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルの場合に限り IP 送信元バインディング テーブルを使用しません。

IPSG は、アクセス ポートやトランク ポートなどのレイヤ 2 ポートに限りサポートされます。IPSG を、送信元 IP アドレス フィルタリングや送信元 IP および MAC アドレス フィルタリングとともに設定できます。

- 「送信元 IP アドレス フィルタリング」(P.23-18)
- 「送信元 IP および MAC アドレス フィルタリング」(P.23-18)
- 「スタティック ホストの IP ソース ガード」(P.23-18)

送信元 IP アドレス フィルタリング

IPSG がこのオプションでイネーブルの場合、IP トラフィックは送信元 IP アドレスに基づいてフィルタリングされます。送信 IP アドレスが DHCP スヌーピング バインディング データベースのエントリまたは IP 送信元バインディング テーブル内のバインディングと一致した場合、スイッチは IP トラフィックを転送します。

DHCP スヌーピング バインディングまたはスタティック IP 送信元バインディングがインターフェイスで追加、変更、削除された場合、スイッチは IP 送信元バインディングを変更してポート ACL を修正し、ポート ACL をインターフェイスに適用します。

(DHCP スヌーピングで動的に学習されたか手動で設定された) IP 送信元バインディングが設定されていないインターフェイスで IPSG をイネーブルにする場合、スイッチはインターフェイス上のすべての IP トラフィックを拒否するポート ACL を作成し、適用します。IP ソース ガードをディセーブルにする場合、スイッチはポート ACL をインターフェイスから削除します。

送信元 IP および MAC アドレス フィルタリング

IP トラフィックは送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。スイッチは、送信元 IP アドレスおよび MAC アドレスが IP 送信元バインディング テーブルのエントリと一致する場合にトラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP トラフィックおよび非 IP トラフィックをフィルタリングします。IP または非 IP パケットの送信元 MAC アドレスが有効な IP 送信元バインディングと一致する場合、スイッチはパケットを転送します。スイッチは、DHCP パケットを除く他のすべてのタイプのパケットを廃棄します。

スイッチは、ポート セキュリティを使用して送信元 MAC アドレスをフィルタリングします。ポート セキュリティ違反が発生する際にインターフェイスをシャットダウンできます。

スタティック ホストの IP ソース ガード



(注)

アップリンク ポートまたはトランク ポートに、スタティック ホストの IPSG (IP ソース ガード) を使用しないでください。

スタティック ホストの IPSG は、IPSG の機能を非 DHCP 環境およびスタティック環境に拡張します。以前の IPSG は、スイッチに接続されたホストの検証に DHCP スヌーピングによって作成されたエントリーを使用しました。有効な DHCP バインディング エントリーのないホストから受信したトラフィックは破棄されます。このセキュリティ機能は、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックを制限します。DHCP スヌーピング バインディング データベースと手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。IPSG の以前のバージョンでは、IPSG が機能するために DHCP 環境が必要でした。

スタティック ホストの IPSG によって DHCP がいない場合も IPSG は機能します。スタティック ホストの IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリーを利用します。スイッチは、ARP 要求またはその他の IP パケットに基づいてスタティックなエントリーを作成し、所定のポートに有効なホストの一覧を維持します。所定のポートへのトラフィック送信が許可されるホストの数も指定できます。これは、レイヤ 3 ポート セキュリティと等価です。

スタティック ホストの IPSG は、ダイナミック ホストもサポートします。ダイナミック ホストが IP DHCP スヌーピング テーブルで入手できる DHCP 割り当て IP アドレスを受信した場合、同じエントリーが IP デバイス トラッキング テーブルによって学習されます。スタック環境では、マスター フェールオーバーが発生すると、メンバー ポートに対応付けられたスタティック ホストの IP ソース ガード エントリーが維持されます。show ip device tracking all EXEC コマンドを入力すると、IP デバイス トラッキング テーブルが、ACTIVE としてエントリーを表示します。



(注) 複数のネットワーク インターフェイスのある一部の IP ホストでは、無効なパケットをネットワーク インターフェイスに注入することもできます。無効なパケットは、ホストの別のネットワーク インターフェイスの IP アドレスまたは MAC アドレスを発信元アドレスとして含まれます。無効なパケットが原因になって、スタティック ホストの IPSG がそのホストに接続し、不正な IP または MAC アドレス バインディングを学習し、有効なバインディングを拒否することがあります。ホストによる無効なパケットの挿入を防止するには、対応するオペレーティング システムおよびネットワーク インターフェイスのベンダーにご相談ください。

スタティック ホストの IPSG は、最初に ACL ベースのスヌーピング メカニズムによって IP または MAC バインディングを動的に学習します。IP または MAC バインディングは、ARP および IP パケットによってスタティック ホストから学習されます。それらは、デバイス トラッキング データベースに保存されます。動的に学習された、または所定のポートに静的に設定された IP アドレスの数が最大値に達したとき、ハードウェアは新しい IP アドレスのあるパケットを破棄します。何らかの理由で移動または削除されたホストを解決するため、スタティック ホストは IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングを無効にします。この機能は、DHCP スヌーピングと共に使用できます。DHCP とスタティック ホストの両方に接続されたポート上に複数のバインディングが確立されます。たとえば、バインディングは DHCP スヌーピング バインディング データベースに加えて、両方のデバイスのトラッキング データベースに保存されます。

IP ソース ガードの設定

- 「デフォルトの IP ソース ガードの設定」 (P.23-20)
- 「IP ソース ガード設定時の注意事項」 (P.23-20)
- 「IP ソース ガードのイネーブル化」 (P.23-21)
- 「スタティック ホストの IP ソース ガードの設定」 (P.23-22)

デフォルトの IP ソース ガードの設定

デフォルトでは、IP ソース ガードはディセーブルに設定されています。

IP ソース ガード設定時の注意事項

- 非ルーテッド ポートに限りスタティック IP バインディングを設定できます。 **ip source binding mac-address vlan vlan-id ip-address interface interface-id** グローバル コンフィギュレーション コマンドをルーテッド インターフェイスに入力した場合、このエラー メッセージが表示されます。

Static IP source binding can only be configured on switch port.

- IP ソース ガードと送信元 IP フィルタリングがインターフェイスでイネーブルの場合、DHCP スヌーピングは、インターフェイスのアクセス VLAN でイネーブルでなければなりません。
- 複数の VLAN があるトランク インターフェイスで IP ソース ガードがイネーブルで、DHCP スヌーピングがすべての VLAN でイネーブルの場合、送信元 IP アドレス フィルタがすべての VLAN に適用されます。



(注) IP ソース ガードがイネーブルでトランク インターフェイス上の VLAN で DHCP スヌーピングがディセーブルの場合、スイッチは適切にトラフィックをフィルタリングできません。

- IP ソース ガードと送信元 IP および MAC アドレス フィルタリングがイネーブルの場合、DHCP スヌーピングおよびポート セキュリティがインターフェイスでイネーブルでなければなりません。また、 **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力し、DHCP サーバが Option 82 をサポートするように設定する必要があります。IP ソース ガードと MAC アドレス フィルタリングがイネーブルの場合、DHCP ホストの MAC アドレスはホストにリースが与えられるまで学習されません。パケットがサーバからホストに転送される場合、DHCP スヌーピングでは Option 82 のデータを使用してホスト ポートを識別します。
- プライベート VLAN が設定されているインターフェイスで IP ソース ガードを設定する場合、ポートセキュリティはサポートされません。
- IP ソース ガードは EtherChannel でサポートされません。
- 802.1X ポートベース認証がイネーブルである場合、IP ソース ガードの機能をイネーブルにできません。
- Ternary Content Addressable Memory (TCAM) エントリ数が最大数を超えた場合、CPU の使用量が増加します。
- スイッチ スタックでは、IP ソース ガードがスタック メンバー インターフェイスに設定されていて、 **no switch stack-member-number provision** グローバル コンフィギュレーション コマンドを入力してこのスイッチ設定を削除する場合、インターフェイス スタティック バインディングがバインディング テーブルから削除されます。実行コンフィギュレーションからは削除されません。 **switch stack-member-number provision** コマンドを入力してスイッチを再びプロビジョニングする場合、バインディングが元に戻されます。バインディングを実行コンフィギュレーションから削除するには、 **no switch provision** グローバル コンフィギュレーション コマンドを入力する前に IP ソース ガードを無効にしなければいけません。インターフェイスがバインディング テーブルから削除されている間にスイッチをリロードする場合、コンフィギュレーションも削除されます。プロビジョニングされたスイッチの詳細については、「[スタックのオフライン設定](#)」(P.5-7) を参照してください。

IP ソース ガードのイネーブル化

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip verify source または ip verify source port-security	IP ソース ガードと送信元 IP アドレス フィルタリングをイネーブルにします。 IP ソース ガードと送信元 IP および MAC アドレス フィルタリングをイネーブルにします。 (注) ip verify source port-security インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の 2 つの注意事項があります。 <ul style="list-style-type: none"> • DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 • DHCP パケットの MAC アドレスは、セキュアアドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュアアドレスとして学習されます。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ip source binding mac-address vlan vlan-id ip-address interface interface-id	スタティック IP 送信元バインディングを追加します。 各スタティック バインディングに対してこのコマンドを入力します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip verify source [interface interface-id]	IP ソース ガードの設定を確認します。
ステップ 8	show ip source binding [ip-address] [mac-address] [dhcp-snooping static] [interface interface-id] [vlan vlan-id]	スイッチ、特定の VLAN、または特定のインターフェイス上の IP 送信元バインディングを表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP ソース ガードおよび送信元 IP アドレス フィルタリングをディセーブルにするには、**no ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP 送信元バインディング エントリを削除するには、**no ip source** グローバル コンフィギュレーション コマンドを使用します。

次に、IP ソース ガードと送信元 IP および MAC フィルタリングを VLAN 10 および VLAN 11 でイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
```

```
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Switch(config)# end
```

スタティック ホストの IP ソース ガードの設定

- 「レイヤ 2 アクセス ポートでのスタティック ホストの IP ソース ガードの設定」(P.23-22)
- 「プライベート VLAN ホスト ポートでのスタティック ホストの IP ソース ガードの設定」(P.23-25)

レイヤ 2 アクセス ポートでのスタティック ホストの IP ソース ガードの設定



(注)

スタティック ホストの IPSG を機能させるには、**ip device tracking maximum limit-number** インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。ポート上で IP デバイス トラッキングをグローバルにイネーブルに設定することなくこのコマンドだけを設定すると (つまり、該当するインターフェイス上で IP デバイス トラッキング最大数を設定することによって)、スタティック ホストの IPSG は、該当するインターフェイスからのすべての IP トラフィックを拒否します。この要件は、プライベート VLAN ホスト ポート上のスタティック ホストの IPSG にも適用されます。

特権 EXEC モードで実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip device tracking	IP ホスト テーブルをオンにして、IP デバイス トラッキングをグローバルにイネーブルにします。
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switchport mode access	ポートをアクセスとして設定します。
ステップ 5	switchport access vlan vlan-id	このポートの VLAN を設定します。
ステップ 6	ip verify source tracking port-security	スタティック ホストの IPSG と MAC アドレス フィルタリングをイネーブルにします。 (注) ip verify source port-security インターフェイス コンフィギュレーション コマンドを使用して IP ソース ガードとポート セキュリティの両方をイネーブルにする場合は、次の注意事項があります。 <ul style="list-style-type: none"> DHCP サーバで Option 82 をサポートしていないと、クライアントには IP アドレスが割り当てられません。 DHCP パケットの MAC アドレスは、セキュアアドレスとして学習されません。スイッチが DHCP 以外のデータ トラフィックを受信した場合にだけ、DHCP クライアントの MAC アドレスはセキュアアドレスとして学習されます。

	コマンド	目的
ステップ 7	<code>ip device tracking maximum number</code>	IP デバイス トラッキング テーブルがポート上で許可するスタティック IP の数の最大限度を設定します。指定できる範囲は 1 ~ 10 です。最大数は 10 です。 (注) <code>ip device tracking maximum limit-number</code> インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	<code>switchport port-security</code>	(任意) このポートのポートセキュリティをアクティブにします。
ステップ 9	<code>switchport port-security maximum value</code>	(任意) このポートの MAC アドレスの最大値を設定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show ip verify source interface interface-id</code>	設定を確認し、スタティック ホストの IPSG 許可 ACL を表示します。
ステップ 12	<code>show ip device track all [active inactive] count</code>	スイッチ インターフェイスの所定のホストのための IP と MAC のバインディングを表示することで設定を確認します。 <ul style="list-style-type: none"> • all active : アクティブな IP または MAC バインディング エントリだけを表示します。 • all inactive : 非アクティブな IP または MAC バインディング エントリだけを表示します。 • all : アクティブまたは非アクティブの IP または MAC バインディング エントリを表示します。

次に、インターフェイス上のスタティック ホストの IPSG を停止する方法を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、ポート上のスタティック ホストの IPSG をイネーブルにする方法を示します。

```
Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security
```

次に、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG および IP フィルタリングをイネーブルにする方法、および、インターフェイス Gi0/3 の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----  -
Gi0/3     ip trk       active       40.1.1.24       -----
Gi0/3     ip trk       active       40.1.1.20       -----
Gi0/3     ip trk       active       40.1.1.21       -----
```

次に、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG および IP-MAC フィルタリングをイネーブルにする方法、および、インターフェイス Gi0/3 の有効な IP-MAC バインディングを確認し、最大値に到達したインターフェイス上のバインディングの数を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----  -
Gi0/3     ip-mac trk   active      40.1.1.24      00:00:00:00:03:04  1
Gi0/3     ip-mac trk   active      40.1.1.20      00:00:00:00:03:05  1
Gi0/3     ip-mac trk   active      40.1.1.21      00:00:00:00:03:06  1
Gi0/3     ip-mac trk   active      40.1.1.22      00:00:00:00:03:07  1
Gi0/3     ip-mac trk   active      40.1.1.23      00:00:00:00:03:08  1
```

次に、すべてのインターフェイスに対するすべての IP または MAC バインディング エントリを表示する例を示します。CLI はすべてのアクティブなエントリおよび非アクティブなエントリを表示します。インターフェイスでホストが学習された場合、新しいエントリはアクティブとしてマークされます。同じホストがそのインターフェイスから接続解除され別のインターフェイスに接続される場合、新しい IP または MAC バインディング エントリは、ホストが検出されるとすぐにアクティブとして表示されます。以前のインターフェイス上のこのホストの古いエントリ非アクティブとしてマークされます。

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----
   IP Address      MAC Address      Vlan  Interface      STATE
-----
200.1.1.8         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.9         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.10        0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.1         0001.0600.0000  9     GigabitEthernet0/2  ACTIVE
200.1.1.1         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.2         0001.0600.0000  9     GigabitEthernet0/2  ACTIVE
200.1.1.2         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.3         0001.0600.0000  9     GigabitEthernet0/2  ACTIVE
200.1.1.3         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.4         0001.0600.0000  9     GigabitEthernet0/2  ACTIVE
200.1.1.4         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.5         0001.0600.0000  9     GigabitEthernet0/2  ACTIVE
200.1.1.5         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.6         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
200.1.1.7         0001.0600.0000  8     GigabitEthernet0/1  INACTIVE
```

次に、すべてのインターフェイスに対するすべてのアクティブな IP または MAC バインディング エントリを表示する例を示します。

```
Switch# show ip device tracking all active
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.1	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE

次に、すべてのインターフェイスに対するすべての非アクティブな IP または MAC バインディング エントリを表示する例を示します。ホストは GigabitEthernet 0/1 上で最初に学習され、次に GigabitEthernet 0/2 に移動されました。GigabitEthernet 0/1 上で学習された IP または MAC バインディング エントリは非アクティブとしてマークされます。

```
Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.10	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.1	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE

次に、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの数を表示する例を示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
```

Interface	Maximum Limit	Number of Entries
Gi0/3	5	

プライベート VLAN ホスト ポートでのスタティック ホストの IP ソース ガードの設定



(注)

スタティック ホストの IPSG を機能させるには、`ip device tracking maximum limit-number` インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。ポート上で IP デバイス トラッキングをグローバルにイネーブルに設定することなくこのコマンドだけを設定すると (つまり、該当するインターフェイス上で IP デバイス トラッキング最大数を設定することによって)、スタティック ホストの IPSG は、該当するインターフェイスからのすべての IP トラフィックを拒否します。この要件は、レイヤ 2 アクセス ポート上のスタティック ホストの IPSG にも適用されます。

レイヤ 2 アクセス ポート上でスタティック ホストの IPSG と IP フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

■ IP ソース ガードの設定

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan <i>vlan-id1</i></code>	VLAN コンフィギュレーション モードを開始します。
ステップ 3	<code>private-vlan primary</code>	プライベート VLAN ポートにプライマリ VLAN を設定します。
ステップ 4	<code>exit</code>	VLAN コンフィギュレーション モードを終了します。
ステップ 5	<code>vlan <i>vlan-id2</i></code>	別の VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 6	<code>private-vlan isolated</code>	プライベート VLAN ポートに独立 VLAN を設定します。
ステップ 7	<code>exit</code>	VLAN コンフィギュレーション モードを終了します。
ステップ 8	<code>vlan <i>vlan-id1</i></code>	コンフィギュレーション VLNA モードを開始します。
ステップ 9	<code>private-vlan association 201</code>	独立プライベート VLAN ポートの VLAN を関連付けます。
ステップ 10	<code>exit</code>	VLAN コンフィギュレーション モードを終了します。
ステップ 11	<code>interface fastEthernet <i>interface-id</i></code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	<code>switchport mode private-vlan host</code>	(任意) ポートをプライベート VLAN ホストとして設定します。
ステップ 13	<code>switchport private-vlan host-association <i>vlan-id1</i> <i>vlan-id2</i></code>	(任意) このポートを対応するプライベート VLAN と関連付けます。
ステップ 14	<code>ip device tracking maximum <i>number</i></code>	IP デバイストラッキング テーブルがポート上で許可するスタティック IP の数の最大値を設定します。 最大値は 10 です。  (注) スタティック ホストの IPSG を機能させるには、 <code>ip device tracking maximum number</code> インターフェイス コマンドをグローバルに設定する必要があります。
ステップ 15	<code>ip verify source tracking [port-security]</code>	このポートのスタティック ホストの IPSG および MAC アドレス フィルタリングをアクティブにします。
ステップ 16	<code>end</code>	コンフィギュレーション インターフェイス モードを終了します。
ステップ 17	<code>show ip device tracking all</code>	設定を確認します。
ステップ 18	<code>show ip verify source interface <i>interface-id</i></code>	IP ソース ガードの設定を確認します。スタティック ホストの IPSG 許可 ACL を表示します。

次に、スタティック ホストの IPSG と IP フィルタリングをプライベート VLAN ホスト ポートでイネーブルにする方法を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
```



```
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking
```

```
Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
40.1.1.24	0000.0000.0304	200	FastEthernet0/3	ACTIVE
40.1.1.20	0000.0000.0305	200	FastEthernet0/3	ACTIVE
40.1.1.21	0000.0000.0306	200	FastEthernet0/3	ACTIVE
40.1.1.22	0000.0000.0307	200	FastEthernet0/3	ACTIVE
40.1.1.23	0000.0000.0308	200	FastEthernet0/3	ACTIVE

出力は、インターフェイス Fa0/3 で学習された 5 つの有効な IP MAC バインディングを示しています。プライベート VLAN の場合、バインディングはプライマリ VLAN ID と対応付けられています。したがって、この例では、プライマリ VLAN ID、200 が表に示されています。

```
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----  -
Fa0/3     ip trk       active      40.1.1.23  200
Fa0/3     ip trk       active      40.1.1.24  200
Fa0/3     ip trk       active      40.1.1.20  200
Fa0/3     ip trk       active      40.1.1.21  200
Fa0/3     ip trk       active      40.1.1.22  200
Fa0/3     ip trk       active      40.1.1.23  201
Fa0/3     ip trk       active      40.1.1.24  201
Fa0/3     ip trk       active      40.1.1.20  201
Fa0/3     ip trk       active      40.1.1.21  201
Fa0/30/3  ip trk       active      40.1.1.22  201
```

出力は、プライマリ VLAN とセカンダリ VLAN の両方に存在する 5 つの有効な IP MAC バインディングを示しています。

IP ソース ガード情報の表示

IP ソース ガード情報を表示するには、表 23-3 に示す、1 つまたは複数の特権 EXEC コマンドを使用します。

表 23-3 IP ソース ガード情報の表示用コマンド

コマンド	目的
show ip device tracking	すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチの IP 送信元バインディングを表示します。
show ip verify source	スイッチの IP ソース ガード設定を表示します。

DHCP サーバのポートベースのアドレス割り当ての概要

DHCP サーバのポートベースのアドレス割り当ては、接続しているデバイス クライアント ID またはクライアント ハードウェアのアドレスにかかわらず、DHCP が 1 つのイーサネット スイッチ ポート上で同じ IP アドレスを保持できるようにする機能です。

イーサネット スイッチがネットワークに配置されている場合は、直接接続しているデバイスに接続できます。工場の床などの環境によっては、デバイスが故障したときに、代替のデバイスを既存のネットワークで即時に動作させる必要があります。現在の DHCP 実装では、DHCP が代替のデバイスに同じ IP アドレスを提供することは保証されていません。制御ソフトウェア、モニタリング ソフトウェアなどのソフトウェアは、スタティック IP アドレスが各デバイスに関連していることを前提としています。デバイスを交換する場合は、DHCP クライアントが変更されてもアドレス割り当ては固定のままとなる必要があります。

DHCP サーバのポートベースのアドレス割り当て機能を設定すると、ポートに到着する DHCP メッセージのクライアント ID またはクライアント ハードウェアのアドレスが変わっても、同じ IP アドレスが同じ接続ポートに常に提供されるようになります。DHCP プロトコルは DHCP パケットのクライアント ID オプションによって DHCP クライアントを認識します。クライアント ID オプションを持たないクライアントは、クライアント ハードウェアのアドレスによって特定されます。この機能を設定すると、インターフェイスのポート名によってクライアント ID またはハードウェア アドレスは無効になり、実際の接続ポイント、スイッチ ポートがクライアント ID となります。

どのような場合であっても、同じポートにイーサネット ケーブルを接続することで、DHCP によって同じ IP アドレスが接続しているデバイスに割り当てられます。

DHCP サーバのポートベースのアドレス割り当て機能は、Cisco IOS DHCP サーバに限りサポートされ、サードパーティ製のサーバではサポートされません。

DHCP サーバのポートベースのアドレス割り当ての設定

ここでは、次の設定情報について説明します。

- 「ポートベースのアドレス割り当てのデフォルト設定」 (P.23-28)
- 「ポートベースのアドレス割り当ての設定時の注意事項」 (P.23-28)
- 「DHCP サーバのポートベースのアドレス割り当てのイネーブル化」 (P.23-29)

ポートベースのアドレス割り当てのデフォルト設定

デフォルトで、DHCP サーバのポートベースのアドレス割り当てはディセーブルです。

ポートベースのアドレス割り当ての設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当ての設定時の注意事項について説明します。

- ポートごとに、1 つの IP アドレスだけを割り当てることができます。
- 予約された (事前に割り当てられた) アドレスは、**clear ip dhcp binding** グローバル コンフィギュレーション コマンドを使用してもクリアできません。
- 事前に割り当てられたアドレスは、通常のダイナミック IP アドレス割り当てから自動的に除外されます。事前に割り当てられたアドレスはホスト プールで使用できませんが、DHCP アドレス プールごとに複数のアドレスを事前に割り当てることができます。

- DHCP プールから予約済みのアドレスへの割り当てを制限するには（予約済みでないアドレスはクライアントには提供されず、その他のクライアントはプールから供給されません）、**reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。

DHCP サーバのポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルでイネーブルにし、インターフェイスで加入者 ID を自動的に生成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dhcp use subscriber-id client-id	すべての着信 DHCP メッセージにおいて、加入者 ID をクライアント ID としてグローバルで使用するよう DHCP サーバを設定します。
ステップ 3	ip dhcp subscriber-id interface-name	インターフェイスの略称に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドより優先されます。
ステップ 4	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	ip dhcp server use subscriber-id client-id	インターフェイス上のすべての着信 DHCP メッセージにおいて、加入者 ID をクライアント ID として使用するよう DHCP サーバを設定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP ポートベースのアドレス割り当てをスイッチでイネーブルにしてから、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスを事前に割り当てて、それをクライアントに関連付けます。DHCP プールから予約済みのアドレスへの割り当てを制限するには、**reserved-only** DHCP プール コンフィギュレーション コマンドを使用します。ネットワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライアントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこのコマンドを使用して、DHCP プールを装備した 1 組のスイッチが共通の IP サブネットを共有し、他のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスを事前に割り当てて、それをインターフェイス名によって特定されたクライアントに関連付けるには、特権 EXEC モードで次の手順を実行します。

■ DHCP サーバのポートベースのアドレス割り当ての設定

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dhcp pool poolname	DHCP プール コンフィギュレーション モードを開始し、DHCP プールの名前を定義します。プール名には、文字列 (例: Engineering) または整数 (例: 0) を使用できます。
ステップ 3	network network-number [mask /prefix-length]	DHCP アドレス プールのサブネット ネットワーク番号とマスクを指定します。
ステップ 4	address ip-address client-id string [ascii]	インターフェイス名によって特定される DHCP クライアントの IP アドレスを予約します。 <i>string</i> : ASCII 値または 16 進数値を設定できます。
ステップ 5	reserved-only	(任意) DHCP アドレス プールの予約済みアドレスだけを使用します。デフォルトでは、プールアドレスは制限されません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip dhcp pool	DHCP プール設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP ポートベースのアドレス割り当てをディセーブルにするには、**no ip dhcp use subscriber-id client-id** グローバル コンフィギュレーション コマンドを使用します。加入者 ID の自動生成をディセーブルにするには、**no ip dhcp subscriber-id interface-name** グローバル コンフィギュレーション コマンドを使用します。インターフェイスで加入者 ID をディセーブルにするには、**no ip dhcp server use subscriber-id client-id** インターフェイス コンフィギュレーション コマンドを使用します。

DHCP プールから IP アドレスの予約を削除するには、**no address ip-address client-id string** DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを制限されない状態に変更するには、**no reserved-only** DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージのクライアント ID フィールドを無視して、その代わりに加入者 ID を使用します。加入者 ID は、インターフェイスの略称および事前に割り当てられたクライアント IP アドレス 10.1.1.7 に基づいて決定されます。

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcpool
network 10.1.1.0 255.255.255.0
```

```
address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>
```

次に、事前に割り当てられたアドレスが DHCP プールで正しく予約されている例を示します。

```
switch# show ip dhcp pool dhcpool
Pool dhcp pool:
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 0
  Excluded addresses : 4
  Pending event : none
  1 subnet is currently in the pool:
  Current index   IP address range      Leased/Excluded/Total
  10.1.1.1       10.1.1.1 - 10.1.1.254  0 / 4 / 254
  1 reserved address is currently in the pool
  Address         Client
  10.1.1.7       Et1/0
```

DHCP サーバのポートベースのアドレス割り当て機能の設定の詳細については、Cisco.com にアクセスして検索フィールドに *Cisco IOS IP Addressing Services* と入力して Cisco IOS ソフトウェア マニュアルを参照してください。マニュアルには次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバのポートベースのアドレス割り当ての表示

DHCP サーバのポートベースのアドレス割り当て情報を表示するには、表 23-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-4 DHCP サーバのポートベースのアドレス割り当てを表示するコマンド

コマンド	目的
<code>show interface interface id</code>	特定のインターフェイスのステータスおよび設定を表示します。
<code>show ip dhcp pool</code>	DHCP アドレス プールを表示します。
<code>show ip dhcp binding</code>	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

■ DHCP サーバのポートベースのアドレス割り当ての表示



CHAPTER 24

ダイナミック ARP インспекションの設定

この章では、Catalyst 3750 スイッチにダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) インспекションを設定する方法について説明します。この機能により、同じ VLAN 内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

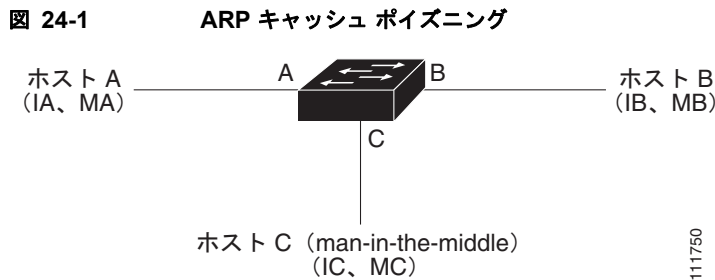
この章で説明する内容は、次のとおりです。

- 「[ダイナミック ARP インспекションの概要](#)」 (P.24-1)
- 「[ダイナミック ARP インспекションの設定](#)」 (P.24-5)
- 「[ダイナミック ARP インспекション情報の表示](#)」 (P.24-15)

ダイナミック ARP インспекションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることでレイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現しています。たとえば、ホスト B がホスト A に情報を送信しようとしていて、ARP キャッシュ内にホスト A の MAC アドレスがないとします。ホスト B は、ブロードキャスト ドメイン内のすべてのホストに対してブロードキャスト メッセージを生成し、ホスト A の IP アドレスに関連する MAC アドレスを取得します。ブロードキャスト ドメイン内のすべてのホストは ARP 要求を受信し、ホスト A は MAC アドレスで応答します。ただし、ARP 要求を受信しなくても ARP がホストからの余計な応答を許可するために、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生する可能性があります。攻撃のあと、攻撃下にあるデバイスからのすべてのトラフィックは攻撃者のコンピュータを介してルータ、スイッチ、またはホストに流れていきます。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、サブネット上の他のホストへ向かうトラフィックを代行受信することで、ネットワーク上のレイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータを攻撃します。図 24-1 は、ARP キャッシュ ポイズニングの例です。



ホスト A、B、C は、インターフェイス A、B、C 上のスイッチに接続されていて、すべてが同じサブネット上にあります。IP アドレスおよび MAC アドレスはカッコ内に示してあります。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用しています。ホスト A は、ホスト B と IP レイヤで通信を行う必要がある場合、ARP 要求をブロードキャストし、IP アドレス IB に関連する MAC アドレスを取得します。スイッチおよびホスト B は、ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を含むホストの ARP バインディングを ARP キャッシュに入力します (たとえば IP アドレス IA が MAC アドレス MA にバインドされる)。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB と MAC アドレス MB が関連付けられているホストの ARP バインディングを持つ ARP キャッシュを読み込みます。

ホスト C は、IP アドレス IA (または IB) と MAC アドレス MC が関連付けられているホストのバインディングを持つ偽造 ARP 応答をブロードキャストすることで、スイッチ、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。ポイズニングされた ARP キャッシュのあるホストは、IA または IB 向けのトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。つまりホスト C がそのトラフィックを代行受信します。ホスト C は IA および IB に関連付けられた本当の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをそれらのホストに転送できるのです。ホスト C は、ホスト A からホスト B へのトラフィック ストリームに割り込んで、一般的な *man-in-the middle* 攻撃を行います。

ダイナミック ARP インспекションは、ネットワーク内の ARP パケットを検査するセキュリティ機能です。このインспекションでは、無効な IP と MAC アドレスのバインディングを持つ ARP パケットを代行受信し、記録して、廃棄します。この機能により、ある種の *man-in-the-middle* 攻撃からネットワークを保護できます。

ダイナミック ARP インспекションにより、有効な ARP 要求および応答だけがリレーされることが保証されます。スイッチは次のアクティビティを実行します。

- 信頼できないポート上のすべての ARP 要求および応答を代行受信します。
- ローカル ARP キャッシュの更新前、またはパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP と MAC アドレスのバインディングがあるかを確認します。
- 無効な ARP パケットを廃棄します。

ダイナミック ARP インспекションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに保存されている、有効な IP と MAC アドレスのバインディングに基づいて、ARP パケットの有効性を判断します。このデータベースは、DHCP スヌーピングが VLAN およびスイッチでイネーブルの場合に、DHCP スヌーピングによって構築されます。ARP パケットが信頼できるインターフェイスで受信される場合、スイッチはチェックなしにパケットを転送します。信頼できないインターフェイスでは、スイッチは有効な場合だけパケットを転送します。

ip arp inspection vlan vlan-range グローバル コンフィギュレーション コマンドを使用して VLAN 単位でダイナミック ARP インспекションをイネーブルにできます。設定手順については、「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.24-7) を参照してください。

非 DHCP 環境では、ダイナミック ARP インспекションは、スタティックに設定された IP アドレスを持つホストのユーザ設定 ARP Access Control List (ACL; アクセス コントロール リスト) に対して、ARP パケットを検証できます。ARP ACL は、`arp access-list acl-name` グローバル コンフィギュレーション コマンドを使用して定義されます。設定手順については、「[非 DHCP 環境の ARP ACL の設定 \(P.24-9\)](#)」を参照してください。スイッチは、廃棄されたパケットを記録します。ログ バッファの詳細については、「[廃棄されたパケットのロギング \(P.24-5\)](#)」を参照してください。

パケット内の IP アドレスが無効か、または ARP パケットの本体にある MAC アドレスがイーサネット ヘッダーで指定されているアドレスと一致しない場合に、ARP パケットを廃棄するようにダイナミック ARP インспекションを設定できます。`ip arp inspection validate {[src-mac] [dst-mac] [ip]}` グローバル コンフィギュレーション コマンドを使用します。詳細については、「[妥当性チェックの実行 \(P.24-12\)](#)」を参照してください。

インターフェイス信頼状態およびネットワーク セキュリティ

ダイナミック ARP インспекションは、信頼状態とスイッチ上の各インターフェイスとを関連付けます。信頼できるインターフェイスに着信したパケットは、すべてのダイナミック ARP インспекションの検証チェックを迂回し、信頼できないインターフェイスに着信したパケットはダイナミック ARP インспекションの検証プロセスで処理されます。

一般的なネットワーク設定では、ホスト ポートに接続するすべてのスイッチ ポートを `untrusted` に設定し、スイッチに接続しているすべてのスイッチ ポートを `trusted` に設定します。このような設定では、指定したスイッチからネットワークに入ったすべての ARP パケットがセキュリティ チェックを迂回します。VLAN またはネットワーク内のその他の場所でその他の検証を行う必要はありません。信頼設定を `ip arp inspection trust` インターフェイス コンフィギュレーション コマンドを使用して設定します。

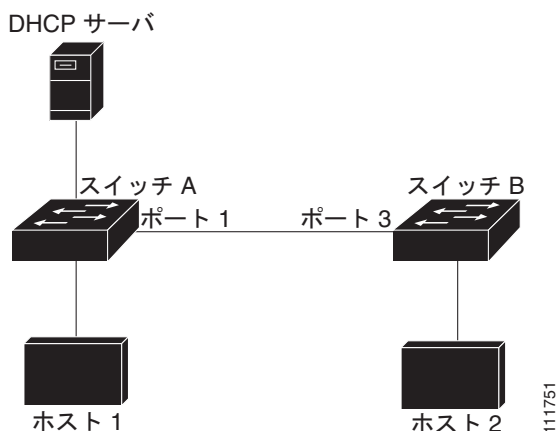


注意

信頼状態は慎重に設定してください。インターフェイスを信頼すべきときに `untrusted` と設定すると、接続が切断される可能性があります。

[図 24-2](#) では、スイッチ A およびスイッチ B の両方が、ホスト 1 およびホスト 2 のそれぞれを含む VLAN でダイナミック ARP インспекションを実行しているとします。ホスト 1 およびホスト 2 がスイッチ A に接続している DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP アドレスと MAC アドレスのペアをバインドします。このため、スイッチ A およびスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットはスイッチ B によって廃棄されます。ホスト 1 およびホスト 2 の間の接続は失われます。

図 24-2 ダイナミック ARP インспекションがイネーブルな VLAN での ARP パケット インспекション



実際にインターフェイスを信頼できない場合にインターフェイスを信頼できるように設定してしまうと、ネットワークにセキュリティホールが残ってしまいます。スイッチ A でダイナミック ARP インспекションが動作していない場合、ホスト 1 は簡単にホスト B の ARP キャッシュをポイズニングできます (スイッチ間のリンクが **trusted** に設定されている場合はホスト 2 も可能)。この状態は、スイッチ B がダイナミック ARP インспекションを実行していても発生します。

ダイナミック ARP インспекションは、ダイナミック ARP インспекションを実行しているスイッチに接続している (信頼できないインターフェイス上の) ホストがネットワーク内の他のホストの ARP キャッシュをポイズニングしないようにするものです。ただし、ダイナミック ARP インспекションでは、ネットワークの他の部分にあるホストでは、ダイナミック ARP インспекションを実行しているスイッチに接続しているホストのキャッシュに対するポイズニングは回避されません。

VLAN 内にあるスイッチの中で、ダイナミック ARP インспекションを実行しているものとしていないものがある場合、そのようなスイッチに接続しているインターフェイスを **untrusted** に設定します。ただし、ダイナミック ARP インспекションを実行していないスイッチからのパケットのバインディングを検証するには、**ARP ACL** を使用してダイナミック ARP インспекションを実行するようにスイッチを設定します。そのようなバインディングをレイヤ 3 で判別できない場合、ダイナミック ARP インспекションを実行しているスイッチを、ダイナミック ARP インспекションを実行していないスイッチから分離します。設定手順については、「[非 DHCP 環境の ARP ACL の設定](#)」(P.24-9) を参照してください。



(注) DHCP サーバおよびネットワークの設定により、VLAN 内のすべてのスイッチにある指定した ARP パケットを検査できない場合があります。

ARP パケットのレート制限

スイッチの CPU はダイナミック ARP インспекション検証チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。デフォルトで、信頼できないインターフェイスのレートは、1 秒あたり 15 パケット (pps) です。信頼できるインターフェイスはレート制限されません。**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用してこの設定を変更できます。

着信 ARP パケットのレートが設定された制限を越えた場合、スイッチはポートを `errdisable` ステータスにします。ユーザが介入するまでポートは `errdisable` ステータスのままになります。`errdisable recovery` グローバル コンフィギュレーション コマンドを使用して、指定したタイムアウト期間の経過後ポートがこのステータスから自動的に回復するように `errdisable` 回復をイネーブルにできます。



(注)

EtherChannel のレート制限は、スタック内の各スイッチに別々に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にポートを持つ各スイッチは最大 20 pps を搬送できます。スイッチの 1 つが制限を超えると、EtherChannel 全体が `errdisable` ステータスになります。

設定手順については、「[着信 ARP パケットのレート制限](#)」(P.24-11) を参照してください。

ARP ACL と DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP と MAC アドレスのバインディングのリスト用に DHCP スヌーピング バインディング データベースを使用します。

ARP ACL は DHCP スヌーピング バインディング データベース内のエントリよりも優先度が高くなります。`ip arp inspection filter vlan` グローバル コンフィギュレーション コマンドを使用して ACL を設定した場合、スイッチは ACL だけを使用します。スイッチは最初に ARP パケットとユーザ定義の ARP ACL を比較します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって読み込まれたデータベースに有効なバインディングがあっても、スイッチもパケットを拒否します。

廃棄されたパケットのロギング

スイッチがパケットを廃棄する際に、ログ バッファにエントリを配置してレート制限ベースにシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれています。

`ip arp inspection log-buffer` グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数、およびシステム メッセージを生成するのに指定した間隔で必要となるエントリ数を設定します。`ip arp inspection vlan logging` グローバル コンフィギュレーション コマンドを使用してロギングされるパケットのタイプを指定できます。設定手順については、「[ログ バッファの設定](#)」(P.24-13) を参照してください。

ダイナミック ARP インспекションの設定

ここでは、次の設定情報について説明します。

- 「[デフォルトのダイナミック ARP インспекションの設定](#)」(P.24-6)
- 「[ダイナミック ARP インспекションの設定時の注意事項](#)」(P.24-6)
- 「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.24-7) (DHCP 環境で必須)
- 「[非 DHCP 環境の ARP ACL の設定](#)」(P.24-9) (非 DHCP 環境で必須)
- 「[着信 ARP パケットのレート制限](#)」(P.24-11) (任意)
- 「[妥当性チェックの実行](#)」(P.24-12) (任意)
- 「[ログ バッファの設定](#)」(P.24-13) (任意)

デフォルトのダイナミック ARP インспекションの設定

表 24-1 に、デフォルトのダイナミック ARP インспекションの設定を示します。

表 24-1 デフォルトのダイナミック ARP インспекションの設定

機能	デフォルト設定
ダイナミック ARP インспекション	すべての VLAN でディセーブルです。
インターフェイス信頼状態	すべてのインターフェイスが信頼できません。
着信 ARP パケットのレート制限	ネットワークがスイッチドネットワークでホストが 1 秒あたり 15 の新しいホストと接続することを想定した場合、レートは信頼できないインターフェイスで 15 pps です。 信頼できるすべてのインターフェイス上ではレートは制限されません。 バースト間隔は 1 秒です。
非 DHCP 環境の ARP ACL	ARP ACL は定義されません。
検証チェック	チェックは実行されません。
ログ バッファ	ダイナミック ARP インспекションがイネーブルの場合、すべての拒否または廃棄 ARP パケットがログされます。 ログ内のエントリ数は 32 です。 システム メッセージ数は 1 秒あたり 5 に制限されています。 ロギングレート間隔は 1 秒です。
VLAN 単位ロギング	拒否または廃棄されたすべての ARP パケットがログされます。

ダイナミック ARP インспекションの設定時の注意事項

ダイナミック ARP インспекションの設定時の注意事項は次のとおりです。

- ダイナミック ARP インспекションは着信セキュリティ機能で、発信チェックは実行しません。
- ダイナミック ARP インспекションは、ダイナミック ARP インспекションをサポートしていないスイッチや、この機能をイネーブルにしていないスイッチに接続されたホストでは有効ではありません。man-in-the-middle 攻撃が単一のレイヤ 2 ブロードキャスト ドメインに限定されているため、ダイナミック ARP インспекション チェックのあるドメインとチェックのないドメインとを分離します。この処置により、ダイナミック ARP インспекションをイネーブルにしたドメイン内のホストの ARP キャッシュが保護されます。
- 着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP インспекションは DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしていることを確認します。設定の詳細については、[第 23 章「Dynamic Host Configuration Protocol \(DHCP\) 機能および IP ソース ガード \(IPSG\) 機能の設定」](#)を参照してください。

DHCP スヌーピングがディセーブルの場合または非 DHCP 環境では、ARP ACL を使用してパケットを許可または拒否します。

- ダイナミック ARP インспекションは、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされています。



(注) RSPAN VLAN 上でダイナミック ARP インспекションをイネーブルにしないでください。RSPAN VLAN 上でダイナミック ARP インспекションをイネーブルにすると、ダイナミック ARP インспекション パケットが RSPAN 宛先ポートに到達しないことがあります。

- 物理ポートとチャネルポートの信頼状態が一致した場合に限り、物理ポートは EtherChannel ポートチャネルに加入できます。そうでない場合、物理ポートはポートチャネル内で停止したままになります。ポートチャネルは、チャネルに最初に参加した物理ポートの信頼状態を継承します。その結果、最初の物理ポートの信頼状態はチャネルの信頼状態と一致する必要がありません。
逆にいえば、ポートチャネルの信頼状態を変更した場合、スイッチはチャネルを構成するすべての物理ポートの信頼状態を新規に設定します。
- レート制限はスイッチスタックの各スイッチで個別に計算されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも大きいことを意味します。たとえば、スイッチ 1 にポートが 1 つ、スイッチ 2 にポートが 1 つある EtherChannel 上でレート制限を 30 pps に設定した場合、EtherChannel を errdisable にせずに、各ポートは 29 pps でパケットを受信できます。
- ポートチャネルの動作レートは、チャネル内のすべての物理ポートを累積したものです。たとえば、ポートチャネルの ARP レート制限を 400 pps に設定した場合、チャネル上に集約される全インターフェイスで合計 400 pps を受信します。EtherChannel ポートの着信 ARP パケットのレートは、全チャネルメンバーからのパケットの着信レートを合計したものです。チャネルポートメンバーの着信 ARP パケットのレートを検査したあとに、EtherChannel ポートのレート制限を設定します。
物理ポート上の着信パケットのレートは、物理ポート設定ではなくポートチャネル設定に対してチェックされます。ポートチャネルのレート制限設定は、物理ポートの設定からは独立しています。
EtherChannel が設定レートよりも多くの ARP パケットを受信する場合、(すべての物理ポートを含む) チャネルは errdisable ステートになります。
- 着信トランクポート上の ARP パケットのレートを制限していることを確認します。集約を反映して、複数のダイナミック ARP インспекション対応 VLAN でパケットを処理するために、トランクポートを高めレートに設定します。また、`ip arp inspection limit none` インターフェイスコンフィギュレーションコマンドを使用してレートを無制限にできます。1 つの VLAN でレート制限が高いと、ソフトウェアがポートを errdisable ステートにするときに、他の VLAN が DoS 攻撃を受ける可能性があります。
- ダイナミック ARP インспекションをスイッチでイネーブルにする際に、ARP トラフィックをポーリングするために設定されたポリシーは無効となります。その結果、すべての ARP トラフィックが CPU に送信されます。

DHCP 環境でのダイナミック ARP インспекションの設定

この手順は、2 つのスイッチがこの機能をサポートしている場合にダイナミック ARP インспекションを設定する方法について説明します。図 24-2 (P.24-4) で示しているように、ホスト 1 はスイッチ A に接続していて、ホスト 2 はスイッチ B に接続しています。両方のスイッチが、ホストが位置する VLAN 1 でダイナミック ARP インспекションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同じ DHCP サーバから IP アドレスを取得します。したがって、スイッチ A にはホスト 1 およびホスト 2 のバインディングがあり、スイッチ B にはホスト 2 のバインディングがあります。



(注) 着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP インспекションは DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしていることを確認します。設定の詳細については、第 23 章「Dynamic Host Configuration Protocol (DHCP) 機能および IP ソース ガード (IPSG) 機能の設定」を参照してください。

1 つのスイッチのみがダイナミック ARP インспекションをサポートしている場合の、この機能の設定の詳細については、「非 DHCP 環境の ARP ACL の設定」(P.24-9) を参照してください。

ダイナミック ARP インспекションを設定するには、特権 EXEC モードで次の手順を行います。この手順を両方のスイッチで実行する必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	<code>show cdp neighbors</code>	スイッチ間の接続を確認します。
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>ip arp inspection vlan <i>vlan-range</i></code>	ダイナミック ARP インспекションを VLAN 単位でイネーブルにします。デフォルトで、ダイナミック ARP インспекションはすべての VLAN でディセーブルに設定されています。 <i>vlan-range</i> では、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	<code>interface <i>interface-id</i></code>	他のスイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>ip arp inspection trust</code>	スイッチ間の接続を <code>trusted</code> に設定します。 デフォルトでは、すべてのインターフェイスが <code>untrusted</code> です。スイッチは、信頼できるインターフェイス上にある他のスイッチから受信した ARP パケットをチェックしません。単純にパケットを転送するだけです。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および応答を代行受信します。ローカル キャッシュの更新前、およびパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP アドレスと MAC アドレスのバインディングがあるかを確認します。スイッチは、 <code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドによって指定されたロギング設定に従って、無効なパケットを廃棄してログ バッファに記録します。詳細については、「ログ バッファの設定」(P.24-13) を参照してください。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip arp inspection interfaces</code> <code>show ip arp inspection vlan <i>vlan-range</i></code>	ダイナミック ARP インспекションの設定を確認します。
ステップ 8	<code>show ip dhcp snooping binding</code>	DHCP バインディングを確認します。
ステップ 9	<code>show ip arp inspection statistics vlan <i>vlan-range</i></code>	ダイナミック ARP インспекションの設定をチェックします。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP インспекションをディセーブルにするには、**no ip arp inspection vlan vlan-range** グローバル コンフィギュレーション コマンドを使用します。ポートを **untrusted** の状態に戻すには、**no ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

以下は、VLAN 1 のスイッチ A でダイナミック ARP インспекションを設定する方法の例です。スイッチ B でも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境の ARP ACL の設定

この手順は、[図 24-2 \(P.24-4\)](#) で示すスイッチ B がダイナミック ARP インспекションまたは DHCP スヌーピングをサポートしていない場合に、ダイナミック ARP インспекションを設定する方法を示しています。

スイッチ A のポート 1 を **trusted** に設定すると、スイッチ A およびホスト 1 はスイッチ B またはホスト 2 から攻撃される可能性があるため、セキュリティ ホールができてしまいます。この可能性をなくするため、スイッチ A のポート 1 を **untrusted** に設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定して VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスが静的でなく、スイッチ A で ACL 設定を適用できない場合は、レイヤ 3 でスイッチ B とスイッチ A を分離し、ルータを使用してその間でパケットをルーティングする必要があります。

スイッチ A で ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境で必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	arp access-list acl-name	ARP ACL を定義し、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセスリストは定義されていません。 (注) ARP アクセスリストの最後には、暗黙の deny ip any mac any コマンドがあります。
ステップ 3	permit ip host sender-ip mac host sender-mac [log]	指定したホスト (ホスト 2) からの ARP パケットを許可します。 <ul style="list-style-type: none"> sender-ip に対して、ホスト 2 の IP アドレスを入力します。 sender-mac に対して、ホスト 2 の MAC アドレスを入力します。 (任意) Access Control Entry (ACE; アクセス コントロール エントリ) が一致した場合にログ バッファ内のパケットをログするために log を指定します。ip arp inspection vlan logging グローバル コンフィギュレーション コマンドを matchlog キーワードとともに設定した場合、一致も記録されます。詳細については、「ログ バッファの設定 (P.24-13)」を参照してください。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 5 ip arp inspection filter <i>arp-acl-name</i> vlan <i>vlan-range</i> [static] 	ARP ACL に VLAN を適用します。デフォルトで、どの VLAN にも ARP ACL が定義されていません。 <ul style="list-style-type: none"> • <i>arp-acl-name</i> には、ステップ 2 で作成した ACL 名を指定します。 • <i>vlan-range</i> には、スイッチおよびホストが含まれる VLAN を指定します。VLAN ID 番号によって識別される単一の VLAN を指定したり、ハイフンで区切って VLAN の範囲を指定したり、カンマで区切って一連の VLAN を指定したりできます。指定できる範囲は 1 ~ 4094 です。 • (任意) ARP ACL 内の暗黙の拒否を明示的な拒否として処理し、ACL の前の句と一致しないパケットを廃棄するには、static を指定します。DHCP バインディングは使用されません。 このキーワードを指定しない場合、パケットを拒否する ACL に暗黙拒否がないことを意味し、パケットが ACL 内のどの句とも一致しない場合に DHCP バインディングがパケットを許可するか拒否するかを判断します。 <p>IP および MAC アドレスのバインディングのみを含む ARP パケットが ACL と比較されます。パケットは、アクセスリストが許可した場合に限り許可されます。</p>
ステップ 6 interface <i>interface-id</i> 	スイッチ B に接続されたスイッチ A インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7 no ip arp inspection trust 	スイッチ B に接続しているスイッチ A インターフェイスを untrusted として設定します。 <p>デフォルトでは、すべてのインターフェイスが untrusted です。信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および応答を代行受信します。ローカル キャッシュの更新前、およびパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP アドレスと MAC アドレスのバインディングがあるかを確認します。スイッチは、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドによって指定されたロギング設定に従って、無効なパケットを廃棄してログ バッファに記録します。詳細については、「ログ バッファの設定」(P.24-13) を参照してください。</p>
ステップ 8 end 	特権 EXEC モードに戻ります。
ステップ 9 show arp access-list [<i>acl-name</i>] show ip arp inspection vlan <i>vlan-range</i> show ip arp inspection interfaces 	設定を確認します。
ステップ 10 copy running-config startup-config 	(任意) コンフィギュレーション ファイルに設定を保存します。

ARP、ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に添付されている ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、*host2* という ARP ACL を設定し、ホスト 2 (IP アドレスが 1.1.1.1 で MAC アドレスが 0001.0001.0001) からの ARP パケットを許可し、ACL を VLAN 1 に適用し、スイッチ A のポート 1 を *untrusted* に設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチの CPU はダイナミック ARP インспекション検証チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。

着信 ARP パケットのレートが設定された制限を越えた場合、スイッチはポートを *errdisable* ステートにします。指定したタイムアウト期間の経過後、ポートがこのステートから自動的に回復するように *errdisable* 回復をイネーブルにしないと、ポートは *errdisable* ステートのままになります。



(注)

インターフェイスにレート制限を設定しない場合、インターフェイスの信頼状態の変更によって、レート制限がその信頼状態のデフォルト値に変更されます。レート制限を設定したあと、信頼状態が変更される際にインターフェイスはレート制限を保存します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力した場合、インターフェイスはデフォルトのレート制限に戻ります。

トランク ポートおよび EtherChannel のレート制限の設定時の注意事項については、「[ダイナミック ARP インспекションの設定時の注意事項](#)」(P.24-6) を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	レート制限を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip arp inspection limit {rate pps [burst interval seconds] none}	<p>インターフェイス上の着信 ARP 要求および応答のレートを制限します。</p> <p>デフォルトのレートは信頼できないインターフェイスで 15 pps、信頼できるインターフェイスで無制限です。バースト間隔は 1 秒です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> rate pps では、1 秒あたりに処理される着信パケットの上限数を指定します。指定できる範囲は 0 ~ 2048 pps です。 (任意) burst interval seconds では、高いレートの ARP パケットについてインターフェイスがモニタされる累積期間を秒単位で指定します。範囲は 1 ~ 15 です。 rate none では、処理可能な着信 ARP パケットの上限を指定しません。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 5 <code>errdisable recovery cause arp-inspection interval interval</code>	(任意) ダイナミック ARP インспекションの <code>errdisable</code> ステートからのエラー回復をイネーブルにします。 デフォルトで、回復はディセーブルで、回復間隔は 300 秒です。 <code>interval interval</code> では、 <code>errdisable</code> ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ~ 86400 です。
ステップ 6 <code>exit</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show ip arp inspection interfaces</code> <code>show errdisable recovery</code>	設定値を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのレート制限設定に戻すには、`no ip arp inspection limit` インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP インспекションのエラー回復をディセーブルにするには、`no errdisable recovery cause arp-inspection` グローバル コンフィギュレーション コマンドを使用します。

妥当性チェックの実行

ダイナミック ARP インспекションでは、無効な IP/MAC アドレス バインディングのある ARP パケットを代行受信し、記録し、廃棄します。宛先 MAC アドレス、発信者 IP アドレスおよび対象 IP アドレス、送信元 MAC アドレスで追加チェックを実施するようにスイッチを設定できます。

着信 ARP パケットで特定のチェックを実施するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>ip arp inspection validate {[src-mac] [dst-mac] [ip]}</code>	着信 ARP パケットで特定のチェックを実行します。デフォルトで、チェックは実行しません。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <code>src-mac</code> では、ARP ボディ内の発信者 MAC アドレスに対して、イーサネットヘッダーの送信元 MAC アドレスをチェックします。チェックは ARP 要求および応答の両方で実施されます。イネーブルの場合、異なる MAC アドレスのあるパケットは無効として分類され、廃棄されます。 <code>dst-mac</code> では、ARP 形式の対象 MAC アドレスに対して、イーサネットヘッダーの宛先 MAC アドレスを検査します。この検査は ARP 応答で実施されます。イネーブルの場合、異なる MAC アドレスのあるパケットは無効として分類され、廃棄されます。 <code>ip</code> では、無効で予期しない IP アドレスの ARP 形式をチェックします。アドレスには、0.0.0.0、255.255.255.255 およびすべての IP マルチキャスト アドレスが含まれます。発信者 IP アドレスは ARP 要求および応答すべてでチェックされ、対象 IP アドレスは ARP 応答でのみチェックされます。 <p>最低 1 つのキーワードを指定する必要があります。各コマンドは、前のコマンドの設定を上書きします。たとえば、あるコマンドが <code>src</code> および <code>dst mac</code> 検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにした場合、2 番目のコマンドによって <code>src</code> および <code>dst mac</code> 検証はディセーブルになります。</p>

	コマンド	目的
ステップ 3	exit	特権 EXEC モードに戻ります。
ステップ 4	show ip arp inspection vlan <i>vlan-range</i>	設定値を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

チェックをディセーブルにするには、**no ip arp inspection validate [src-mac] [dst-mac] [ip]** グローバル コンフィギュレーション コマンドを使用します。転送、廃棄、MAC 検証失敗、および IP 検証失敗 パケットの統計情報を表示するには、**show ip arp inspection statistics** 特権 EXEC コマンドを使用します。

ログ バッファの設定

スイッチがパケットを廃棄する際に、ログ バッファにエントリを配置してレート制限ベースにシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれています。

ログ バッファ エントリは、複数のパケットを表示できます。たとえば、インターフェイスが同じ ARP パラメータを持つ VLAN 上で多くのパケットを受信する場合、スイッチはパケットをログ バッファ内の 1 つのエントリに結合して、エントリの単一のシステム メッセージを生成します。

ログ バッファがオーバーフローした場合、つまり、ログ イベントがログ バッファに収まらない場合、**show ip arp inspection log** 特権 EXEC コマンドの表示が影響を受けます。表示内の「--」は、パケット カウントと時間を除く、すべてのデータの代わりに表示されます。他の統計情報はエントリ用に提供されます。このエントリを表示で見える場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

ログ バッファ設定は、スイッチ スタックの各スタック メンバーに適用されます。各スタック メンバーには指定された **logs number** エントリが含まれ、設定されたレートでシステム メッセージを生成します。たとえば、インターバル (レート) が 1 エントリ/秒の場合、最大 5 つのシステム メッセージが 5 メンバー スイッチ スタック内で秒ごとに生成されます。

ログ バッファを設定するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>ip arp inspection log-buffer {entries number logs number interval seconds}</code>	<p>ダイナミック ARP インспекション ログバッファを設定します。</p> <p>デフォルトで、ダイナミック ARP インспекションがイネーブルの場合、拒否または廃棄 ARP パケットがログされます。ログ エントリの数は 32 です。システム メッセージ数は 1 秒あたり 5 に制限されています。ログ レート間隔は 1 秒です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • entries number では、バッファ内に記録されるエントリ数を指定します。指定できる範囲は 0 ~ 1024 です。 • logs number interval seconds では、指定した間隔でシステム メッセージを生成するためのエントリ数を指定します。 <p>logs number に指定できる範囲は 0 ~ 1024 です。値を 0 にすると、エントリはログ バッファに配置されますが、システム メッセージは生成されません。</p> <p>interval seconds に指定できる範囲は 0 ~ 86400 秒 (1 日) です。0 値は、システム メッセージが即座に生成されます (またログ バッファは常に空です)。</p> <p>0 の間隔設定は、ログ設定 0 を上書きします。</p> <p>logs および interval 設定は相互作用します。logs number X が interval seconds Y より大きい場合、X を Y で除算した (X/Y) 数のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y を X で除算した (Y/X) 秒毎に送信されます。</p>
ステップ 3 <code>ip arp inspection vlan vlan-range logging {acl-match {matchlog none} dhcp-bindings {all none permit}}</code>	<p>記録されるパケットのタイプを VLAN 単位で制御します。デフォルトで、すべての拒否および廃棄パケットが記録されます。用語 <i>logged</i> は、エントリはログ バッファに置かれてシステム メッセージが生成されることを意味します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • vlan-range では、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 • acl-match matchlog では、ACL ログ設定に基づいたパケットを記録します。このコマンドで matchlog キーワードを指定し、permit または deny ARP アクセスリスト コンフィギュレーション コマンドで log キーワードを指定した場合、ACL で許可または拒否された ARP パケットが記録されます。 • acl-match none では、ACL と一致するパケットを記録しません。 • dhcp-bindings all では、DHCP バインディングと一致するパケットがすべて記録されます。 • dhcp-bindings none では、DHCP バインディングと一致するパケットが記録されません。 • dhcp-bindings permit では、DHCP バインディング許可パケットを記録します。
ステップ 4 <code>exit</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 5 <code>show ip arp inspection log</code>	設定値を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのログ バッファ設定に戻すには、`no ip arp inspection log-buffer {entries | logs}` グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻すには、`no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}` グローバル コンフィギュレーション コマンドを使用します。ログ バッファをクリアするには、`clear ip arp inspection log` 特権 EXEC コマンドを使用します。

ダイナミック ARP インспекション情報の表示

ダイナミック ARP インспекション情報を表示するには、表 24-2 で説明している特権 EXEC コマンドを使用します。

表 24-2 ダイナミック ARP インспекション情報のコマンド

コマンド	説明
<code>show arp access-list [acl-name]</code>	ARP ACL の詳細情報を表示します。
<code>show ip arp inspection interfaces [interface-id]</code>	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
<code>show ip arp inspection vlan vlan-range</code>	指定された VLAN に対するダイナミック ARP インспекションの設定および動作状態を表示します。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP インспекションがイネーブル (アクティブ) である VLAN の情報だけが表示されます。

ダイナミック ARP インспекション統計情報を消去または表示するには、表 24-3 で説明している特権 EXEC コマンドを使用します。

表 24-3 ダイナミック ARP インспекションの統計情報を消去または表示するコマンド

コマンド	説明
<code>clear ip arp inspection statistics</code>	ダイナミック ARP インспекションの統計情報を消去します。
<code>show ip arp inspection statistics [vlan vlan-range]</code>	指定した VLAN の転送パケット、廃棄パケット、MAC 確認エラー パケット、IP 確認エラー パケット、ACL の許可および拒否パケット、DHCP 許可および拒否パケットの統計情報が表示されます。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP インспекションがイネーブル (アクティブ) である VLAN の情報だけが表示されます。

`show ip arp inspection statistics` コマンドでは、スイッチは信頼できるダイナミック ARP インспекション ポート上の各 ARP 要求および応答パケットの転送パケット数を増やします。スイッチは、各パケットに対して、送信元 MAC、宛先 MAC、または IP 検証チェックで拒否された ACL または DHCP 許可パケット数を増加させ、スイッチは該当する失敗カウントを増加させます。

ダイナミック ARP インспекション ロギング情報を消去または表示するには、表 24-4 で説明している特権 EXEC コマンドを使用します。

表 24-4 ダイナミック ARP インспекションのロギング情報を消去または表示するコマンド

コマンド	説明
<code>clear ip arp inspection log</code>	ダイナミック ARP インспекション ログ バッファをクリアします。
<code>show ip arp inspection log</code>	ダイナミック ARP インспекション ログ バッファの設定と内容を表示します。

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



CHAPTER 25

IGMP スヌーピングおよび MVR の設定

この章では、Internet Group Management Protocol (IGMP) スヌーピングを Catalyst 3750 スイッチ上で設定する方法について、ローカル IGMP スヌーピング、Multicast VLAN Registration (MVR) の適用を含めて説明します。また、IGMP フィルタリングを使用したマルチキャスト グループ メンバシップの制御と、IGMP スロットリング アクションの設定手順についても説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

IP バージョン 6 (IPv6) トラフィックでは、Multicast Listener Discovery (MLD) スヌーピングが IPv4 トラフィックに対する IGMP スヌーピングと同じ機能を実行します。MLD スヌーピングの詳細については、[第 40 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』 Release 12.2 の「IP Multicast Routing Commands」のセクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「[IGMP スヌーピングの概要](#)」 (P.25-2)
- 「[IGMP スヌーピングの設定](#)」 (P.25-7)
- 「[IGMP スヌーピング情報の表示](#)」 (P.25-16)
- 「[MVR の概要](#)」 (P.25-18)
- 「[MVR の設定](#)」 (P.25-20)
- 「[MVR 情報の表示](#)」 (P.25-24)
- 「[IGMP フィルタリングおよびスロットリングの設定](#)」 (P.25-25)
- 「[IGMP フィルタリングおよび IGMP スロットリング設定の表示](#)」 (P.25-30)



(注)

IGMP スヌーピング、MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理することもできますし、スタティック IP アドレスを使用することもできます。

IGMP スヌーピングの概要

レイヤ 2 スイッチは IGMP スヌーピングを使用して、レイヤ 2 インターフェイスを動的に設定し、マルチキャストトラフィックが IP マルチキャストデバイスと対応付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャストトラフィックのフラッディングを制限できます。名称が示すとおり、IGMP スヌーピングの場合、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャストグループとメンバーポートを追跡する必要があります。特定のマルチキャストグループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブルエントリからホストポートを削除します。マルチキャストクライアントから IGMP メンバシップレポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。



(注)

IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャストルータ（スタックマスターに IP サービスイメージを搭載した Catalyst 3750 スイッチも含む）は、すべての VLAN に定期的に一般クエリーを送信します。このマルチキャストトラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC（メディアアクセス制御）アドレスに基づくグループではなく、IP マルチキャストグループに基づくブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグループの場合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。スイッチでは IP マルチキャストグループを使用するので、アドレスエイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャストグループは動的に学習されます。ただし、**ip igmp snooping vlan *vlan-id* static ip *address* interface *interface-id*** グローバル コンフィギュレーション コマンドを使用すると、マルチキャストグループを静的に設定できます。グループメンバシップをマルチキャストグループアドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャストグループメンバシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャストトラフィックはルーティングする必要がないのでマルチキャストインターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピングクエリーを設定できます。IGMP スヌーピングクエリーの詳細については、「[IGMP スヌーピングクエリアの設定](#)」(P.25-14) を参照してください。

ポートスパンニングツリー、ポートグループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャストグループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

- 「[IGMP バージョン](#)」(P.25-3)
- 「[マルチキャストグループへの加入](#)」(P.25-3)
- 「[マルチキャストグループからの脱退](#)」(P.25-5)
- 「[即時脱退](#)」(P.25-6)
- 「[IGMP 脱退タイマーの設定](#)」(P.25-6)
- 「[IGMP レポート抑制](#)」(P.25-6)
- 「[IGMP スヌーピングおよびスイッチスタック](#)」(P.25-7)

IGMP バージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これら 3 つのバージョンは、スイッチ上でそれぞれ相互運用できます。たとえば、IGMPv2 スイッチ上で IGMP スヌーピングがイネーブルの場合、このスイッチが IGMPv3 レポートをホストから受信すると、この IGMPv3 レポートをマルチキャスト ルータへ転送できます。



(注) スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support (BISS) をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラグディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。



(注) IGMP フィルタリングまたは MVR が実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

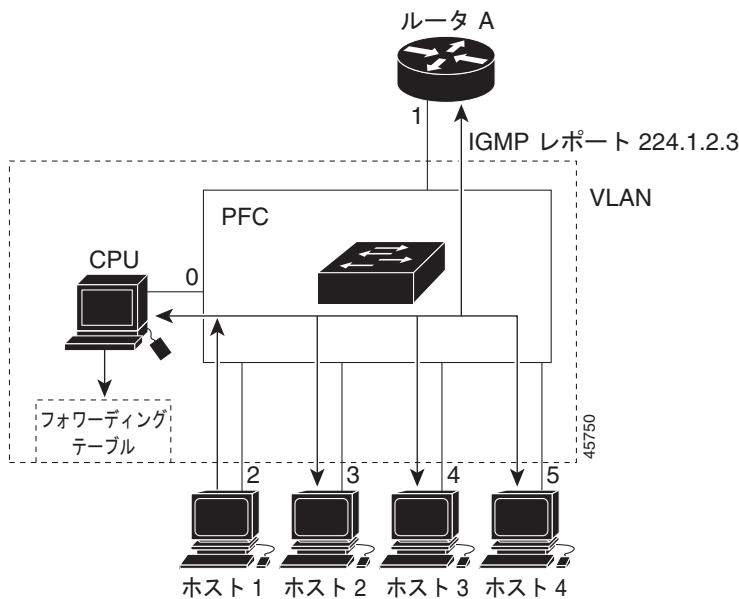
IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの送受信を行うことができます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a.html

マルチキャスト グループへの加入

スイッチに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリーを受信したスイッチは、そのクエリーを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはスイッチに Join メッセージを送信することによって応答します。スイッチの Central Processing Unit (CPU; 中央処理装置) は、そのグループのマルチキャスト転送テーブル エントリがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。図 25-1 を参照してください。

図 25-1 IGMP Join の初期メッセージ



ルータ A がスイッチに一般クエリーを送り、スイッチはそのクエリーをポート 2 ~ 5、つまり同一 VLAN のすべてのメンバーに転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバシップ レポート (IGMP Join メッセージ) をマルチキャストします。スイッチの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します (表 25-1 を参照)。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 25-1 IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2

スイッチのハードウェアは、マルチキャスト グループの他のパケットと IGMP 情報パケットを区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛での、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

別のホスト (たとえばホスト 4) が同じグループに非請求の IGMP Join メッセージを送信する場合 (図 25-2 を参照)、CPU はメッセージを受信して、転送テーブルにホスト 4 のポート番号を追加します (表 25-2 を参照)。転送テーブルによって、CPU だけに IGMP メッセージが転送されるので、スイッチ上の他のポートにメッセージがフラッディングされることはありません。既知のマルチキャスト トラフィックはすべて、CPU ではなくグループに転送されます。

図 25-2 2 番めのホストのマルチキャスト グループへの加入

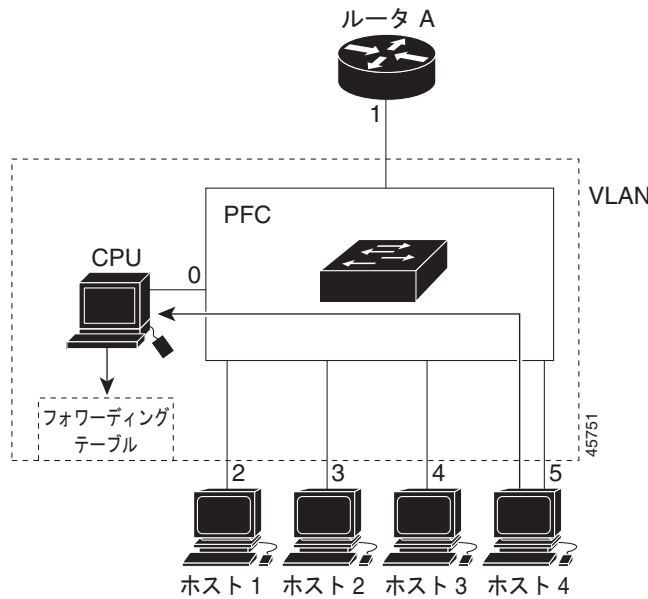


表 25-2 更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリーを定期的を送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャストトラフィックを受信しなければならない場合、ルータは VLAN に引き続き、マルチキャストトラフィックを転送します。スイッチは、その IGMP スヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャストグループトラフィックを転送します。

ホストがマルチキャストグループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したスイッチは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャストトラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチからインターフェイスにグループ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルニングされます。即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。



(注) 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。1 つのポートに複数のホストが接続されている VLAN で即時脱退機能をイネーブルにすると、一部のホストが誤って切断される可能性があります。

設定手順については、「[IGMP 即時脱退のイネーブル化](#)」(P.25-11) を参照してください。

IGMP 脱退タイマーの設定

グループ固有のクエリーを送信したあとのスイッチの待機時間を設定して、ホストがまだ指定のマルチキャスト グループに関心があるかどうかを確認できます。IGMP 脱退応答時間は、100 ~ 5000 ミリ秒の間で設定できます。タイマーはグローバルにまたは VLAN 単位で設定できますが、VLAN に脱退時間を設定すると、グローバルに設定した脱退時間は上書きされます。

設定手順については、「[IGMP 脱退タイマーの設定](#)」(P.25-12) を参照してください。

IGMP レポート抑制



(注) IGMP レポート抑制がサポートされるのは、マルチキャストクエリーが IGMPv1 および IGMPv2 レポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブルの場合 (デフォルト)、このスイッチは、グループに対応するすべてのホストからの最初の IGMP レポートをすべてのマルチキャスト ルータに送信します。スイッチは、グループに対応する残りの IGMP レポートについては、マルチキャスト ルータに送信しません。この機能により、重複したレポートがマルチキャスト デバイスに送信されるのを防ぎます。

マルチキャスト ルータのクエリーに、IGMPv1 および IGMPv2 レポートだけに対応したレポートが含まれている場合、スイッチはグループ内のすべてのホストから、最初の IGMPv1 または IGMPv2 レポートだけを、すべてのマルチキャスト ルータに転送します。

また、マルチキャスト ルータ クエリーに、IGMPv3 レポートの要求も含まれている場合、スイッチは、グループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。設定手順については、「[IGMP レポート抑制のディセーブル化](#)」(P.25-16) を参照してください。

IGMP スヌーピングおよびスイッチ スタック

IGMP スヌーピングはスイッチ スタックに対して機能します。つまり、1 つのスイッチから取得された IGMP 制御情報は、スタック内のすべてのスイッチに配信されます（スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照）。IGMP マルチキャストデータがスタックに入るときに経路するスタック メンバーに関係なく、データはそのグループに登録されたホストに到達します。

スタック内のスイッチに障害が発生したか、またはスイッチがスタックから削除された場合は、そのスイッチ上のマルチキャスト グループのメンバーだけがマルチキャスト データを受信しなくなります。スタック内の他のスイッチ上のその他のマルチキャスト グループ メンバーはすべて、マルチキャスト データ ストリームを引き続き受信します。ただし、スタック マスターが削除された場合は、レイヤ 2 およびレイヤ 3 (IP マルチキャスト ルーティング) の両方に共通するマルチキャスト グループの収束時間が長くなることがあります。

IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。ここでは、次の設定情報について説明します。

- 「IGMP スヌーピングのデフォルト設定」 (P.25-7)
- 「IGMP スヌーピングのイネーブル化およびディセーブル化」 (P.25-8)
- 「スヌーピング方法の設定」 (P.25-9)
- 「マルチキャスト ルータ ポートの設定」 (P.25-10)
- 「グループに加入するホストの静的な設定」 (P.25-10)
- 「IGMP 即時脱退のイネーブル化」 (P.25-11)
- 「IGMP 脱退タイマーの設定」 (P.25-12)
- 「TCN 関連のコマンドの設定」 (P.25-12)
- 「IGMP スヌーピング クエリアの設定」 (P.25-14)
- 「IGMP レポート抑制のディセーブル化」 (P.25-16)

IGMP スヌーピングのデフォルト設定

表 25-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 25-3 IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	未設定
マルチキャスト ルータの学習 (スヌーピング) 方式	PIM-DVMRP
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN ¹ フラッド クエリー カウント	2
TCN クエリー送信要求	ディセーブル

表 25-3 IGMP スヌーピングのデフォルト設定 (続き)

機能	デフォルト設定
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN = Topology Change Notification (トポロジ変更通知)

IGMP スヌーピングのイネーブル化およびディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブルです。グローバルにイネーブルまたはディセーブルに設定されている場合、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルです。デフォルトでは、IGMP スヌーピングはすべての VLAN でイネーブルですが、VLAN 単位で IGMP スヌーピングをイネーブルおよびディセーブルに設定できます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングよりも優先されます。グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチ上で IGMP スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping</code>	既存のすべての VLAN インターフェイスで、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN インターフェイス上で IGMP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i></code>	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan *vlan-id*** グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリ ごとに転送テーブルに追加されます。スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol Independent Multicast (PIM) パケット、および Distance Vector Multicast Routing Protocol (DVMRP) パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol (CGMP) パケットの待ち受け
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。デフォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングします。CGMP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan vlan-id mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、その他の CGMP パケットは待ち受けません。PIM パケットと DVMRP パケットだけでマルチキャスト ルータ ポートを学習するには、**ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp** グローバル コンフィギュレーション コマンドを使用します。



(注)

学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャスト ルータがない場合は、**ip cgmp router-only** コマンドを入力し、ルータに動的にアクセスする必要があります。詳細は、[第 46 章「IP マルチキャスト ルーティングの設定」](#)を参照してください。

VLAN インターフェイスがマルチキャスト ルータに動的にアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan vlan-id mrouter learn {cgmp pim-dvmrp}	VLAN で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 マルチキャスト ルータの学習方式を指定します。 <ul style="list-style-type: none"> • cgmp : CGMP パケットを待ち受けます。この方法は、制御トラフィックを減らす場合に有用です。 • pim-dvmrp : IGMP クエリーおよび PIM パケットと DVMRP パケットをスヌーピングします。これがデフォルトです。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの学習方式に戻すには、**no ip igmp snooping vlan vlan-id mrouter learn cgmp** グローバル コンフィギュレーション コマンドを使用します。

次に、CGMP パケットを学習方式として使用するよう IGMP スヌーピングを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加する（マルチキャスト ルータに静的な接続を追加する）には、スイッチで **ip igmp snooping vlan mrouter** グローバル コンフィギュレーション コマンドを使用します。



(注) マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

マルチキャスト ルータへの静的な接続をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。 <ul style="list-style-type: none"> VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 インターフェイスは物理インターフェイスにすることもポートチャネルにすることもできます。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping mrouter [vlan <i>vlan-id</i>]	VLAN インターフェイス上で IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ip igmp snooping vlan *vlan-id* mrouter interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch(config)# end
```

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i></code>	マルチキャスト グループのメンバーとしてレイヤ 2 ポートを静的に設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> は、マルチキャスト グループの VLAN ID です。有効範囲は 1 ~ 1001 および 1006 ~ 4094 です。 <i>ip-address</i> は、グループの IP アドレスです。 <i>interface-id</i> は、メンバー ポートです。物理インターフェイスまたはポート チャネル (1 ~ 48) に設定できます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip igmp snooping groups</code>	メンバー ポートおよび IP アドレスを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、`no ip igmp snooping vlan vlan-id static ip-address interface interface-id` グローバル コンフィギュレーション コマンドを使用します。

次に、ポート上のホストを静的に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。



(注) 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

IGMP 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping vlan <i>vlan-id</i> immediate-leave</code>	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip igmp snooping vlan <i>vlan-id</i></code>	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN 上で IGMP 即時脱退をディセーブルにするには、`no ip igmp snooping vlan vlan-id immediate-leave` グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP 脱退タイマーの設定

IGMP 脱退タイマーを設定するときには、次の注意事項に従ってください。

- 脱退時間はグローバルまたは VLAN 単位で設定できます。
- VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
- デフォルトの脱退時間は 1000 ミリ秒です。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼動しているホストでのみサポートされます。
- ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間と異なることがあります。

IGMP 脱退タイマーの設定をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp snooping last-member-query-interval time</code>	グローバルに IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 32768 ミリ秒です。デフォルト値は 1000 ミリ秒です。
ステップ 3	<code>ip igmp snooping vlan vlan-id last-member-query-interval time</code>	(任意) VLAN インターフェイス上で、IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 32768 ミリ秒です。 (注) VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp snooping</code>	(任意) 設定された IGMP 脱退タイマーを表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、`no ip igmp snooping last-member-query-interval` グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN から IGMP 脱退タイマーの設定を削除するには、`no ip igmp snooping vlan vlan-id last-member-query-interval` グローバル コンフィギュレーション コマンドを使用します。

TCN 関連のコマンドの設定

ここでは、TCN イベント中にフラッディングしたマルチキャスト トラフィックを制御する方法を説明します。

- 「TCN イベント後のマルチキャスト フラッディング時間の制御」(P.25-13)
- 「フラッディング モードからの回復」(P.25-13)
- 「TCN イベント中のマルチキャスト フラッディングのディセーブル化」(P.25-14)

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、TCN イベント後にフラッディングするマルチキャスト トラフィックの時間を制御できます。このコマンドは、TCN イベント後にフラッディングするマルチキャスト データのトラフィックに対し、一般クエリー数を設定します。クライアントが場所を変更することで同ポートの受信者がブロックされたあと、現在転送中の場合、またはポートが Leave メッセージを送信せずにダウンした場合などが、TCN イベントに該当します。

ip igmp snooping tcn flood query count コマンドを使用して、TCN フラッディング クエリー カウントを 1 に設定した場合、一般クエリーを 1 つ受信するまでフラッディングが続きます。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般クエリーに基づいて再度学習されます。

TCN フラッディング クエリー カウントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping tcn flood query count <i>count</i>	マルチキャスト トラフィックのフラッディングに使用する一般 IGMP クエリー数を指定します。指定できる範囲は 1 ~ 10 です。デフォルトのフラッディング クエリー カウントは 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	TCN の設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのフラッディング クエリー カウントに戻す場合は、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニング ツリーのルートは特別な IGMP Leave メッセージ (グローバル Leave メッセージ) をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニング ツリーのルートであるかどうかに関わらず、グローバル Leave メッセージを送信します。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからの回復に努めます。スイッチがスパニング ツリーのルートであれば、このコンフィギュレーション コマンドに関係なく、Leave メッセージが常に送信されます。デフォルトでは、クエリー送信要求はディセーブルに設定されています。

スイッチがスパニング ツリー ルートであるかどうかに関わらず、グローバル Leave メッセージを送信するように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping tcn query solicit	IGMP Leave (グローバル Leave) メッセージを送信し、TCN イベント中のフラッディング モードからの回復を促します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	TCN の設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのクエリー送信要求に戻す場合は、**no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチは TCN を受信すると、一般クエリーを 2 つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッディングします。異なるマルチキャストグループのホストに接続しているポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損失が発生する可能性があります。その場合、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用して、この状態を制御できます。

インターフェイス上でマルチキャストフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no ip igmp snooping tcn flood	スパンニング ツリーの TCN イベント中に発生するマルチキャストトラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャストフラッディングはイネーブルです。
ステップ 4	exit	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping	TCN の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイス上でマルチキャストフラッディングを再度イネーブルにする場合、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定するときには、次の注意事項に従ってください。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。イネーブルになると、IGMP スヌーピング クエリアはクエリー送信元アドレスとして IP アドレスを使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) IP アドレス (存在する場合) を使用しようとします。SVI IP アドレスが存在しない場合、スイッチはスイッチ上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアはスイッチ上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャストルータの存在を検出すると、非クエリア ステートになります。

- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブルステートになります。
 - IGMP スヌーピングが VLAN でディセーブルの場合
 - PIM が、VLAN に対応する SVI でイネーブルの場合

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping querier	IGMP スヌーピング クエリア機能をイネーブルにします。
ステップ 3	ip igmp snooping querier address <i>ip_address</i>	(任意) IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用しようとします。 (注) IGMP スヌーピング クエリアはスイッチ上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
ステップ 4	ip igmp snooping querier query-interval <i>interval-count</i>	(任意) IGMP クエリアの間隔を設定します。指定できる範囲は 1 ~ 18000 秒です。
ステップ 5	ip igmp snooping querier tcn query [count <i>count interval interval]</i>	(任意) Topology Change Notification (TCN; トポロジ変更通知) クエリーの間隔を設定します。指定できる count の範囲は 1 ~ 10 です。指定できる interval 範囲は 1 ~ 255 秒です。
ステップ 6	ip igmp snooping querier timer expiry <i>timeout</i>	(任意) IGMP クエリアが期限切れになるまでの時間を設定します。指定できる範囲は 60 ~ 300 秒です。
ステップ 7	ip igmp snooping querier version <i>version</i>	(任意) クエリア機能が使用する IGMP バージョン番号 1 または 2 を選択します。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show ip igmp snooping vlan <i>vlan-id</i>	(任意) VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

次に、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

次に、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

IGMP レポート抑制のディセーブル化



(注)

IGMP レポート抑制がサポートされるのは、マルチキャスト クエリーが IGMPv1 および IGMPv2 レポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能はサポートされません。

IGMP レポート抑制はデフォルトでイネーブルです。IGMP レポート抑制がイネーブルの場合、スイッチは、マルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。

IGMP レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no ip igmp snooping report-suppression	IGMP レポート抑制をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP レポート抑制を再びイネーブルにする場合は、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

動的に学習された、あるいは静的に設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP アドレス マルチキャスト エントリを表示することもできます。

IGMP スヌーピング情報を表示するには、表 25-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 25-4 IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
<code>show ip igmp snooping [vlan <i>vlan-id</i>]</code>	<p>スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ip igmp snooping groups [count dynamic [count] user [count]]</code>	<p>スイッチまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • dynamic : IGMP スヌーピングによって学習されたエントリを表示します。 • user : ユーザによって設定されたマルチキャスト エントリだけを表示します。
<code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i> count dynamic [count] user[count]]</code>	<p>マルチキャスト VLAN またはその VLAN の特定のパラメータについて、マルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • vlan-id : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • dynamic : IGMP スヌーピングによって学習されたエントリを表示します。 • ip_address : 指定のグループ IP アドレスのマルチキャスト グループについて、特性を表示します。 • user : ユーザによって設定されたマルチキャスト エントリだけを表示します。
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	<p>動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。</p> <p>(注) IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p>
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>]</code>	<p>IP アドレス、および VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p>
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code>	<p>IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。</p>

各コマンドのキーワードおよびオプションの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

MVR の概要

MVR は、イーサネット リング ベースのサービス プロバイダー ネットワークにおいて、マルチキャスト トラフィックを大規模展開するアプリケーション（サービス プロバイダー ネットワークによる複数のテレビチャンネルのブロードキャストなど）を想定して開発されました。MVR によってポート上の加入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有できます。MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されません。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退（Join および Leave）を行うことが前提です。これらのメッセージは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作します。それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

スイッチの CPU は、MVR IP マルチキャストストリームとそれに対応するスイッチ転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホストメンバシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバー ポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアント ポートから転送されます。それ以外のポートからは転送されません。MVR ホストから受信した IGMP レポートも、スイッチのすべての MVR データ ポートから転送されます。したがって、互換モードでスイッチを稼働させた場合と異なり、MVR データ ポートリンクで不要な帯域幅を使用しなくすみます。

MVR に関与するのはレイヤ 2 ポートだけです。ポートを MVR レシーバー ポートとして設定する必要があります。各スイッチ スタックでサポートされる MVR マルチキャスト VLAN は、1 つのみです。

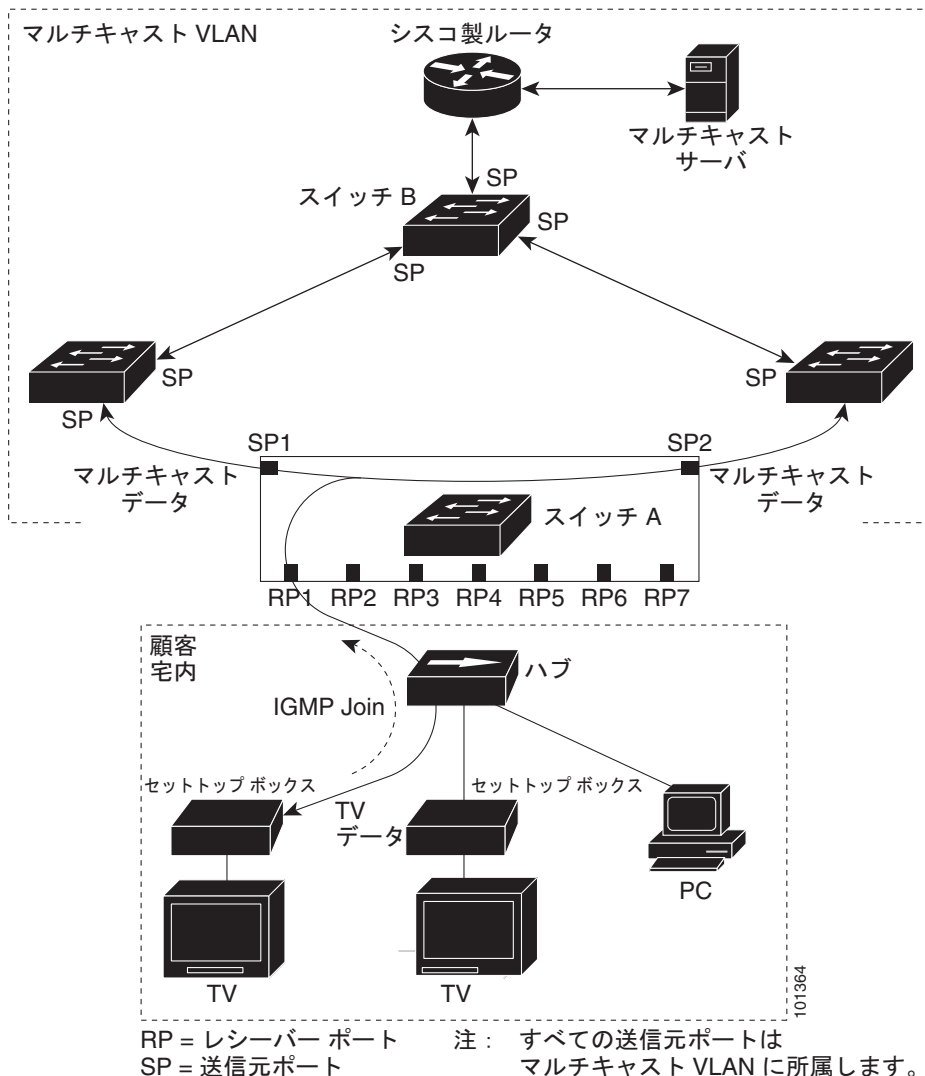
受信ポートおよび送信元ポートは、スイッチ スタック内のそれぞれ別のスイッチに設定できます。マルチキャスト VLAN で送信されるマルチキャスト データはスタック内のすべての MVR 受信ポートに転送されます。スタックに新規に追加されたスイッチには、デフォルトで受信ポートが設定されています。

スイッチに障害が発生するか、スタックから削除されると、このスイッチに属するレシーバー ポートだけがマルチキャスト データを受信しなくなります。その他のスイッチのその他のすべての受信ポートは、引き続きマルチキャスト データを受信します。

マルチキャスト TV アプリケーションで MVR を使用する場合

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマルチキャスト ストリームを受信できます。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR レシーバー ポートとして設定されたスイッチ ポートです。
 図 25-3 に構成例を示します。Dynamic Host Configuration Protocol (DHCP) はセットトップ ボックスまたは PC に IP アドレスを割り当てます。加入者がチャンネルを選択すると、セットトップ ボックスまたは PC からスイッチ A に、所定のマルチキャストに加入するための IGMP レポートが送信されます。IGMP レポートが設定されている IP マルチキャスト グループ アドレスの 1 つと一致すると、スイッチの CPU がハードウェア アドレス テーブルを変更して、指定のマルチキャスト ストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバー ポートと VLAN を追加します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを MVR 送信元ポートといいます。

図 25-3 MVR の例



加入者がチャンネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップボックスからマルチキャストストリームに対する IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバーポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、同じグループに加入している別のセットトップボックスがある場合、そのセットトップボックスはクエリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はそのグループの転送先としてのレシーバーポートを除外します。

即時脱退機能を使用しない場合、レシーバーポートの加入者から IGMP Leave メッセージを受信したスイッチは、そのポートに IGMP クエリーを送信し、IGMP グループメンバシップレポートを待ちます。設定された時間内にレポートが届かないと、レシーバーポートがマルチキャストグループメンバシップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバーポートから IGMP クエリーが送信されません。Leave メッセージの受信後ただちに、マルチキャストグループメンバシップからレシーバーポートが削除されるので、脱退のための待ち時間が短縮されます。即時脱退機能をイネーブルにするのは、接続されているレシーバーデバイスが 1 つだけのレシーバーポートに限定してください。

MVR を使用すると、VLAN ごとに加入者用のテレビチャンネルマルチキャストトラフィックを複製しなくて済みます。すべてのチャンネル用のマルチキャストトラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランク全体で 1 回送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN に送られます。これらのメッセージは、レイヤ 3 デバイス上（スイッチ B）のマルチキャスト VLAN のマルチキャストトラフィックストリームに対し、動的に登録します。アクセスレイヤスイッチ（スイッチ A）が転送動作を変更し、マルチキャスト VLAN から別個の VLAN 上の加入者ポートへトラフィックを転送できるようにするので、選択されたトラフィックが 2 つの VLAN 間を伝送されます。

IGMP レポートは、マルチキャストデータと同じ IP マルチキャストグループアドレスに送信されます。スイッチ A の CPU は、レシーバーポートから送られたすべての IGMP Join および Leave メッセージを取り込み、MVR モードに基づいて、送信元（アップリンク）ポートのマルチキャスト VLAN に転送しなければなりません。

MVR の設定

ここでは、次の設定情報について説明します。

- 「MVR のデフォルト設定」(P.25-20)
- 「MVR 設定時の注意事項および制限事項」(P.25-21)
- 「MVR グローバルパラメータの設定」(P.25-21)
- 「MVR インターフェイスの設定」(P.25-23)

MVR のデフォルト設定

表 25-5 に、MVR のデフォルト設定を示します。

表 25-5 MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャストアドレス	未設定
クエリーの応答時間	0.5 秒

表 25-5 MVR のデフォルト設定 (続き)

機能	デフォルト設定
マルチキャスト VLAN	VLAN 1
モード	compatible
インターフェイスのデフォルト (ポート単位)	レシーバー ポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

MVR を設定するときには、次の注意事項に従ってください。

- レシーバー ポートはアクセス ポートでなければなりません。トランク ポートにすることはできません。スイッチ上のレシーバー ポートは、異なる VLAN に所属していてもかまいませんが、マルチキャスト VLAN には所属させないでください。
- スイッチ上で設定できるマルチキャスト エントリ (MVR グループアドレス) の最大数 (受信できるテレビ チャンネルの最大数) は 256 です。
- 送信元 VLAN で受信され、レシーバー ポートから脱退する MVR マルチキャスト データは、スイッチで Time to Live (TTL) が 1 だけ少なくなります。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するので、スイッチ上でエイリアスの IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと相互運用している場合は、相互間でエイリアスとなる、または予約済みの IP マルチキャスト アドレス (224.0.0.xxx の範囲) を使用して IP アドレスを設定しないでください。
- プライベート VLAN に MVR を設定しないでください。
- スイッチ上でマルチキャスト ルーティングがイネーブルの場合、MVR はサポートされません。MVR がイネーブルの場合に、マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されません。マルチキャスト ルーティングおよびマルチキャスト ルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとする、MVR をイネーブルにする操作が取り消され、エラー メッセージが表示されます。
- MVR はスイッチ上で IGMP スヌーピングと共存できます。
- MVR レシーバー ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。

MVR グローバル パラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合には (MVR VLAN 以外)、最初に MVR をイネーブルにする必要があります。



(注)

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mvr</code>	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	<code>mvr group ip-address [count]</code>	スイッチ上で IP マルチキャスト アドレスを設定するか、または <i>count</i> パラメータを使用して、連続する MVR グループ アドレスを設定します (<i>count</i> の範囲は 1 ~ 256、デフォルトは 1)。このアドレスに送信されたマルチキャスト データは、スイッチ上のすべての送信元ポートおよびそのマルチキャスト アドレスのデータを受信するために選ばれたすべてのレシーバー ポートに送信されます。マルチキャスト アドレスとテレビ チャネルは 1 対 1 の対応です。
ステップ 4	<code>mvr querytime value</code>	(任意) マルチキャスト グループ メンバシップからポートを削除する前に、レシーバー ポートで IGMP レポートのメンバシップを待機する最大時間を設定します。この値は 10 分の 1 秒単位で設定します。範囲は 1 ~ 100、デフォルトは 10 分の 5 秒、すなわち 0.5 秒です。
ステップ 5	<code>mvr vlan vlan-id</code>	(任意) マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートをこの VLAN に所属させる必要があります。VLAN の範囲は 1 ~ 1001 および 1006 ~ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	<code>mvr mode {dynamic compatible}</code>	(任意) MVR の動作モードを指定します。 <ul style="list-style-type: none"> • dynamic : 送信元ポートでダイナミック MVR メンバシップを使用できます。 • compatible : Catalyst 3500 XL スイッチおよび Catalyst 2900 XL スイッチとの互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。 デフォルトは compatible モードです。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show mvr</code> または <code>show mvr members</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルトの設定に戻すには、`no mvr [mode | group ip-address | querytime | vlan]` グローバル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにして、MVR グループ アドレスを設定し、クエリー タイムを 1 秒 (10 分の 10 秒) に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナミックに設定する例を示します。

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

`show mvr members` 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mvr</code>	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	<code>interface interface-id</code>	設定するレイヤ 2 ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>mvr type {source receiver}</code>	<p>MVR ポートを次のいずれかに設定します。</p> <ul style="list-style-type: none"> source : マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。 receiver : 加入者ポートであり、マルチキャスト データを受信するだけの場合、レシーバー ポートとしてポートを設定します。静的に、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。レシーバー ポートをマルチキャスト VLAN に所属させることはできません。 <p>デフォルトでは、非 MVR ポートとして設定されます。非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。</p>
ステップ 5	<code>mvr vlan vlan-id group [ip-address]</code>	<p>(任意) マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。グループ メンバーとして静的に設定されたポートは、静的に削除されないかぎり、グループ メンバーのままです。</p> <p>(注) 互換モードでは、このコマンドが適用されるのはレシーバー ポートだけです。ダイナミック モードでは、レシーバー ポートおよび送信元ポートに適用されます。</p> <p>レシーバー ポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャスト グループに動的に加入することもできます。</p>
ステップ 6	<code>mvr immediate</code>	<p>(任意) ポート上で MVR の即時脱退機能をイネーブルにします。</p> <p>(注) このコマンドが適用されるのは、レシーバー ポートだけです。また、イネーブルにするのは、単一のレシーバー デバイスが接続されているレシーバー ポートに限定してください。</p>
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show mvr</code> <code>show mvr interface</code> または <code>show mvr members</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの設定に戻すには、`no mvr [type | immediate | vlan vlan-id | group]` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをレシーバーポートとして設定し、マルチキャストグループアドレスに送信されたマルチキャストトラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port      Type          Status          Immediate Leave
----      -
Gil1/0/2  RECEIVER     ACTIVE/DOWN    ENABLED
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR の設定を表示するには、特権 EXEC モードで表 25-6 のコマンドを使用します。

表 25-6 MVR 情報を表示するためのコマンド

コマンド	目的
<code>show mvr</code>	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまたはディセーブルの判別、マルチキャスト VLAN、マルチキャストグループの最大数 (256) および現在の数 (0 ~ 256)、クエリーの応答時間、および MVR モードです。
<code>show mvr interface [interface-id] [members [vlan vlan-id]]</code>	すべての MVR インターフェイスおよびそれぞれの MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。 <ul style="list-style-type: none"> Type : RECEIVER (レシーバー) または SOURCE (送信元) Status : 次のいずれか 1 つ <ul style="list-style-type: none"> ACTIVE は、ポートが VLAN に含まれていることを意味します。 UP/DOWN は、ポートが転送中または転送中ではないことを示します。 INACTIVE は、ポートが VLAN に含まれていないことを意味します。 Immediate Leave (即時脱退機能) - イネーブルまたはディセーブル members キーワードを入力すると、そのポート上のすべてのマルチキャストグループメンバーが表示されます。VLAN ID を入力した場合は、VLAN 上のすべてのマルチキャストグループメンバーが表示されます。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show mvr members [ip-address]</code>	すべての IP マルチキャストグループまたは指定した IP マルチキャストグループ IP アドレスに含まれているレシーバーポートおよび送信元ポートがすべて表示されます。

IGMP フィルタリングおよびスロットリングの設定

都市部や Multiple-Dwelling Unit (MDU; 集合住宅) などの環境では、スイッチポート上のユーザが属する一連のマルチキャストグループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャストサービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャストグループの数を、スイッチポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャストプロファイルを設定し、それらを各スイッチポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャストグループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャストグループへのアクセスを拒否する IGMP プロファイルがスイッチポートに適用されると、IP マルチキャストトラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャストトラフィックを受信できなくなります。マルチキャストグループへのアクセスがフィルタリングアクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバシップレポート (Join および Leave レポートを含む) だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャストトラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャストトラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャストグループアドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャストエントリを上書きします。



(注)

IGMP フィルタリングが実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

ここでは、次の設定情報について説明します。

- 「IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定」(P.25-26)
- 「IGMP プロファイルの設定」(P.25-26) (任意)
- 「IGMP プロファイルの適用」(P.25-27) (任意)
- 「IGMP グループの最大数の設定」(P.25-28) (任意)
- 「IGMP スロットリングアクションの設定」(P.25-29) (任意)

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

表 25-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 25-7 IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用されない
IGMP グループの最大数	最大数は設定されない
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

転送テーブルに登録されているグループが最大数に達しているとき、デフォルトの IGMP スロットリング アクションは IGMP レポートを拒否します。設定時の注意事項については、「[IGMP スロットリング アクションの設定](#)」(P.25-29) を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、`ip igmp profile` グローバル コンフィギュレーション コマンドおよびプロファイル番号を使用して、IGMP プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始します。ポートから送信される IGMP Join 要求をフィルタリングするために使用される IGMP プロファイルのパラメータは、このモードから指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用して、プロファイルを作成できます。

- **deny** : 一致するアドレスを拒否します。デフォルトで設定されています。
- **exit** : IGMP プロファイル コンフィギュレーション モードを終了します。
- **no** : コマンドを否定するか、または設定をデフォルトに戻します。
- **permit** : 一致するアドレスを許可します。
- **range** : プロファイルの IP アドレス範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。

デフォルトでは、スイッチには IGMP プロファイルが設定されていません。プロファイルが設定されており、**permit** および **deny** キーワードがいずれも指定されていない場合、デフォルトでは、IP アドレス範囲へのアクセスが拒否されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp profile profile number</code>	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。プロファイル番号の範囲は 1 ~ 4294967295 です。
ステップ 3	<code>permit deny</code>	(任意) IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。

コマンド	目的
ステップ 4 range ip multicast address	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 range コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show ip igmp profile profile number	プロファイルの設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range ip multicast address** IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否 (デフォルト) である場合は、**show ip igmp profile** の出力には表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して、該当するインターフェイスにプロファイルを適用します。IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。EtherChannel ポート グループに所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 3 ip igmp filter profile number	指定された IGMP プロファイルをインターフェイスに適用します。指定できる範囲は 1 ~ 4294967295 です。
ステップ 4 end	特権 EXEC モードに戻ります。

IGMP フィルタリングおよびスロットリングの設定

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

インターフェイスからプロファイルを削除するには、`no ip igmp filter profile number` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの最大数の設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、`ip igmp max-groups` インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト設定 (制限なし) に戻すには、このコマンドの `no` 形式を使用します。

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。また、このコマンドを論理 EtherChannel インターフェイスでも使用することはできますが、EtherChannel ポート グループに属するポート上では、使用できません。

転送テーブルの IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 3	<code>ip igmp max-groups number</code>	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ~ 4294967294 です。デフォルトでは最大数は設定されません。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

グループの最大数に関する制限を削除し、デフォルト設定 (制限なし) に戻すには、`no ip igmp max-groups` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定したあと、**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドを使用して受信した IGMP レポートの新しいグループで、既存のグループを上書きします。IGMP Join レポートを廃棄するデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

IGMP スロットリングを設定するときには、次の注意事項に従ってください。

- この制限事項は、レイヤ 2 ポートのみにも適用されます。このコマンドは、論理 EtherChannel インターフェイスでは使用できませんが、EtherChannel ポート グループに属するポートでは使用できません。
- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action {deny | replace}** コマンドを入力しても効果はありません。
- インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリング アクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。
 - スロットリング アクションを **deny** に設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、スイッチは、インターフェイスで受信した次の IGMP レポートを廃棄します。
 - スロットリング アクションを **replace** に設定すると、すでに転送テーブルに登録されていたエントリは削除されます。フォワーディング テーブルのエントリが最大数まで達したら、スイッチはランダムに選択したエントリを受信した IGMP レポートで上書きします。

スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、**IGMP スロットリング アクション**を設定します。

転送テーブルに最大数のエントリが登録されているときにスロットリング アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 3	ip igmp max-groups action {deny replace}	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 <ul style="list-style-type: none"> • deny : レポートを廃棄します。 • replace : 既存のグループを、IGMP レポートを受信した新しいグループで上書きします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

■ IGMP フィルタリングおよび IGMP スロットリング設定の表示

レポートの廃棄というデフォルトのアクションに戻すには、`no ip igmp max-groups action` インターフェイス コンフィギュレーション コマンドを使用します。

IGMP フィルタリングおよび IGMP スロットリング設定の表示

IGMP プロファイルの特性を表示したり、スイッチ上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。また、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 25-8 の特権 EXEC コマンドを使用して、IGMP フィルタリングおよび IGMP スロットリングの設定を表示します。

表 25-8 IGMP フィルタリングおよび IGMP スロットリングの設定を表示するためのコマンド

コマンド	目的
<code>show ip igmp profile [profile number]</code>	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
<code>show running-config [interface interface-id]</code>	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはスイッチ上のすべてのインターフェイスの設定を表示します。



CHAPTER 26

ポート単位のトラフィック制御の設定

この章では、Catalyst 3750 スイッチにポートベースのトラフィック制御機能を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「ストーム制御の設定」(P.26-1)
- 「保護ポートの設定」(P.26-6)
- 「ポート ブロッキングの設定」(P.26-7)
- 「ポート セキュリティの設定」(P.26-9)
- 「ポート単位のトラフィック制御設定の表示」(P.26-21)

ストーム制御の設定

ここでは、次の概念と設定情報について説明します。

- 「ストーム制御の概要」(P.26-1)
- 「ストーム制御のデフォルト設定」(P.26-3)
- 「ストーム制御およびしきい値レベルの設定」(P.26-3)
- 「小さいフレームの着信レートの設定」(P.26-5)

ストーム制御の概要

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、ユニキャスト）のトラフィック レート。
- ビット単位で受信するパケット（ブロードキャスト、マルチキャスト、ユニキャスト）のトラフィック レート。
- 秒単位で受信するパケットおよび小さいフレームのトラフィック レート。この機能は、グローバルでイネーブルに設定されています。小さいフレームのしきい値は、インターフェイスごとに設定します

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らないかぎり、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らないかぎり、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

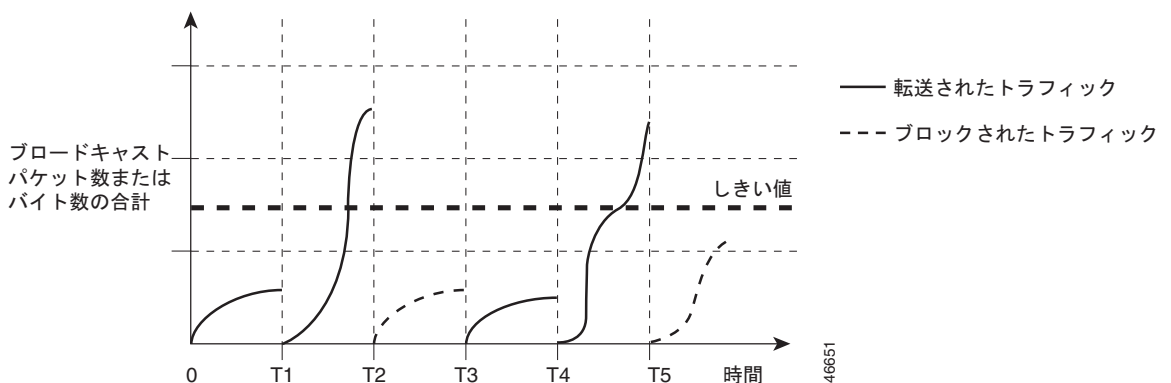


(注)

マルチキャスト トラフィックのストーム制御しきい値に達した場合、Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) フレーム、Cisco Discovery Protocol (CDP) フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティングアップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図 26-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも当てはまります。この例では、T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべて廃棄されます。したがって、T2 と T5 のあとのインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らないかぎり、ブロードキャスト トラフィックが再び転送されます。

図 26-1 ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせると、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過するパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。



(注)

パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、ユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はスイッチ インターフェイス上でディセーブルになります。したがって、抑制レベルは 100% です。

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数パーセントの差異が生じる可能性があります。



(注)

ストーム制御は、物理インターフェイス上でサポートされます。また、EtherChannel 上でもストーム制御を設定できます。ストーム制御が EtherChannel に設定されている場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

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

コマンド	目的
ステップ 3 <code>storm-control {broadcast multicast unicast} level {level [level-low] bps bps [bps-low] pps pps [pps-low]}</code>	<p>ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ~ 100.00 です。 • (任意) <i>level-low</i> には、下限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。この値は上限抑制レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定していない場合、上限抑制レベルと同じ値が設定されます。指定できる範囲は 0.00 ~ 100.00 です。 <p>しきい値に最大値 (100%) を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。</p> <ul style="list-style-type: none"> • <i>bps bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 • (任意) <i>bps-low</i> には、下限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値 レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 • <i>pps pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 • (任意) <i>pps-low</i> には、下限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値 レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。</p>
ステップ 4 <code>storm-control action {shutdown trap}</code>	<p>ストームが検出された場合に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。</p> <ul style="list-style-type: none"> • ストーム中、ポートを <code>error-disable</code> の状態にするには、<code>shutdown</code> キーワードを選択します。 • ストームが検出された場合、SNMP (簡易ネットワーク管理プロトコル) トラップを生成するには、<code>trap</code> キーワードを選択します。

コマンド	目的
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show storm-control [<i>interface-id</i>] [broadcast multicast unicast]	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、**no storm-control {broadcast | multicast | unicast} level** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で、上限抑制レベルを 87%、下限抑制レベルを 65% に設定し、ユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポート上で、ブロードキャスト アドレスのストーム制御を 20% のレベルでイネーブルにする例を示します。ブロードキャスト トラフィックが、トラフィック ストーム制御インターバル内にポートで使用できる総帯域幅のうち、設定された 20% のレベルを超えた場合、トラフィック ストーム制御インターバルが終わるまで、スイッチはすべてのブロードキャスト トラフィックを廃棄します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# storm-control broadcast level 20
```

小さいフレームの着信レートの設定

67 バイトより小さい着信 VLAN タグ付きパケットは、小さいフレームと見なされます。スイッチは小さいフレームを転送しますが、スイッチのストーム制御カウンタの増分対象ではありません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが特定のレート（しきい値）で着信した場合にポートを **errdisable** にするよう設定できます。

小さいフレームの着信機能をスイッチ上でグローバルでイネーブルにしてから、各インターフェイスのパケットについて小さいフレームのしきい値を設定します。特定のレート（しきい値）で到着する、最小サイズより小さいパケットは、ポートが **errdisable** であるために廃棄されます。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを入力すると、特定の時間が経過したあとにポートは再びイネーブルになります（回復時間を設定するには、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します）。

各インターフェイスのしきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 errdisable detect cause small-frame	小さいフレームの着信レート機能をスイッチでイネーブルにします。
ステップ 3 errdisable recovery interval interval	(任意) 特定の errdisable ステートから回復する時間を指定します。
ステップ 4 errdisable recovery cause small-frame	(任意) 小さいフレームの着信により errdisable となったポートが自動的に再びイネーブルになるまでの回復時間を設定します。

	コマンド	目的
ステップ 5	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	<code>small violation-rate pps</code>	インターフェイスに、着信パケットを廃棄してポートを <code>errdisable</code> にするしきい値レートを設定します。指定できる範囲は 1 ~ 10,000 パケット/秒 (pps) です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show interfaces interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、小さいフレームの着信レート機能をイネーブルにして、ポートの回復時間を設定し、ポートを `errdisable` にするしきい値を設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

保護ポートの設定

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートである他のポートに、トラフィック（ユニキャスト、マルチキャスト、またはブロードキャスト）をすべて転送するわけではありません。レイヤ 2 では、保護ポート間でデータ トラフィックを転送できません。CPU で処理されてソフトウェアで転送される、Protocol Independent Multicast (PIM) パケットのような制御トラフィックだけが転送されます。保護ポート間を通過するトラフィックはすべて、レイヤ 3 デバイスを介して転送しなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチ スタックは単一の論理スイッチを表すため、スイッチ スタック内の保護ポート間では、これらのポートがスタック内の同じスイッチ上にあるか、異なるスイッチ上にあるかに関係なく、レイヤ 2 トラフィックは転送されません。

ここでは、次の設定情報について説明します。

- 「保護ポートのデフォルト設定」(P.26-6)
- 「保護ポート設定時の注意事項」(P.26-7)
- 「保護ポートの設定」(P.26-7)

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポート設定時の注意事項

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャンネルで保護ポートをイネーブルにした場合は、そのポート チャンネル グループ内のすべてのポートでイネーブルになります。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、第 17 章「[プライベート VLAN の設定](#)」を参照してください。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport protected</code>	インターフェイスを保護ポートに設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、`no switchport protected` インターフェイス コンフィギュレーション コマンドを使用します。

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、スイッチは未知の宛先 MAC（メディア アクセス制御）アドレスが指定されたパケットをすべてのポートからフラッドします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッドされないようにします。



(注)

マルチキャスト トラフィックの場合、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダー内に IPv4 または IPv6 情報が含まれるマルチキャスト パケットはブロックしません。

ここでは、次の設定情報について説明します。

- ・「ポートブロッキングのデフォルト設定」(P.26-8)
- ・「インターフェイスでのフラッディングトラフィックのブロッキング」(P.26-8)

ポートブロッキングのデフォルト設定

デフォルトでは、ポートから未知のマルチキャストおよびユニキャストトラフィックのフラッディングがブロックされず、すべてのポートにこのようなパケットがフラッディングされます。

インターフェイスでのフラッディングトラフィックのブロッキング



(注)

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポートチャンネルのマルチキャストまたはユニキャストトラフィックをブロックすると、ポートチャンネルグループのすべてのポートでブロックされます。

インターフェイスからのユニキャストパケットおよびレイヤ 2 マルチキャストパケットのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport block multicast</code>	ポートからの未知のマルチキャストの転送をブロックします。 (注) 純粋なレイヤ 2 マルチキャストトラフィックだけをブロックします。ヘッダー内に IPv4 または IPv6 情報が含まれるマルチキャストパケットはブロックしません。
ステップ 4	<code>switchport block unicast</code>	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でトラフィックがブロックされずに、通常の転送が行われるデフォルトの状態にインターフェイスを戻すには、`no switchport block {multicast | unicast}` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のユニキャストおよびレイヤ 2 マルチキャストフラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポートセキュリティの設定

ポートセキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュアポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレスグループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュアポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュアポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュアポートにアクセスしようとしたときにも、違反のフラグが立てられます。

ここでは、次の概念と設定情報について説明します。

- 「ポートセキュリティの概要」(P.26-9)
- 「ポートセキュリティのデフォルト設定」(P.26-11)
- 「ポートセキュリティの設定時の注意事項」(P.26-12)
- 「ポートセキュリティのイネーブル化および設定」(P.26-13)
- 「ポートセキュリティ エージングのイネーブル化および設定」(P.26-18)
- 「ポートセキュリティおよびスイッチ スタック」(P.26-20)
- 「ポートセキュリティおよびプライベート VLAN」(P.26-20)

ポートセキュリティの概要

ここでは、次の概要について説明します。

- 「セキュア MAC アドレス」(P.26-9)
- 「セキュリティ違反」(P.26-10)

セキュア MAC アドレス

ポートで許可されるセキュアアドレスの最大数を設定するには、**switchport port-security maximum value** インターフェイス コンフィギュレーション コマンドを使用します。



(注)

最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス : **switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス : 動的に設定されてアドレス テーブルだけに保存され、スイッチの再起動時に削除されます。

- スティッキーセキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。スティッキー ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはスティッキー ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的に反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキー セキュア アドレスが保存されていない場合、アドレスは失われます。

スティッキー ラーニングをディセーブルにした場合、スティッキー セキュア MAC アドレスはダイナミック セキュア MAC アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな Switch Database Management (SDM; スイッチ データベース管理) テンプレートによって決まります。第 8 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数です。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合

違反が発生した場合の対処に基づいて、次の 4 つの違反モードのいずれかをインターフェイスに設定できます。

- **protect** (保護)：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさなにかぎり、未知の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が発生したことは通知されません。



(注) トランク ポートに **protect** 違反モードを設定することは推奨しません。protect モードの場合、ポートが最大限度に達していなくてもいずれかの VLAN が最大限度に達すると、ラーニングをディセーブルにします。

- **restrict** (制限)：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさなにかぎり、未知の送信元アドレスを持つパケットは廃棄されます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。

- **shutdown** (シャットダウン) : ポートセキュリティ違反により、インターフェイスが **errdisable** になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。SNMP トラップが送信されて **Syslog** メッセージがログされ、違反カウンタが増加します。セキュアポートが **errdisable** ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。これがデフォルトのモードです。
- **shutdown vlan** (VLAN シャットダウン) : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が **errdisable** になります。

表 26-1 に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 26-1 セキュリティ違反モードの処置

違反モード	トラフィックの転送 ¹	SNMP トラップの送信	Syslog メッセージの送信	エラーメッセージの表示 ²	違反カウンタの増加	ポートのシャットダウン
protect	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり
shutdown vlan	なし	あり	あり	なし	あり	なし ³

1. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットが廃棄されます。
2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラーメッセージを返します。
3. 違反が発生した VLAN だけがシャットダウンします。

ポートセキュリティのデフォルト設定

表 26-2 に、インターフェイスに対するポートセキュリティのデフォルト設定を示します。

表 26-2 ポートセキュリティのデフォルト設定

機能	デフォルト設定
ポートセキュリティ	ポート上でディセーブル。
スティッキー アドレス ラーニング	ディセーブル。
ポートあたりのセキュア MAC アドレスの最大数	1
違反モード	shutdown (シャットダウン)。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブル。エージング タイムは 0。 スタティック エージングはディセーブル。 タイプは absolute。

ポートセキュリティの設定時の注意事項

ポートセキュリティを設定するときには、次の注意事項に従ってください。

- ポートセキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートを Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) の宛先ポートにすることはできません。
- セキュア ポートは、Fast EtherChannel やギガビット EtherChannel ポート グループに属することができません。



(注) 音声 VLAN はアクセス ポートだけでサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN も設定されているインターフェイスでポートセキュリティをイネーブルにする際には、ポート上で許可されるセキュアアドレスの最大数を 2 に設定します。ポートを Cisco IP Phone に接続している場合、IP Phone に MAC アドレスが 1 つ必要になります。Cisco IP Phone アドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 つの PC を Cisco IP Phone に接続する場合、追加の MAC アドレスは不要です。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュアアドレスを設定する必要があります。
- トランク ポートが、ポートセキュリティを設定され、データトラフィックについてはアクセス VLAN に、音声トラフィックについては音声 VLAN に割り当てられている場合、**switchport voice** および **switchport priority extend** インターフェイス コンフィギュレーション コマンドを入力しても効果はありません。
接続されたデバイスが同じ MAC アドレスを使用して、最初にアクセス VLAN の IP アドレスを要求し、次に音声 VLAN の IP アドレスを要求すると、アクセス VLAN だけに IP アドレスが割り当てられます。
- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって書き換えられます。新しい値が以前の値より小さく、インターフェイス上ですでに設定されているセキュアアドレスの数が新しい値を上回る場合は、コマンドが拒否されます。
- スイッチは、スティッキーセキュア MAC アドレスのポートセキュリティ エージングをサポートしていません。

表 26-3 に、他のポートベース機能と互換性のあるポートセキュリティについてまとめます。

表 26-3 他のスイッチ機能とポートセキュリティとの互換性

ポートタイプまたはポートの機能	ポートセキュリティとの互換性
DTP ¹ ポート ²	なし
トランク ポート	あり
ダイナミック アクセス ポート ³	なし
ルーテッド ポート	なし
SPAN 送信元ポート	あり
SPAN 宛先ポート	なし
EtherChannel	なし
トンネリング ポート	あり

表 26-3 他のスイッチ機能とポートセキュリティとの互換性 (続き)

ポートタイプまたはポートの機能	ポートセキュリティとの互換性
保護ポート	あり
IEEE 802.1X ポート	あり
音声 VLAN ポート ⁴	あり
プライベート VLAN ポート	あり
IP ソース ガード	あり
ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査	あり
Flex Link	あり

1. DTP = Dynamic Trunking Protocol
2. **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート。
3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol (VQP) ポート。
4. ポートに最大限可能なセキュアなアドレスを設定します (アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数)。

ポートセキュリティのイネーブル化および設定

ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 switchport mode {access trunk}	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード (dynamic auto) のインターフェイスは、セキュアポートとして設定できません。
ステップ 4 switchport voice vlan vlan-id	ポート上で音声 VLAN をイネーブルにします。 <i>vlan-id</i> : 音声トラフィックに使用する VLAN を指定します。
ステップ 5 switchport port-security	インターフェイス上でポートセキュリティをイネーブルにします。

コマンド	目的
ステップ 6 <code>switchport port-security</code> <code>[maximum value [vlan {vlan-list </code> <code>{access voice}}]]</code>	<p>(任意) インターフェイスに対するセキュア MAC アドレスの最大数を設定します。スイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって決まります。第 8 章「スイッチ SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> • vlan-list : トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。指定されなかった VLAN には、VLAN 単位の最大値が使用されます。 • access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合に限り有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>

コマンド	目的
ステップ 7 <code>switchport port-security [violation {protect restrict shutdown shutdown vlan}]</code>	<p>(任意) 違反モード、つまりセキュリティ違反が検出されたときの対応を、次のいずれかに設定します。</p> <ul style="list-style-type: none"> protect (保護) : ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が発生したことは通知されません。 <p>(注) トランク ポートに protect モードを設定することは推奨しません。protect モードの場合、ポートが最大限度に達していなくてもいずれかの VLAN が最大限度に達すると、ラーニングをディセーブルにします。</p> <ul style="list-style-type: none"> restrict : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。 shutdown : 違反が発生すると、インターフェイスが errdisable になり、ポートの LED が消灯します。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。 shutdown vlan : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。 <p>(注) セキュア ポートが errdisable ステートになった場合は、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力して、このステートを解除します。手動で再びイネーブルにするには、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力するか、clear errdisable interface vlan 特権 EXEC コマンドを入力します。</p>

コマンド	目的
ステップ 8 switchport port-security [mac-address mac-address [vlan {vlan-id {access voice}}]	<p>(任意) インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。</p> <p>(注) このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> • vlan-id : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合に限り有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
ステップ 9 switchport port-security mac-address sticky	<p>(任意) インターフェイスでスティッキー ラーニングをイネーブルにします。</p>
ステップ 10 switchport port-security mac-address sticky [mac-address vlan {vlan-id {access voice}}]	<p>(任意) スティッキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p>(注) このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。</p> <p>(任意) vlan : VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> • vlan-id : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • access : アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • voice : アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p>(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合に限り有効です。</p>
ステップ 11 end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	show port-security	設定を確認します。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

セキュア ポートではないデフォルトの状態にインターフェイスを戻す場合は、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。スティッキー ラーニングがイネーブルの状態でのこのコマンドを入力すると、スティッキー セキュア アドレスが実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。ここですべてのアドレスが動的に学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻す場合は、**no switchport port-security maximum value** インターフェイス コンフィギュレーション コマンドを使用します。違反モードをデフォルト状態 (shutdown モード) に戻す場合は、**no switchport port-security violation {protocol | restrict}** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでスティッキー ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスがスティッキー セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、スティッキー MAC アドレスによる設定を保存した場合、**no switchport port-security mac-address sticky** コマンドの入力後に設定をもう一度保存しないと、スイッチの再起動時にスティッキー アドレスが復元されます。

MAC アドレス テーブルからスイッチまたはインターフェイス上のセキュア アドレスすべてまたは特定 (設定、ダイナミック、スティッキー) のセキュア アドレスすべてを削除するには、**clear port-security {all | configured | dynamic | sticky}** 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイス上のすべてのダイナミック セキュア アドレスをアドレス テーブルから削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドのあとに、(インターフェイスでポート セキュリティを再びイネーブルにするために) **switchport port-security** コマンドを入力します。**no switchport port-security** コマンドを使用する前に、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用してスティッキー セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換した場合、手動で設定されたものを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

設定済みのセキュア MAC アドレスをアドレス テーブルから明確に削除する場合、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用しなければなりません。

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポートのスティッキー ポートセキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します (データ VLAN に 10、音声 VLAN に 10 を割り当てます)。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポートセキュリティ エージングのイネーブル化および設定

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポートセキュリティ エージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- **absolute** : 指定されたエージング タイムの経過後に、ポート上のセキュア アドレスが削除されます。
- **inactivity** : 指定されたエージング タイムの間、セキュア アドレスが非アクティブであった場合に限り、ポート上のセキュア アドレスが削除されます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポート上のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュア アドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

ポートセキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

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

コマンド	目的
ステップ 3 switchport port-security aging {static time time type {absolute inactivity}}	<p>セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。</p> <p>(注) スイッチは、スタティック セキュア アドレスのポートセキュリティ エージングをサポートしていません。</p> <p>このポートでスタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、static を入力します。</p> <p><i>time</i> には、このポートのエージング タイムを指定します。指定できる範囲は、0 ~ 1440 分です。</p> <p>type には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • absolute : エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した <i>time</i> (分単位) が経過すると期限切れになり、セキュア アドレス リストから削除されます。 • inactivity : エージング タイプを非アクティブ エージングとして設定します。指定された <i>time</i> 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスが期限切れになります。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show port-security [interface interface-id] [address]	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上のすべてのセキュア アドレスに対してポートセキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** インターフェイス コンフィギュレーション コマンドを使用します。静的に設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上のセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスに対して、エージングをイネーブルにし、非アクティブ エージング タイプのエージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

上記のコマンドを確認するには、**show port-security interface interface-id** 特権 EXEC コマンドを使用します。

ポートセキュリティおよびスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュアアドレスを受け取ります。新規スタックメンバーは、他のスタックメンバーからすべてのダイナミックセキュアアドレスをダウンロードします。

スイッチ（スタック マスターまたはスタック メンバーのいずれか）がスタックから脱退すると、残りのスタックメンバーに通知されて、そのスイッチによって設定または学習されたセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

ポートセキュリティおよびプライベート VLAN

管理者はポートセキュリティを使用して、ポートで学習する MAC アドレスの数を制限したり、ポートで学習可能な MAC アドレスを指定したりできます。

PVLAN ホストおよび混合モード ポート上でポートセキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode private-vlan {host promiscuous}</code>	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	<code>switchport port-security</code>	インターフェイス上でポートセキュリティをイネーブルにします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show port-security [interface interface-id] [address]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```



(注)

ポートセキュリティとプライベート VLAN の両方が設定されたポートを、セキュア PVLAN ポートと呼びます。セキュア PVLAN ポートでセキュアアドレスを学習すると、同一のプライマリ VLAN に属する他のセキュア PVLAN ポートで同じセキュアアドレスを学習できません。ただし、非セキュア PVLAN ポートで学習したアドレスは、同一プライマリ VLAN に属するセキュア PVLAN で学習できます。

ホスト ポートで学習したセキュアアドレスは、関連するプライマリ VLAN で自動的に複製されます。同様に、混合ポートで学習したセキュアアドレスは、すべての関連するセカンダリ VLAN で自動的に複製されます。ユーザがスタティック アドレス (`mac-address-table static` コマンドを使用) をセキュア ポートに設定することはできません。

ポート単位のトラフィック制御設定の表示

show interfaces *interface-id* switchport 特権 EXEC コマンドを使用すると、(他の特性の中から) インターフェイスのトラフィックの抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、ストーム制御およびポートセキュリティの設定が表示されます。

トラフィックの制御情報を表示するには、表 26-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 26-4 トラフィック制御ステータスおよび設定を表示するためのコマンド

コマンド	目的
show interfaces [<i>interface-id</i>] switchport	すべてのスイッチング (非ルーティング) ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポートブロッキングおよびポート保護の設定を含めて表示します。
show storm-control [<i>interface-id</i>] [broadcast multicast unicast]	すべてのインターフェイスまたは指定されたインターフェイスに設定されているストーム制御抑制レベルを、指定されたトラフィックタイプについて、またはブロードキャストトラフィック (トラフィックタイプが入力されていない場合) について表示します。
show port-security [interface <i>interface-id</i>]	スイッチまたは指定されたインターフェイスのポートセキュリティ設定を、各インターフェイスで許容されるセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [interface <i>interface-id</i>] address	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface <i>interface-id</i> vlan	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。

■ ポート単位のトラフィック制御設定の表示



CHAPTER 27

CDP の設定

この章では、Catalyst 3750 スイッチに Cisco Discovery Protocol (CDP) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチスタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 の「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

- 「CDP の概要」 (P.27-1)
- 「CDP の設定」 (P.27-2)
- 「CDP のモニタおよびメンテナンス」 (P.27-5)

CDP の概要

CDP はすべてのシスコ製デバイス（ルータ、ブリッジ、アクセスサーバ、およびスイッチ）のレイヤ 2（データリンクレイヤ）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスに近接しているシスコ製デバイスを検出できます。また、下位レイヤのトランスペアレントプロトコルが稼動している近接デバイスのデバイスタイプや、SNMP（簡易ネットワーク管理プロトコル）エージェントアドレスを学習することもできます。この機能によって、アプリケーションから近接デバイスに SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol (SNAP) をサポートしているすべてのメディアで動作します。CDP はデータリンクレイヤだけで動作するため、異なるネットワークレイヤプロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す Time To Live (TTL)、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、近接デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタメンバー、およびコマンドスイッチから最大 3 台（デフォルト）離れたクラスタ対応の他のデバイスについての情報を維持します。

スイッチは CDP バージョン 2 をサポートします。

CDP およびスイッチ スタック

スイッチ スタックは、ネットワーク内で 1 つのスイッチと見なされます。したがって、CDP は個々のスタック メンバーではなく、スイッチ スタックを検出します。スタック メンバーの追加または削除などが行われて、スイッチ スタック メンバシップが変更されると、スイッチ スタックは近接ネットワーク デバイスに CDP メッセージを送信します。

CDP の設定

ここでは、次の設定情報について説明します。

- 「CDP のデフォルト設定」 (P.27-2)
- 「CDP の特性の設定」 (P.27-2)
- 「CDP のディセーブル化およびイネーブル化」 (P.27-3)
- 「インターフェイス上での CDP のディセーブル化およびイネーブル化」 (P.27-4)

CDP のデフォルト設定

表 27-1 に、CDP のデフォルト設定を示します。

表 27-1 CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー (パケット更新頻度)	60 秒
CDP ホールドタイム (廃棄までの時間)	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の特性の設定

CDP 更新の頻度、廃棄するまで情報を保持する期間、およびバージョン 2 アドバタイズを送信するかどうかを設定できます。

CDP タイマー、ホールドタイム、およびアドバタイズ タイプを設定するには、特権 EXEC モードで次の手順を実行します。



(注) ステップ 2 ~ 4 はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>cdp timer seconds</code>	(任意) CDP 更新の送信頻度 (秒) を設定します。 指定できる範囲は 5 ~ 254 です。デフォルトは 60 秒です。

コマンド	目的
ステップ 3 <code>cdp holdtime seconds</code>	(任意) デバイスから送信された情報を受信側デバイスが廃棄するまで保持する期間を指定します。 指定できる範囲は 10 ~ 255 秒です。デフォルトは 180 秒です。
ステップ 4 <code>cdp advertise-v2</code>	(任意) バージョン 2 アドバタイズを送信するように CDP を設定します。 これがデフォルトのステートです。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show cdp</code>	設定値を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

次に、CDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

その他の CDP `show` コマンドについては、「[CDP のモニタおよびメンテナンス](#)」(P.27-5) を参照してください。

CDP のディセーブル化およびイネーブル化

CDP はデフォルトでイネーブルです。



(注)

スイッチ クラスタと他のシスコ製デバイス (Cisco IP Phone など) は、CDP メッセージを定期的に変換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。詳細は、[第 6 章「スイッチのクラスタ化」](#) および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。

CDP デバイス検出機能をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>no cdp run</code>	CDP をディセーブルにします。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。

ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>cdp run</code>	ディセーブル化されている CDP をイネーブルにします。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。

次に、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

インターフェイス上での CDP のディセーブル化およびイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。

ポート上で CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no cdp enable	インターフェイス上で CDP をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定のポート上で、ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	cdp enable	インターフェイス上で、ディセーブル化されている CDP をイネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、特定のポート上で、ディセーブル化されている CDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

CDP のモニタおよびメンテナンス

デバイス上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
clear cdp counters	トラフィック カウンタをゼロにリセットします。
clear cdp table	ネイバーに関する情報を格納する CDP テーブルを削除します。
show cdp	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を表示します。
show cdp entry <i>entry-name</i> [protocol version]	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼動しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface [<i>interface-id</i>]	CDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors [<i>interface-id</i>] [detail]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数、チェックサム エラーを含む）を表示します。



CHAPTER 28

LLDP、LLDP-MED、および接続された場所のサービスの設定

この章では、Catalyst 3750 スイッチで Link Layer Discovery Protocol (LLDP)、LLDP Media Endpoint Discovery (LLDP-MED) および接続された場所のサービスを設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 の「System Management Commands」を参照してください。

- 「LLDP、LLDP-MED、および接続された場所のサービスの概要」 (P.28-1)
- 「LLDP、LLDP-MED、および接続された場所のサービスの設定」 (P.28-5)
- 「LLDP、LLDP-MED、および接続された場所のサービスのモニタリングおよびメンテナンス」 (P.28-11)

LLDP、LLDP-MED、および接続された場所のサービスの概要

LLDP

Cisco Discovery Protocol (CDP; シスコ検出プロトコル) は、すべてのシスコ製デバイス (ルータ、ブリッジ、アクセス サーバ、およびスイッチ) のレイヤ 2 (データ リンク レイヤ) 上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、ネットワーク接続されている他のシスコ製デバイスを自動的に検出し、識別できます。

スイッチでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB Link Layer Discovery Protocol (LLDP) をサポートしています。LLDP は、ネットワークデバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用する近隣探索プロトコルです。このプロトコルはデータ リンク レイヤで動作するため、異なるネットワーク レイヤプロトコルが稼動する 2 つのシステムで互いの情報を学習できます。

LLDP は一連のアトリビュートをサポートし、これらを使用して隣接するデバイスを検出します。アトリビュートには **Type**、**Length**、および **Value** があり、これらを **TLV** と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に **TLV** を使用できます。このプロトコルは、設定の情報、デバイスの機能、デバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV (IEEE 802.1 に固有の TLV)
- MAC/PHY コンフィギュレーション/ステータス TLV (IEEE 802.3 に固有の TLV)



(注)

スイッチ スタックは、ネットワーク内で 1 つのスイッチと見なされます。したがって、LLDP は個々のスタック メンバーではなく、スイッチ スタックを検出します。

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) は LLDP の拡張版で、IP 電話などのエンドポイント デバイスとスイッチなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet (PoE)、コンポーネント管理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイネーブルです。

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能を識別できます。

- ネットワーク ポリシー TLV

ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 アトリビュートをポート上の特定アプリケーションにアドバタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のスイッチに接続し、VLAN 番号を取得してから、呼制御の通信を開始できます。

ネットワーク ポリシー プロファイル TLV を定義して、VLAN、Class of Service (CoS; サービスクラス)、Differentiated Services Code Point (DSCP; DiffServ コードポイント)、およびタグ付けモードの値を指定し、音声と音声シグナリングのプロファイルを作成できます。次に、これらのプロファイルアトリビュートはスイッチ上で中央管理されて、IP 電話に伝播されます。

- 電源管理 TLV

LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。スイッチおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの電源情報を通知することができます。

LLDP-MED は、きめ細かい電力要件、エンドポイント電源プライオリティ、および、エンドポイントとネットワーク接続デバイスの電源ステータスをアダプタイズする拡張電源 TLV もサポートします。しかし、エンドポイントとネットワーク接続デバイス間の電力ネゴシエーションは行いません。

Cisco IOS Release 12.2(52)SE 以降では、LLDP がイネーブルに設定され、電力がポートに供給されている場合、システム電力バジェットが電源 TLV が適切に調整されるように、実際のエンドポイント デバイスの電力要求を決定します。スイッチは要求を処理し、現在の電力バジェットに基づいて電力を認可または拒否します。要求が認可されると、スイッチはパワー バジェットを更新します。要求が拒否された場合は、スイッチはポートの電力をオフにし、Syslog メッセージを生成して電力バジェットを更新します。LLDP-MED がディセーブルに設定されているか、または、エンドポイントが LLDP-MED 電源 TLV をサポートしていない場合、初期割り当て値 (15.4 W) は接続期間全体で使用されます。

電力設定を変更するには、**power inline {auto [max max-wattage] | never | static [max max-wattage]}** インターフェイス コンフィギュレーション コマンドを入力します。デフォルトで、Power over Ethernet (PoE) インターフェイスは **auto** モードです。値が指定されない場合、**maximum** は (15.4 W) に設定されます。

- コンポーネント管理 TLV

エンドポイントは、スイッチにエンドポイントの詳細なコンポーネント情報を送信することが可能です。コンポーネント情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフトウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。

- ロケーション TLV

スイッチからのロケーション情報をエンドポイント デバイスに提供します。ロケーション TLV はこの情報を送信することができます。

- 都市ロケーション情報

都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

- ELIN ロケーション情報

発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号 (ELIN) によって決定されます。これは、緊急通報を Public Safety Answering Point (PSAP) ヘルパーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

接続された場所のサービス

スイッチは、接続された場所のサービス機能を使用して、その接続されたデバイスの場所および接続のトラッキング情報を Cisco Mobility Services Engine (MSE) へ送信します。トラッキングできるデバイスは、ワイヤレス エンドポイント、ワイヤ エンドポイント、ワイヤ スイッチまたはワイヤ コントローラです。スイッチは、デバイスのリンク アップ イベントとリンク ダウン イベントを Network Mobility Services Protocol (NMSP; ネットワーク モビリティ サービス プロトコル) のロケーションおよびアタッチメント通知を介して MSE に通知します。

MSE がスイッチとの NMSP 接続を開始すると、サーバポートが開きます。MSE がスイッチに接続しているときは、バージョンの互換性を確保するための一連のメッセージ交換とサービス交換情報、およびその後にロケーション情報の同期があります。接続後、スイッチは定期的にロケーションおよびアタッチメント通知を MSE に送信します。1 つの間隔で検出されたリンク アップ イベントとリンク ダウン イベントは、各間隔の終わりに集約されて送信されます。

スイッチは、リンク アップ イベントとリンク ダウン イベントでのデバイスの有無を判別するとき、MAC アドレス、IP アドレス、ユーザ名などのクライアント固有の情報を取得します。クライアントが LLDP-MED または CDP 対応の場合、スイッチは LLDP-MED ロケーション TLV または CDP を介してシリアル番号および UDI を取得します。

デバイスの機能に応じて、スイッチはリンク アップ時に次のクライアント情報を取得します。

- ポート接続で指定されたスロットとポート
- クライアント MAC アドレスで指定された MAC アドレス
- ポート接続で指定された IP アドレス
- 802.1X ユーザ名 (適用される場合)
- デバイス カテゴリは、*wired station* として指定される
- ステータスは *new* として指定される
- シリアル番号、UDI
- 型番
- スイッチがアソシエーションを検出してから経過した時間 (秒)

デバイスの機能に応じて、スイッチはリンク ダウン時に次の情報を取得します。

- 切断されたスロットとポート
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名 (適用される場合)
- デバイス カテゴリは、*wired station* として指定される
- ステータスは *delete* として指定される
- シリアル番号、UDI
- スイッチがアソシエーションの解除を検出してから経過した時間 (秒)

スイッチはシャットダウン時に、ステータスが *delete* のアタッチメント通知と IP アドレスを送信してから、MSE との NMSP 接続を閉じます。MSE はこの通知を、スイッチに関連付けられているすべてのワイヤクライアントのアソシエーションの解除として解釈します。

スイッチのロケーション アドレスを変更すると、スイッチは影響を受けるポートと変更されたアドレス情報を示す NMSP ロケーション通知メッセージを送信します。

LLDP、LLDP-MED、および接続された場所のサービスの設定

- 「デフォルト LLDP 設定」 (P.28-5)
- 「設定時の注意事項」 (P.28-5)
- 「LLDP のイネーブル化」 (P.28-6)
- 「LLDP 特性の設定」 (P.28-6)
- 「LLDP-MED TLV の設定」 (P.28-7)
- 「ネットワーク ポリシー TLV の設定」 (P.28-8)
- 「ロケーション TLV と接続された場所の サービスの設定」 (P.28-9)

デフォルト LLDP 設定

表 28-1 デフォルト LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム (廃棄までの時間)	120 秒
LLDP タイマー (パケット更新頻度)	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル (すべての TLV を送受信不可)
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 送信	ディセーブル
LLDP med-tlv-select	ディセーブル (すべての LLDP-MED TLV を送信不可) LLDP がグローバルにイネーブルなときは、LLDP-MED-TLV もイネーブルです。

設定時の注意事項

- インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。
- 初めてネットワーク ポリシー プロファイルをインターフェイスに設定する場合は、インターフェイスに **switchport voice vlan** コマンドを適用できません。 **switchport voice vlan vlan-id** がインターフェイスにすでに設定されている場合は、インターフェイスにネットワーク ポリシー プロファイルを適用できます。この方法で、インターフェイスは音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルをインターフェイスに適用します。
- ネットワーク ポリシー プロファイルが適用されているインターフェイスにスタティック セキュア MAC アドレスを設定できません。
- プライベート LAN ポートにはネットワーク ポリシー プロファイルを設定できません。
- 接続された場所を機能させるには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力する必要があります。

LLDP のイネーブル化

LLDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>lldp run</code>	スイッチ上で LLDP をグローバルにイネーブルに設定します。
ステップ 3	<code>interface interface-id</code>	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>lldp transmit</code>	インターフェイスで LLDP パケットを送信できるようにします。
ステップ 5	<code>lldp receive</code>	インターフェイスが LLDP パケットを受信できるようにします。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show lldp</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

LLDP をディセーブルにするには、`no lldp run` グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で LLDP をディセーブルにするには、`no lldp transmit` および `no lldp receive` インターフェイス コンフィギュレーション コマンドを使用します。

次に、LLDP をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

LLDP の特性を設定するには、特権 EXEC モードで次の手順を実行します。



(注) ステップ 2 ~ 5 はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>lldp holdtime seconds</code>	(任意) デバイスからの情報を受信側デバイスが廃棄するまで保持する期間を指定します。 指定できる範囲は 0 ~ 65535 秒です。デフォルトは 120 秒です。

コマンド	目的
ステップ 3 <code>lldp reinit delay</code>	(任意) 任意のインターフェイス上で LLDP の初期化の遅延時間 (秒) を指定します。 指定できる範囲は 2 ~ 5 秒です。デフォルトは 2 秒です。
ステップ 4 <code>lldp timer rate</code>	(任意) LLDP 更新の送信頻度 (秒) を設定します。 指定できる範囲は 5 ~ 65534 秒です。デフォルトは 30 秒です。
ステップ 5 <code>lldp tlv-select</code>	(任意) 送受信する LLDP TLV を指定します。
ステップ 6 <code>lldp med-tlv-select</code>	(任意) 送受信する LLDP-MED TLV を指定します。
ステップ 7 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 8 <code>show lldp</code>	設定を確認します。
ステップ 9 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各 LLDP コマンドの `no` 形式を使用します。

次に、LLDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

LLDP-MED TLV の設定

デフォルトでは、スイッチは、エンドデバイスから LLDP-MED パケットを受信するまで LLDP パケットだけを送信します。受信後は、MED TLV を含む LLDP パケットも送信します。LLDP-MED エントリの期限が切れると、再度 LLDP パケットだけを送信します。

`lldp` インターフェイス コンフィギュレーション コマンドを使用することで、表 28-2 に示された TLV を送信しないようにインターフェイスを設定できます。

表 28-2 LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイス上で TLV をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>interface interface-id</code>	LLDP-MED TLV を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 <code>lldp med-tlv-select tlv</code>	イネーブルにする TLV を指定します。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次に、インターフェイス上で TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

ネットワーク ポリシー TLV の設定

ネットワーク ポリシー プロファイルを作成し、ポリシー アトリビュートを設定して、そのアトリビュートをインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	network-policy profile profile number	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポリシー設定モードを開始します。指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	{voice voice-signaling} vlan [vlan-id {cos cvalue dscp dvalue}] [[dot1p {cos cvalue dscp dvalue}] none untagged]	<p>ポリシー アトリビュートを設定します。</p> <p>voice : 音声アプリケーション タイプを指定します。</p> <p>voice-signaling : 音声シグナリングアプリケーション タイプを指定します。</p> <p>vlan : 音声トラフィック用のネイティブ VLAN を指定します。</p> <p>vlan-id : (任意) 音声トラフィック用の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。</p> <p>cos cvalue : (任意) 設定された VLAN のレイヤ 2 プライオリティ サービス クラス (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルトは 0 です。</p> <p>dscp dvalue : (任意) 設定された VLAN の Differentiated Services Code Point (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルトは 0 です。</p> <p>dot1p : (任意) IEEE 802.1 プライオリティ タグおよび VLAN 0 (ネイティブ VLAN) を使用するように IP 電話を設定します。</p> <p>none : (任意) 音声 VLAN について IP 電話に指示しません。IP 電話では、電話のキーパッドから設定を使用します。</p> <p>untagged : (任意) タグなし音声トラフィックを送信するように IP 電話を設定します。これが IP 電話のデフォルトです。</p>
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	interface interface-id	ネットワーク ポリシー プロファイルを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	network-policy profile number	ネットワーク ポリシー プロファイル番号を指定します。

	コマンド	目的
ステップ 7	<code>lldp med-tlv-select network-policy</code>	ネットワーク ポリシー TLV を指定します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show network-policy profile</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

次に、CoS を使用する音声アプリケーション用に VLAN 100 を設定し、インターフェイス上でネットワーク ポリシー プロファイルとネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

次に、プライオリティ タギングを使用するネイティブ VLAN 用に音声アプリケーション タイプを設定する例を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
Switch(config-network-policy)# voice vlan dot1p dscp 34
```

ロケーション TLV と接続された場所の サービスの設定

エンドポイントのロケーション情報を設定し、その情報をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>location {admin-tag string civic-location identifier id elin-location string identifier id}</code>	エンドポイントのロケーション情報を指定します。 <ul style="list-style-type: none"> admin-tag : 管理タグまたはサイト情報を指定します。 civic-location : 都市ロケーション情報を指定します。 elin-location : Emergency Location Information (ELIN; 緊急ロケーション情報) を指定します。 identifier id : 都市ロケーションの ID を指定します。 string : サイトまたはロケーション情報を英数形式で指定します。
ステップ 3	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	<code>interface interface-id</code>	ロケーション情報を設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

■ LLDP、LLDP-MED、および接続された場所のサービスの設定

コマンド	目的
ステップ 5 location { additional-location-information <i>word</i> civic-location-id <i>id</i> elin-location-id <i>id</i> }	<p>インターフェイスのロケーション情報を入力します。</p> <p>additional-location-information : ロケーションまたは場所の追加情報を指定します。</p> <p>civic-location-id : インターフェイスのグローバル都市ロケーション情報を指定します。</p> <p>elin-location-id : インターフェイスの緊急ロケーション情報を指定します。</p> <p><i>id</i> : 都市ロケーションまたは ELIN ロケーションの ID を指定します。ID の範囲は 1 ~ 4095 です。</p> <p><i>word</i> : 追加のロケーション情報を含む単語または句を指定します。</p>
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show location	設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

次に、スイッチに都市ロケーション情報を設定する例を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

スイッチ上で接続された場所のサービスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。



(注)

スイッチでは、暗号化ソフトウェア イメージが実行されていて、**nmosp** グローバル コンフィギュレーション コマンドがイネーブルになっている必要があります。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 nmosp enable	スイッチ上で NMSP 機能をイネーブルにします。
ステップ 3 nmosp notification interval { attachment location } <i>interval-seconds</i>	<p>NMSP 通知インターバルを指定します。</p> <p>attachment : アタッチメント通知のインターバルを指定します。</p> <p>location : ロケーション通知のインターバルを通知します。</p> <p><i>interval-seconds</i> : スイッチが MSE にロケーションまたはアタッチメントの更新を送信するまでの時間 (秒単位) 指定できる範囲は 1 ~ 30 です。デフォルトは 30 です。</p>
ステップ 4 end	特権 EXEC モードに戻ります。

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

次に、スイッチ上で NMSP をイネーブルにして、ロケーション通知の時間を 10 秒に設定する例を示します。

```
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
```

LLDP、LLDP-MED、および接続された場所のサービスのモニタリングおよびメンテナンス

デバイス上の LLDP、LLDP-MED、および接続された場所のサービスをモニタリングおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
<code>clear lldp counters</code>	トラフィック カウンタをゼロにリセットします。
<code>clear lldp table</code>	LLDP ネイバー情報テーブルを削除します。
<code>clear nmsp statistics</code>	NMSP 統計情報カウンタをクリアします。
<code>show lldp</code>	送信頻度、送信するパケットのホールドタイム、LLDP 初期化前の遅延時間など、インターフェイス上のグローバル情報を表示します。
<code>show lldp entry entry-name</code>	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力してすべてのネイバーを表示するか、ネイバー名を入力できます。
<code>show lldp interface [interface-id]</code>	LLDP がイネーブルになっているインターフェイスに関する情報を表示します。 表示内容を特定のインターフェイスに制限することができます。
<code>show lldp neighbors [interface-id] [detail]</code>	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
<code>show lldp traffic</code>	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタ類を表示します。
<code>show location</code>	エンドポイントのロケーション情報を表示します。
<code>show network-policy profile</code>	設定されたネットワーク ポリシー プロファイルを表示します。
<code>show nmsp</code>	NMSP 情報を表示します。



CHAPTER 29

UDLD の設定

この章では、Catalyst 3750 スイッチに Unidirectional Link Detection (UDLD; 単一方向リンク検出) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「UDLD の概要」 (P.29-1)
- 「UDLD の設定」 (P.29-3)
- 「UDLD ステータスの表示」 (P.29-7)

UDLD の概要

UDLD は、光ファイバまたはツイストペアイーサネットケーブルを通して接続されたデバイスからケーブルの物理設定をモニタしたり、単一方向リンクの存在を検出したりできるようにするためのレイヤ2プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされていなければなりません。UDLD は単一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リンクは、スパニングツリートポロジーループをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD は、通常 (デフォルト) とアグレッシブという2つの動作モードをサポートしています。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブモードの UDLD は、光ファイバリンクおよびツイストペアリンク上の片方向トラフィックと、光ファイバリンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ1のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ1と2の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が標準モードで、1 組のファイバストランドの 1 つが切断された場合、自動ネゴシエーションがアクティブであれば、レイヤ 1 メカニズムがリンクの物理的問題を検出するため、リンクは維持されません。この場合、UDLD は何の処理も行わず、論理リンクは不明となります。

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバリンクまたはツイストペア リンクで、ポートの 1 つがトラフィックを送受信できない。
- 光ファイバリンクまたはツイストペア リンクで、ポートの 1 つがダウンし、残りのインターフェイスが稼動している。
- ケーブルのうち 1 本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD Hello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できないかぎり、リンクをシャットダウンする必要があることを意味しています。

レイヤ 1 の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブ モードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは自動ネゴシエーションでは実行できません。

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

UDLD は、アクティブな各ポート上で Hello パケット（別名アドバタイズまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

スイッチが Hello メッセージを受信すると、エージング タイム（ホールド タイムまたは Time To Live (TTL)）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、スイッチが新しい Hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

UDLD の稼動中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになったり、またはスイッチをリセットした場合、UDLD は設定変更の影響を受けるポートの既存のキャッシュ エントリをすべて消去します。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

- イベントドリブン検出およびエコー

UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコーメッセージを返送します。この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

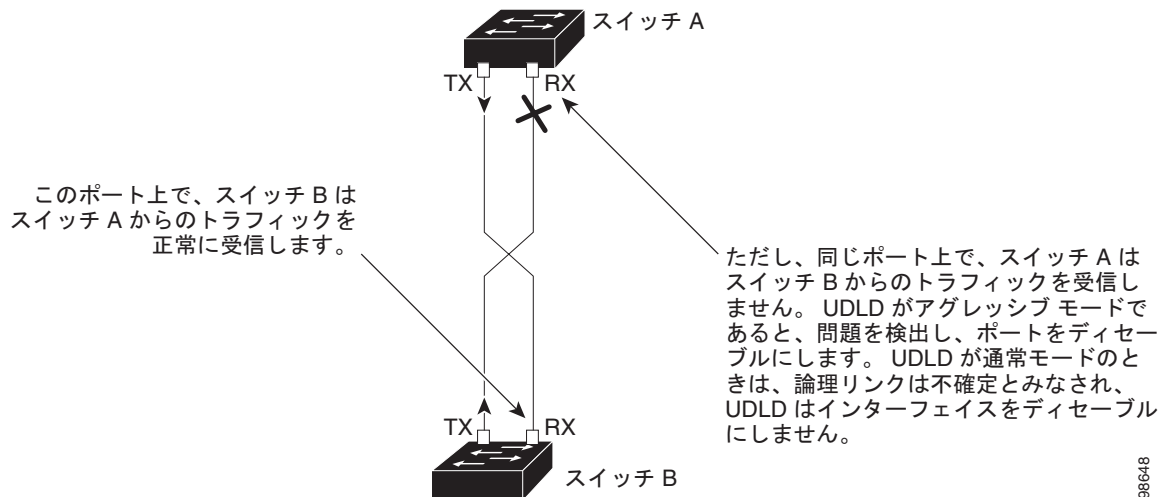
検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされません。UDLD がアグレッシブモードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

通常モードにある UDLD がアドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュエントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブモードをイネーブルにしている、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンクステータスが不確定のままの場合、UDLD はポートをシャットダウンします。

図 29-1 に、単一方向リンク状態の例を示します。

図 29-1 UDLD による単一方向リンクの検出



87936

UDLD の設定

ここでは、次の設定情報について説明します。

- 「UDLD のデフォルト設定」 (P.29-4)
- 「設定時の注意事項」 (P.29-4)
- 「UDLD のグローバルなイネーブル化」 (P.29-5)
- 「インターフェイス上での UDLD のイネーブル化」 (P.29-6)
- 「UDLD によってディセーブル化されたインターフェイスのリセット」 (P.29-6)

UDLD のデフォルト設定

表 29-1 に、UDLD のデフォルト設定を示します。

表 29-1 UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート (光ファイバ メディア用)	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート (ツイストペア (銅線) メディア用)	すべてのイーサネット 10/100 および 1000BASE-TX ポート上でディセーブル
UDLD アグレッシブ モード	ディセーブル

設定時の注意事項

UDLD 設定時の注意事項を次に示します。

- UDLD は Asynchronous Transfer Mode (ATM; 非同期転送モード) ポート上ではサポートされていません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートも単一方向リンクを検出できません。
- モード (通常またはアグレッシブ) を設定する場合、リンクの両側に同じモードを設定します。



注意

ループ ガードは、ポイントツーポイント リンクに限りサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは標準モードで UDLD をイネーブルにし、スイッチおよびスイッチ スタック内のすべてのメンバーのすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>udld {aggressive enable message time message-timer-interval}</code>	UDLD の動作モードを指定します。 <ul style="list-style-type: none"> aggressive : すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 enable : スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、udld enable グローバル コンフィギュレーション コマンドの設定を上書きします。 アグレッシブおよび通常モードの詳細については、「動作モード (P.29-1)」を参照してください。 message time message-timer-interval : アドバタイズ フェーズに存在し、双方向と検出されたポートにおける UDLD プロブ メッセージ間の間隔を設定します。指定できる範囲は 1 ~ 90 秒です。 <p>(注) グローバルな UDLD 設定は、スイッチ スタックに加入するスイッチに自動的に適用されます。</p> <p>(注) このコマンドが作用するのは、光ファイバ ポートだけです。他のポート タイプで UDLD をイネーブルにする場合は、udld インターフェイス コンフィギュレーション コマンドを使用します。詳細については、「インターフェイス上での UDLD のイネーブル化 (P.29-6)」を参照してください。</p>
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4 <code>show udld</code>	設定を確認します。
ステップ 5 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD をグローバルにディセーブルにするには、**no udld enable** グローバル コンフィギュレーション コマンドを使用して、すべての光ファイバ ポート上で標準モードの UDLD をディセーブルにします。すべての光ファイバ ポート上でアグレッシブ モードの UDLD をディセーブルにする場合は、**no udld aggressive** グローバル コンフィギュレーション コマンドを使用します。

インターフェイス上での UDLD のイネーブル化

ポート上で、UDLD をアグレッシブ モードまたは通常モードでイネーブルにするか、または UDLD をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	UDLD のためにイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>udld port [aggressive]</code>	UDLD はデフォルトでディセーブルです。 (注) スイッチ スタックに加入したスイッチでは、インターフェイス固有の UDLD 設定が維持されます。 <ul style="list-style-type: none"> • <code>udld port</code> : 指定されたポート上で、UDLD を通常モードでイネーブルにします。 • <code>udld port aggressive</code> : 指定されたポート上で、UDLD をアグレッシブ モードでイネーブルにします。 (注) 特定の光ファイバポート上で UDLD をディセーブルにする場合は、 <code>no udld port</code> インターフェイス コンフィギュレーション コマンドを使用します。 アグレッシブおよび通常モードの詳細については、「動作モード」(P.29-1) を参照してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show udld interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD によってディセーブル化されたインターフェイスのリセット

UDLD によってディセーブルにされたすべてのポートをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>udld reset</code>	UDLD によってディセーブルにされたすべてのポートをリセットします。
ステップ 2	<code>show udld</code>	設定を確認します。

次のコマンドを使用して、ポートを起動することもできます。

- `shutdown` インターフェイス コンフィギュレーション コマンドに続けて `no shutdown` インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブルのポートを再起動できます。
- `no udld {aggressive | enable}` グローバル コンフィギュレーション コマンドのあとに `udld {aggressive | enable}` グローバル コンフィギュレーション コマンドを実行すると、ディセーブル化されたポートが再びイネーブルになります。

- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port [aggressive]** インターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイバポートが再びイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを入力すると、UDLD の **errdisable** ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを入力すると、UDLD の **errdisable** ステートから回復する時間を指定できます。

UDLD ステータスの表示

指定されたポートまたはすべてのポートの UDLD ステータスを表示するには、**show udld [interface-id]** 特権 EXEC コマンドを使用します。

コマンド出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。



CHAPTER 30

SPAN および RSPAN の設定

この章では、Catalyst 3750 スイッチに Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN; リモート SPAN) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

この章で説明する内容は、次のとおりです。

- 「SPAN および RSPAN の概要」 (P.30-1)
- 「SPAN および RSPAN の設定」 (P.30-10)
- 「SPAN および RSPAN のステータス表示」 (P.30-26)

SPAN および RSPAN の概要

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー (ミラーリング) して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサ装置を宛先ポートに接続すれば、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを閉じることができます。

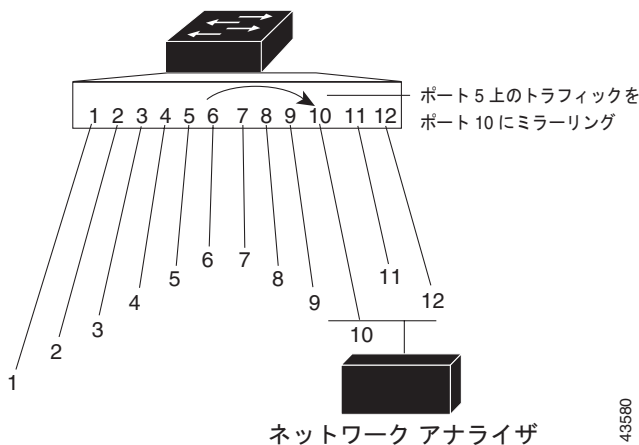
ここでは、次の概要について説明します。

- 「ローカル SPAN」 (P.30-2)
- 「リモート SPAN」 (P.30-3)
- 「SPAN と RSPAN の概念および用語」 (P.30-4)
- 「SPAN および RSPAN と他の機能の相互作用」 (P.30-9)
- 「SPAN/RSPAN およびスイッチ スタック」 (P.30-10)

ローカル SPAN

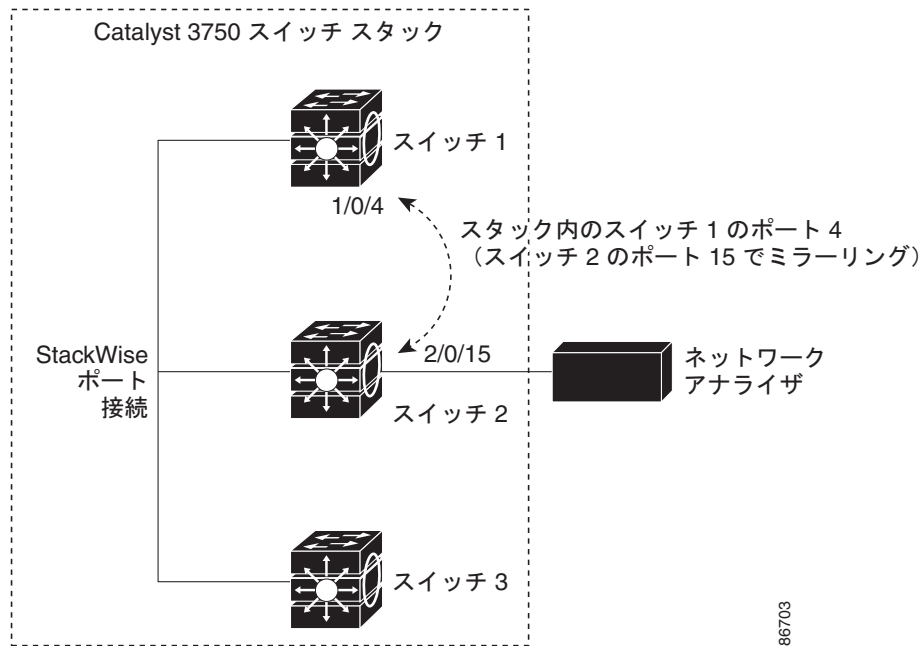
ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチまたはスイッチ スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。たとえば、[図 30-1](#) の場合、ポート 5 (送信元ポート) 上のすべてのトラフィックがポート 10 (宛先ポート) にミラーリングされます。ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

図 30-1 単一スイッチでのローカル SPAN の設定例



[図 30-2](#) に、送信元ポートおよび宛先ポートが異なるスタック メンバー上にある場合の、スイッチ スタックのローカル SPAN の例を示します。

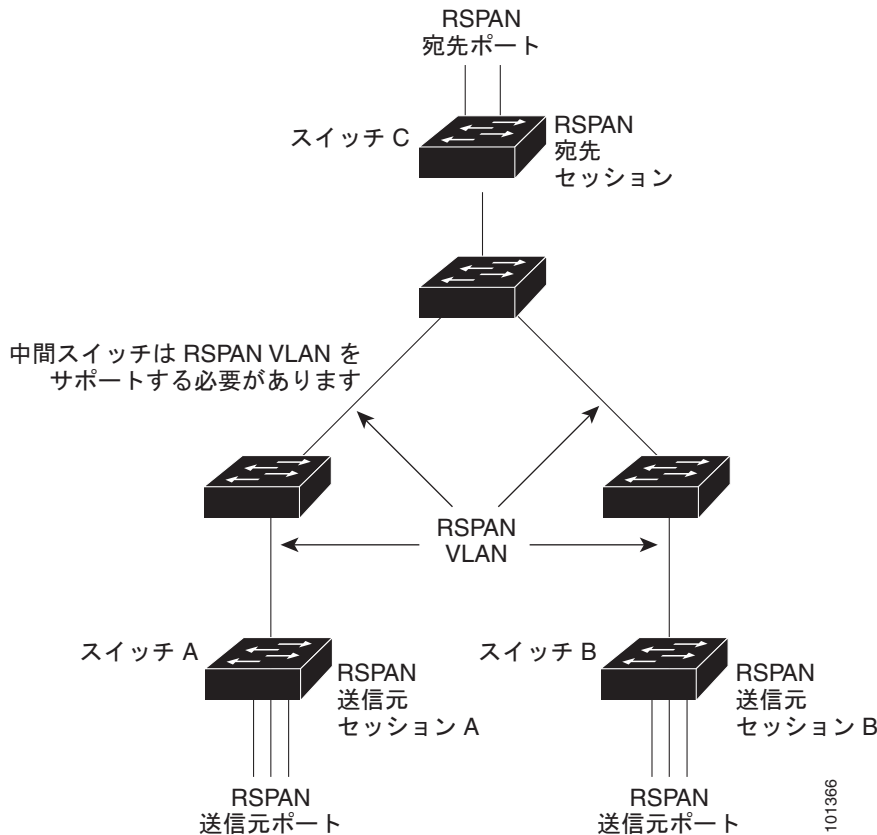
図 30-2 スイッチ スタックでのローカル SPAN の設定例



リモート SPAN

RSPAN は異なるスイッチ（または異なるスイッチ スタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク上にある複数のスイッチのリモート モニタリングを可能にします。図 30-3 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で搬送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 30-3 RSPAN の設定例



SPAN と RSPAN の概念および用語

ここでは、SPAN および RSPAN の設定に関連する概念および用語について説明します。

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート上、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。ローカル SPAN には、送信元セッションおよび宛先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出力の packets セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを通じて宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタグングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、(レイヤ 2 制御パケットを除く) すべての RSPAN VLAN パケットを解析のためにユーザにコピーすることです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要求に応答する必要があります ([RSPAN VLAN] (P.30-9) を参照)。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは最大 2 つの送信元セッションをサポートします (ローカル SPAN および RSPAN 送信元セッション)。同じスイッチ スタック内でローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチ スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックに設定できる宛先ポート数は最大 64 です。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットの廃棄または消失を招くことがあります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは 2 回伝送されます (1 回は標準トラフィックとして、もう 1 回はモニタされたパケットとして)。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- デイセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしないかぎり、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行することはできません。

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプをモニタできます。

- RX (受信) SPAN : 受信 (または入力) SPAN の役割は、送信元インターフェイスまたは VLAN が受信したすべてのパケットを、スイッチが変更または処理を行う前にできるだけ多くモニタすることです。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Differentiated Services Code Point (DSCP) の変更など、ルーティングや Quality of Service (QoS) が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットを廃棄する可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットが廃棄された場合でも、パケットのコピーを受信します。パケットを廃棄する可能性のある機能は、標準および拡張 IP 入力 Access Control List (ACL; アクセスコントロールリスト)、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- TX (送信) SPAN : 送信 (または出力) SPAN の役割は、スイッチによる変更および処理がすべて完了したあとで、送信元インターフェイスが送信したすべてのパケットをできるだけ多くモニターすることです。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

ルーティングが原因で変更されたパケット (Time to Live [TTL; 存続可能時間]、MAC [メディアアクセス制御] アドレス、QoS 値の変更など) は、宛先ポートで (変更されて) コピーされます。

送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方 : SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニターすることもできます。これがデフォルトです。

ローカル SPAN セッションポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol (CDP)、VLAN Trunking Protocol (VTP; VLAN トランキングプロトコル)、Dynamic Trunking Protocol (DTP)、Spanning-Tree Protocol (STP; スパニングツリープロトコル)、Port Aggregation Protocol (PAgP) などの Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) パケットおよびレイヤ 2 プロトコルをモニターしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートの場合と同じカプセル化設定 (タグなし、ISL [スイッチ間リンク]、または IEEE 802.1Q) を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコルパケットを含むすべてのタイプのパケットがモニターされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、ISL、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットが廃棄されることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニターされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スwitchの輻輳が原因で廃棄された出力パケットは、出力 SPAN からも廃棄されます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向 (RX と TX) SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両方のパケットは同じものになります (レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります)。

送信元ポート

送信元ポート (別名 *モニター対象ポート*) は、ネットワークトラフィック分析のためにモニターするスイッチドポートまたはルーテッドポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニターできます。スイッチは、任意の数の送信元ポート (スイッチで利用可能なポートの最大数まで) と任意の数

の送信元 VLAN (サポートされている VLAN の最大数まで) をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ (ローカルまたは RSPAN) であるため、単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向 (入力、出力、または両方) を指定して、各送信元ポートを設定できます。
- すべてのポートタイプ (EtherChannel、ファストイーサネット、ギガビットイーサネットなど) が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポートチャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセスポート、トランクポート、ルーテッドポート、または音声 VLAN ポートに指定できません。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN (VSPAN) では、1 つまたは複数の VLAN のネットワークトラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランクポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランクポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベースセッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタリストが指定されている場合、トランクポートまたは音声 VLAN アクセスポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポートタイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。

- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（別名 モニタ側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチ スタックに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションのみを実行するスイッチまたはスイッチ スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッドポートであった場合、このポートはルーテッドポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィックの転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチ スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化について次のとおり動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には次の特殊な特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラグメントされます。
- RSPAN VLAN では MAC（メディア アクセス制御）アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span VLAN** コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にすることはできません。

VTP に対して可視である VLAN 1 ~ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲（1006 ~ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックをモニタしません。VSPAN がモニタするのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタしません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN からモニタ対象 VLAN にトラフィックをルーティングする場合、そのトラフィックはモニタされず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランッキング：送信元ポート、または宛先ポートの VLAN メンバシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel：EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポート リストからそのポートが自動的に削除されます。

EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループ メンバーのままですが、*inactive* または *suspended* ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されます。

- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集の packets が 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト packets の送信回数は反映されません。
- プライベート VLAN ポートを SPAN 宛先ポートにできません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。

- IEEE 802.1X ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1X をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1X はディセーブルに設定されます。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1X をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1X をイネーブルにしないでください。

SPAN/RSPAN およびスイッチ スタック

スイッチ スタックは 1 つの論理スイッチとして扱われるため、ローカル SPAN 送信元ポートおよび宛先ポートをスタック内の異なるスイッチに設定できます。したがって、スタックにスイッチを追加または削除すると、ローカル SPAN セッションや、RSPAN 送信元または宛先セッションに影響が及ぶことがあります。スタックからスイッチを削除すると、アクティブ セッションが非アクティブになることがあります。スタックにスイッチを追加すると、非アクティブ セッションがアクティブになることがあります。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

SPAN および RSPAN の設定

ここでは、次の設定情報について説明します。

- 「SPAN および RSPAN のデフォルト設定」(P.30-11)
- 「ローカル SPAN の設定」(P.30-11)
- 「RSPAN の設定」(P.30-18)

SPAN および RSPAN のデフォルト設定

表 30-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 30-1 SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート (SPAN および RSPAN)	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方 (both)
カプセル化タイプ (宛先ポート)	ネイティブ形式 (タグなしパケット)
入力転送 (宛先ポート)	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上で、すべての VLAN がモニタ対象
RSPAN VLAN	未設定

ローカル SPAN の設定

ここでは、次の設定情報について説明します。

- 「SPAN 設定時の注意事項」(P.30-11)
- 「ローカル SPAN セッションの作成」(P.30-12)
- 「ローカル SPAN セッションの作成および着信トラフィックの設定」(P.30-15)
- 「フィルタリングする VLAN の指定」(P.30-17)

SPAN 設定時の注意事項

SPAN を設定するときには、次の注意事項に従ってください。

- 各スイッチ スタックにつき、最大 2 つの送信元セッションおよび 64 の RSPAN 宛先セッションを設定できます。送信元セッションは、ローカル SPAN セッションか RSPAN 送信元セッションのどちらかになります。
- 10 ギガビット イーサネット モジュール ポートが SPAN または RSPAN 宛先ポートとして設定されている場合、リンク速度が低下します。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するトラフィックがモニタされるだけです。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。

- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。
- Catalyst 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、3750G-16TD スイッチには、SPAN に関連するハードウェアの制限があります。ルーテッドユニキャストトラフィックの出力 SPAN コピーには、ローカルとリモートの両方の SPAN セッションに関する不正な宛先 MAC アドレスが含まれることがあります。この制限事項はブリッジドパケットには適用されません。ローカル SPAN での対策は、レプリケーションオプションを使用することです。
- 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、3750G-16TD スイッチでは、出力 SPAN ルーテッドパケット（ユニキャストとマルチキャストの両方）に間違った送信元 MAC アドレスが示されます。宛先ポートでネイティブカプセル化を使用したローカル SPAN パケットの場合、パケットには VLAN 1 の MAC アドレスが表示されます。カプセル化レプリケーションオプションが使用されている場合、この問題はローカル SPAN では現れません。この制限事項はブリッジドパケットには適用されません。回避方法として、**monitor session** グローバルコンフィギュレーションコマンドの **encapsulate replicate** キーワードを使用します。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。

コマンド	目的
ステップ 3 <code>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</code>	<p>SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。</p> <p><code>session_number</code> の範囲は、1 ～ 66 です。</p> <p><code>interface-id</code> には、モニタする送信元ポートまたは送信元 VLAN を指定します。</p> <ul style="list-style-type: none"> 送信元 <code>interface-id</code> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（port-channel port-channel-number）があります。有効なポートチャネル番号は 1 ～ 48 です。 <code>vlan-id</code> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 <p>(注) 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) <code>[, -]</code>：一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。</p> <ul style="list-style-type: none"> both：送信トラフィックと受信トラフィックの両方をモニタします。これがデフォルトです。 rx：受信トラフィックをモニタします。 tx：送信トラフィックをモニタします。 <p>(注) <code>monitor session session_number source</code> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>

コマンド	目的
ステップ 4 monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 (注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 (任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、 encapsulation replicate を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。 (注) monitor session <i>session_number</i> destination コマンドを複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show monitor [session <i>session_number</i>] show running-config	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination** **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 へミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ~ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定したあと、宛先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサ装置等) 用に着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「[ローカル SPAN セッションの作成](#)」(P.30-12) を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。
ステップ 3	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx]	SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。

コマンド	目的
ステップ 4 <code>monitor session session_number destination {interface interface-id [, -] [encapsulation replicate] [ingress {dot1q vlan vlan-id isl untagged vlan vlan-id vlan vlan-id}}}</code>	<p>SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。</p> <p><code>session_number</code> には、ステップ 3 で入力したセッション番号を指定します。</p> <p><code>interface-id</code> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</p> <p>(任意) <code>[, -]</code> : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、encapsulation replicate を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式 (タグなし) で送信されます。</p> <p>宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、ingress をキーワードと一緒に入力します。</p> <ul style="list-style-type: none"> • dot1q vlan vlan-id : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 • isl : ISL カプセル化を使用して着信パケットを転送します。 • untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show monitor [session session_number]</code> <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、**no monitor session session_number** グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session session_number source {interface interface-id | vlan vlan-id}** グローバル コンフィギュレーション コマンドまたは **no monitor session session_number destination interface interface-id** グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式を使用すると、カプセル化および入力オプションは無視されません。

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3 monitor session <i>session_number</i> source interface <i>interface-id</i>	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定されたインターフェイスは、あらかじめトランク ポートとして設定されていなければなりません。
ステップ 4 monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。 (任意) [, -] : カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5 monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate]}	SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。 <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 (任意) 送信元インターフェイスのカプセル化方式が宛先インターフェイスで複製されるように指定するには、 encapsulation replicate を入力します。これを選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show monitor [<i>session session_number</i>] show running-config	設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session session_number filter** グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

RSPAN の設定

ここでは、次の設定情報について説明します。

- 「RSPAN 設定時の注意事項」(P.30-18)
- 「RSPAN VLAN としての VLAN の設定」(P.30-19)
- 「RSPAN 送信元セッションの作成」(P.30-20)
- 「RSPAN 宛先セッションの作成」(P.30-22)
- 「RSPAN 宛先セッションの作成および着信トラフィックの設定」(P.30-23)
- 「フィルタリングする VLAN の指定」(P.30-25)

RSPAN 設定時の注意事項

RSPAN を設定するときには、次の注意事項に従ってください。

- 「SPAN 設定時の注意事項」(P.30-11) のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特殊な特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択的にフィルタリングまたはモニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパンニングがサポートされません。

- 次の条件を満たすかぎり、任意の VLAN を RSPAN VLAN として設定できます。
 - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加するすべてのスイッチで RSPAN がサポートされている。
- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがブルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラグディングが防止されます。
- Catalyst 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、3750G-16TD スイッチには、RSPAN に関連するハードウェアの制限があります。
 - ルーテッドユニキャストトラフィックの出力 SPAN コピーには、ローカルとリモートの両方の SPAN セッションに関する不正な宛先 MAC アドレスが含まれることがあります。この制限事項はブリッジドパケットには適用されません。ローカル SPAN での対策は、レプリケーションオプションを使用することです。リモート SPAN セッションの場合、対応策はありません。
 - 出力 SPAN ルーテッドパケット（ユニキャストパケットおよびマルチキャストパケットの両方）に、誤った送信元 MAC アドレスが表示されます。リモート SPAN パケットの場合、送信元 MAC アドレスは出力 VLAN の MAC アドレスである必要がありますが、代わりにパケットに RSPAN VLAN の MAC アドレスが表示されます。回避策はありません。
 - トラフィックが非常に混んでいる間に 2 つの RSPAN 送信元セッションが設定されると、片方の RSPAN セッションのパケットの VLAN ID が別の RSPAN セッションのパケットの VLAN ID を上書きします。上書きされると、この RSPAN VLAN 対象のパケットが誤って別の RSPAN VLAN に送信されます。この問題により RSPAN 宛先セッションは影響を受けません。回避策は RSPAN 送信元セッションを 1 つだけ設定することです。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッションの RSPAN VLAN となる VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のスイッチ、および中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan vlan-id</code>	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。有効範囲は 2 ~ 1001 および 1006 ~ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ~ 1005（トークンリングおよび Fiber Distributed Data Interface（FDDI）VLAN 専用）にすることはできません。
ステップ 3	<code>remote-span</code>	VLAN を RSPAN VLAN として設定します。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {<i>session_number</i> all local remote}	セッションに対する既存の RSPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。

コマンド	目的
ステップ 3 <code>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</code>	<p>RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。</p> <p><code>session_number</code> の範囲は、1 ~ 66 です。</p> <p>RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。</p> <ul style="list-style-type: none"> <code>interface-id</code> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel port-channel-number) があります。有効なポートチャネル番号は 1 ~ 48 です。 <code>vlan-id</code> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) <code>[, -]</code> : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。</p> <ul style="list-style-type: none"> both : 送信トラフィックと受信トラフィックの両方をモニタします。 rx : 受信トラフィックをモニタします。 tx : 送信トラフィックをモニタします。
ステップ 4 <code>monitor session session_number destination remote vlan vlan-id</code>	<p>RSPAN セッションおよび宛先 RSPAN VLAN を指定します。</p> <p><code>session_number</code> には、ステップ 3 で指定した番号を入力します。</p> <p><code>vlan-id</code> には、モニタする送信元 RSPAN VLAN を指定します。</p>
ステップ 5 <code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6 <code>show monitor [session session_number]</code> <code>show running-config</code>	<p>設定を確認します。</p>
ステップ 7 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

SPAN セッションを削除するには、**no monitor session session_number** グローバル コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session session_number source {interface interface-id | vlan vlan-id}** グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session session_number destination remote vlan vlan-id** コマンドを使用します。

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx

Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan <i>vlan-id</i>	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ~ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ~ 4 は不要です。
ステップ 3	remote-span	VLAN を RSPAN VLAN として識別します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	no monitor session {<i>session_number</i> all local remote}	セッションに対する既存の RSPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 6	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	monitor session <i>session_number</i> destination interface <i>interface-id</i>	RSPAN セッションおよび宛先インターフェイスを指定します。 <i>session_number</i> には、ステップ 6 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 encapsulation replicate はコマンドラインのヘルプ スtring に表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	<code>show monitor [session session_number]</code> <code>show running-config</code>	設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、`no monitor session session_number` グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、`no monitor session session_number destination interface interface-id` グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、`no monitor session session_number source remote vlan vlan-id` コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサ装置等) 用に着信トラフィックをイネーブルするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「[RSPAN 宛先セッションの作成](#)」(P.30-22) を参照してください。この手順は、RSPAN VLAN がすでに設定されていることを前提にしています。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {session_number all local remote}</code>	セッションに対する既存の SPAN 設定を削除します。
ステップ 3	<code>monitor session session_number source remote vlan vlan-id</code>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。

コマンド	目的
ステップ 4 <code>monitor session session_number destination {interface interface-id [, -] [ingress {dot1q vlan vlan-id isl untagged vlan vlan-id vlan vlan-id}}}</code>	<p>SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。</p> <p><code>session_number</code> には、ステップ 4 で指定した番号を入力します。</p> <p>RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。</p> <p><code>interface-id</code> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。</p> <p>encapsulation replicate はコマンドラインのヘルプ スtring に表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。</p> <p>(任意) <code>[, -]</code> : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、ingress を追加のキーワードと一緒に入力します。</p> <ul style="list-style-type: none"> • dot1q vlan vlan-id : VLAN をデフォルトの VLAN として指定し、IEEE 802.1Q カプセル化を使用して着信パケットを転送します。 • isl : ISL カプセル化を使用して着信パケットを転送します。 • untagged vlan vlan-id または vlan vlan-id : VLAN をデフォルトの VLAN として指定し、タグなしのカプセル化を使用して着信パケットを転送します。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show monitor [session session_number]</code> <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションを削除する場合は、`no monitor session session_number` グローバル コンフィギュレーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、`no monitor session session_number destination interface interface-id` グローバル コンフィギュレーション コマンドを使用します。このコマンドの `no` 形式を使用すると、入力オプションは無視されます。

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no monitor session {session_number all local remote}</code>	セッションに対する既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除する場合は all 、すべてのローカルセッションを削除する場合は local 、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3	<code>monitor session session_number source interface interface-id</code>	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定されたインターフェイスは、あらかじめトランク ポートとして設定されていなければなりません。
ステップ 4	<code>monitor session session_number filter vlan vlan-id [, -]</code>	SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。 (任意) [, -]: カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	<code>monitor session session_number destination remote vlan vlan-id</code>	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show monitor [session session_number]</code> <code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、**no monitor session session_number filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN のステータス表示

現在の SPAN または RSPAN 設定を表示するには、**show monitor** ユーザ EXEC コマンドを使用します。また、設定された SPAN および RSPAN セッションを表示するには、**show running-config** 特権 EXEC コマンドを使用できます。



CHAPTER 31

RMON の設定

この章では、Catalyst 3750 スイッチに Remote Network Monitoring (RMON) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチスタックを意味します。

RMON は、RMON 準拠のコンソールシステムとネットワークプローブ間で交換可能な一連の統計情報と機能を定義した標準モニタリング仕様です。RMON によって、総合的なネットワーク障害診断、プランニング、パフォーマンスチューニングに関する情報が得られます。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 の「System Management Commands」のセクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

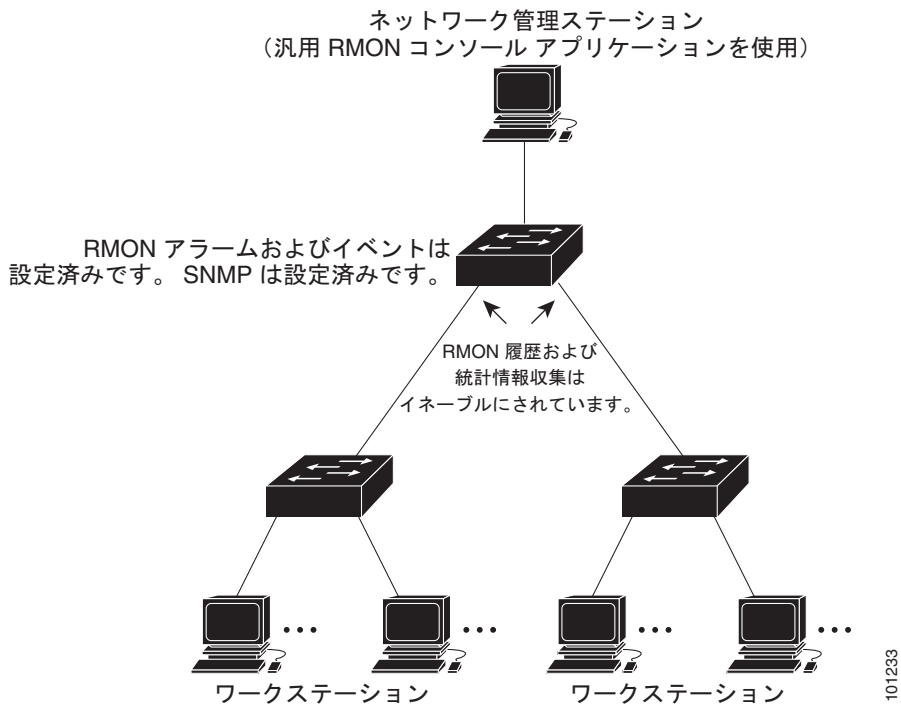
この章で説明する内容は、次のとおりです。

- 「RMON の概要」 (P.31-1)
- 「RMON の設定」 (P.31-3)
- 「RMON ステータスの表示」 (P.31-6)

RMON の概要

RMON は、各種のネットワークエージェントおよびコンソールシステムがネットワークモニタリングデータを交換できるようにするための、Internet Engineering Task Force (IETF) 標準モニタリング仕様です。図 31-1 のように、RMON 機能をスイッチの SNMP (簡易ネットワーク管理プロトコル) エージェントと組み合わせて使用することによって、接続されているすべての LAN セグメント上のスイッチ間で流れるすべてのトラフィックをモニタできます。

図 31-1 リモート モニタリングの例



スイッチは次の RMON グループ (RFC 1757 で定義) をサポートしています。

- 統計情報 (RMON グループ 1) : インターフェイス上のイーサネットの統計情報 (スイッチ タイプとサポートされているインターフェイスに応じて、ファストイーサネットやギガビットイーサネット統計情報など) を収集します。
- 履歴 (RMON グループ 2) : 指定されたポーリング間隔で、イーサネットポート上 (スイッチタイプおよびサポートされるインターフェイスに応じた、ファストイーサネットおよびギガビットイーサネット統計情報を含む) の統計情報グループの履歴を収集します。
- アラーム (RMON グループ 3) : 指定された期間、特定の MIB (管理情報ベース) オブジェクトをモニタし、指定された値 (上限しきい値) でアラームを発生し、別の値 (下限しきい値) でアラームをリセットします。アラームはイベントと組み合わせて使用できます。アラームがイベントを発生させ、イベントによってログエントリまたは SNMP トラップが生成されるようにできます。
- イベント (RMON グループ 9) : アラームによってイベントが発生したときのアクションを指定します。アクションは、ログエントリまたは SNMP トラップを生成できます。

このソフトウェアリリースがサポートするスイッチは、RMON データの処理にハードウェアカウンタを使用するので、モニタが効率的になり、処理能力はほとんど必要ありません。



(注)

RMON アラームでは、64 ビットカウンタはサポートされていません。

RMON の設定

ここでは、次の設定情報について説明します。

- 「[RMON のデフォルト設定](#)」 (P.31-3)
- 「[RMON アラームおよびイベントの設定](#)」 (P.31-3) (必須)
- 「[インターフェイス上でのグループ履歴統計情報の収集](#)」 (P.31-5) (任意)
- 「[インターフェイス上でのイーサネット グループ統計情報の収集](#)」 (P.31-6) (任意)

RMON のデフォルト設定

RMON はデフォルトでディセーブルです。アラームまたはイベントは設定されていません。

RMON アラームおよびイベントの設定

スイッチを RMON 対応として設定するには、CLI (コマンドライン インターフェイス) または SNMP 準拠の Network Management Station (NMS; ネットワーク管理ステーション) を使用します。NMS 上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用することを推奨します。RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。詳細は、[第 33 章「SNMP の設定」](#) を参照してください。



(注) RMON アラームでは、64 ビット カウンタはサポートされていません。

RMON アラームおよびイベントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>rmon alarm number variable interval {absolute delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	<p>MIB オブジェクトにアラームを設定します。</p> <ul style="list-style-type: none"> <i>number</i> には、アラーム番号を指定します。指定できる範囲は 1 ~ 65535 です。 <i>variable</i> には、モニタ対象の MIB オブジェクトを指定します。 <i>interval</i> には、アラームが MIB 変数をモニタする時間を秒数で指定します。指定できる範囲は 1 ~ 4294967295 秒です。 各 MIB 変数を直接テストする場合は、absolute キーワードを指定します。MIB 変数のサンプル間の変動をテストする場合は、delta キーワードを指定します。 <i>value</i> には、アラームを発生させる値およびアラームがリセットされる値を指定します。上限および下限しきい値に指定できる範囲は -2147483648 ~ 2147483647 です。 (任意) <i>event-number</i> には、上限および下限しきい値が限度を超えた場合に発生させるイベントの番号を指定します。 (任意) owner string には、アラームの所有者を指定します。
ステップ 3	<code>rmon event number [description string] [log] [owner string] [trap community]</code>	<p>RMON イベント番号に対応付けられた RMON イベント テーブルにイベントを追加します。</p> <ul style="list-style-type: none"> <i>number</i> には、イベント番号を割り当てます。指定できる範囲は 1 ~ 65535 です。 (任意) description string には、イベントの説明を指定します。 (任意) イベント発生時に RMON ログ エントリを生成する場合は、log キーワードを使用します。 (任意) owner string には、イベントの所有者を指定します。 (任意) trap community には、このトラップ用の SNMP コミュニティ スtring を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アラームをディセーブルにするには、設定した各アラームに対して、**no rmon alarm number** グローバル コンフィギュレーション コマンドを使用します。設定したすべてのアラームを一度にディセーブルにすることはできません。イベントをディセーブルにするには、**no rmon event number** グローバル コンフィギュレーション コマンドを使用します。アラームおよびイベントの詳細および相互作用については、RFC 1757 を参照してください。

任意の MIB オブジェクトにアラームを設定できます。次の例では、**rmon alarm** コマンドを使用して、RMON アラーム番号 10 を設定します。このアラームは、ディセーブルにされないかぎり、20 秒ごとに 1 度の間隔で MIB 変数 *ifEntry.20.1* をモニタし、変数の上下の変動をチェックします。*ifEntry.20.1* 値で MIB カウンタが 100000 から 100015 になるなど、15 以上増加すると、アラームが発生します。そのアラームによってさらにイベント番号 1 が発生します。イベント番号 1 は、**rmon event** コマンドで設定されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。*ifEntry.20.1* 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

次に、**rmon event** コマンドを使用して RMON イベント番号 1 を作成する例を示します。このイベントは *High ifOutErrors* と定義され、アラームによってイベントが発生したときに、ログ エントリが生成されます。ユーザ *jjones* が、このコマンドによってイベント テーブルに作成される行を所有します。次の例の場合も、イベント発生時に SNMP トラップが生成されます。

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

インターフェイス上でのグループ履歴統計情報の収集

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

インターフェイス上でグループ履歴統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	履歴を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	rmon collection history index [buckets bucket-number] [interval seconds] [owner ownername]	指定されたバケット数および時間で、履歴収集をイネーブルにします。 <ul style="list-style-type: none"> <i>index</i> には、RMON 統計グループを指定します。指定できる範囲は 1 ~ 65535 です。 (任意) buckets bucket-number には、RMON 統計グループ履歴収集に必要な最大バケット数を指定します。指定できる範囲は 1 ~ 65535 です。デフォルトのバケット数は 50 です。 (任意) interval seconds には、ポーリング サイクルを秒数で指定します。指定できる範囲は 1 ~ 3600 です。デフォルト値は 1800 秒です。 (任意) owner ownername には、RMON 統計グループの所有者名を入力します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。

	コマンド	目的
ステップ 6	<code>show rmon history</code>	スイッチ履歴テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

履歴収集をディセーブルにするには、`no rmon collection history index` インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイス上でのイーサネット グループ統計情報の収集

インターフェイス上でイーサネット統計グループを収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	統計情報を収集するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>rmon collection stats index [owner ownername]</code>	インターフェイス上で RMON 統計情報収集をイネーブルにします。 <ul style="list-style-type: none"> <code>index</code> には、RMON 統計グループを指定します。指定できる範囲は 1 ~ 65535 です。 (任意) <code>owner ownername</code> には、RMON 統計グループの所有者名を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>show rmon statistics</code>	スイッチ統計テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

イーサネット統計グループの収集をディセーブルにするには、`no rmon collection stats index` インターフェイス コンフィギュレーション コマンドを使用します。

次に、所有者 `root` の RMON 統計情報を収集する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# rmon collection stats 2 owner root
```

RMON ステータスの表示

RMON ステータスを表示するには、表 31-1 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 31-1 RMON ステータスを表示するコマンド

コマンド	目的
<code>show rmon</code>	汎用 RMON 統計情報を表示します。
<code>show rmon alarms</code>	RMON アラーム テーブルを表示します。
<code>show rmon events</code>	RMON イベント テーブルを表示します。

表 31-1 RMON ステータスを表示するコマンド (続き)

コマンド	目的
<code>show rmon history</code>	RMON 履歴テーブルを表示します。
<code>show rmon statistics</code>	RMON 統計情報テーブルを表示します。

これらの表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 の「System Management Commands」のセクションを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。



CHAPTER 32

システム メッセージ ログिंगの設定

この章では、Catalyst 3750 スイッチにシステム メッセージ ログिंगを設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注) このセクションで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「システム メッセージ ログिंगの概要」 (P.32-1)
- 「システム メッセージ ログिंगの設定」 (P.32-2)
- 「ログング設定の表示」 (P.32-14)



注意

高レートでコンソールへのメッセージを記録すると、CPU の利用率が高くなり、スイッチの動作に悪影響を与える可能性があります。

システム メッセージ ログिंगの概要

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をログング プロセスに送信します。スタック メンバーはシステム メッセージをトリガーできます。システム メッセージを生成するスタック メンバーは、ホスト名を *hostname-n* の形式で付加し (*n* は 1 ~ 9 のスイッチ番号)、出力をスタック マスターのログング プロセスにリダイレクトします。スタック マスターはスタック メンバーの 1 つですが、システム メッセージにホスト名を付加しません。ログング プロセスはログ メッセージを各宛先 (設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど) に配信する処理を制御します。ログング プロセスは、コンソールにもメッセージを送信します。



(注) Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

ログング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージが アクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

記録されたシステム メッセージにアクセスするには、スイッチの CLI (コマンドライン インターフェイス) を使用するか、正しく設定された Syslog サーバにシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージをスタンドアロン スイッチ (スイッチ スタックの場合はスタック マスター) の内部バッファに保存します。スタンドアロン スイッチまたはスタック マスターに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポート経由でスイッチにアクセスします。スイッチ スタックの場合は、すべてのスタック メンバーのコンソールに同じコンソール出力が表示されます。

システム メッセージ ログिंगの設定

ここでは、次の設定情報について説明します。

- 「システム ログ メッセージのフォーマット」 (P.32-2)
- 「システム メッセージ ログिंगのデフォルト設定」 (P.32-4)
- 「メッセージ ログिंगのディセーブル化」 (P.32-4) (任意)
- 「メッセージ表示宛先デバイスの設定」 (P.32-5) (任意)
- 「ログ メッセージの同期化」 (P.32-6) (任意)
- 「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」 (P.32-8) (任意)
- 「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」 (P.32-8) (任意)
- 「メッセージ重大度の定義」 (P.32-9) (任意)
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」 (P.32-10) (任意)
- 「設定変更ロガーのイネーブル化」 (P.32-11) (任意)
- 「UNIX Syslog サーバの設定」 (P.32-12) (任意)

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号 (%)、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報 (設定されている場合) で構成されています。メッセージは、次のフォーマットで表示されます。

```
seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)
```

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime [localtime] [msec] [show-timezone]**、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 32-1 に、Syslog メッセージの要素を示します。

表 32-1 システム ログ メッセージの要素

要素	説明
<i>seq no:</i>	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「 ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 (P.32-8) を参照してください。
<i>timestamp</i> のフォーマット： <i>mm/dd hh:mm:ss</i> または <i>hh:mm:ss</i> (短時間) または <i>d h</i> (長時間)	メッセージまたはイベントの日時です。 service timestamps log [datetime log] グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。 詳細については、「 ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 (P.32-8) を参照してください。
<i>facility</i>	メッセージが参照するファシリティ (SNMP、SYS など) です。サポートされるファシリティの一覧については、 表 32-4 (P.32-14) を参照してください。
<i>severity</i>	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。重大度の詳細については、 表 32-3 (P.32-10) を参照してください。
<i>MNEMONIC</i>	メッセージを一意に示すテキスト ストリングです。
<i>description</i>	レポートされているイベントの詳細を示すテキスト ストリングです。
<i>hostname-n</i> (ホスト名 -n)	スタック メンバーのホスト名およびスタック内のスイッチ番号。スタック マスターはスタック メンバーの 1 つですが、システム メッセージにホスト名を付加しません。

次に、スタック マスターおよびスタック メンバー (ホスト名 *Switch-2*) に対するスイッチ システム メッセージの一部の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

システム メッセージ ログイングのデフォルト設定

表 32-2 に、システム メッセージ ログイングのデフォルト設定を示します。

表 32-2 システム メッセージ ログイングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ログイング	イネーブル。
コンソールの重大度	debugging (および数値的により低いレベル。 表 32-3 (P.32-10) を参照)
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイム スタンプ	ディセーブル
同期ログイング	ディセーブル
ログ サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
設定変更ロガー	ディセーブル
サーバ ファシリティ	Local7 (表 32-4 (P.32-14) を参照)
サーバの重大度	informational (および数値的により低いレベル。 表 32-3 (P.32-10) を参照)

メッセージ ログイングのディセーブル化

メッセージ ログイングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ログイングをイネーブルにする必要があります。メッセージ ログイングがイネーブルの場合、ログ メッセージはログイング プロセスに送信されます。ログイング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

メッセージ ログイングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no logging console	メッセージ ログイングをディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config または show logging	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ログイング プロセスがディセーブルの場合、メッセージは生成後すぐに (通常はコマンド出力に割り込む形で) コンソールに表示されます。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return キーを押さなければメッセージが表示されません。詳細については、「[ログ メッセージの同期化](#)」(P.32-6) を参照してください。

メッセージ ログイングをディセーブルにしたあとに再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先デバイスの設定

メッセージ ログイングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。メッセージの受信場所を指定するには、特権 EXEC モードで次のコマンドを 1 つまたは複数使用します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 logging buffered [size]	<p>スタンドアロン スイッチ (スイッチ スタックの場合はスタック マスター) の内部バッファにメッセージをログイングします。指定できる範囲は 4096 ~ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。</p> <p>スタンドアロン スイッチまたはスタック マスターに障害が発生すると、フラッシュ メモリに保存されていないログは失われます。ステップ 4 を参照してください。</p> <p>(注) バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、show memory 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。</p>
ステップ 3 logging host	<p>UNIX Syslog サーバ ホストにメッセージを記録します。</p> <p><i>host</i> には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。</p> <p>ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。</p> <p>Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.32-12) を参照してください。</p>

コマンド	目的
ステップ 4 logging file flash:filename [max-file-size [min-file-size]] [severity-level-number type]	<p>スタンドアロンスイッチ（スイッチ スタックの場合はスタック マスター）のフラッシュ メモリ内のファイルにログ メッセージを保存します。</p> <ul style="list-style-type: none"> • <i>filename</i> には、ログ メッセージのファイル名を入力します。 • （任意）<i>max-file-size</i> には、ログ ファイルの最大サイズを指定します。指定できる範囲は 4096 ～ 2147483647 です。デフォルト値は 4096 バイトです。 • （任意）<i>min-file-size</i> には、ログ ファイルの最小サイズを指定します。指定できる範囲は 1024 ～ 2147483647 です。デフォルト値は 2048 バイトです。 • （任意）<i>severity-level-number type</i> には、ログイングの重大度またはログイング タイプを指定します。重大度の範囲は 0 ～ 7 です。ログイング タイプ キーワードの一覧については、表 32-3 (P.32-10) を参照してください。デフォルトでは、デバッグ メッセージ、および数値的により低いレベルのメッセージがログ ファイルに送信されます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 terminal monitor	<p>現在のセッション中に、コンソール以外の端末にメッセージを記録します。</p> <p>端末パラメータ設定コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。</p>
ステップ 7 show running-config	設定を確認します。
ステップ 8 copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ログ メッセージが内部バッファにコピーされます。循環バッファなので、バッファが一杯になると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。バッファ内の最も古いメッセージが最初に表示されます。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

特定の Power over Ethernet (PoE) 対応ポートで PoE イベントのログイングをイネーブルまたはディセーブルにするには、**logging event power-inline-status** インターフェイス コンフィギュレーション コマンドを使用します。このポートでのログイングは、デフォルトでイネーブルです。

コンソールへのログイングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。ファイルへのログイングをディセーブルにするには、**no logging file** [severity-level-number | type] グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ログイングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷されたあとに、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力用プロンプトが返されたあとに、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示されたあとに、コンソールはユーザ プロンプトを再表示します。

同期ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 line [console vty] line-number [ending-line-number]	<p>メッセージの同期ログイングを行うように、回線を設定します。</p> <ul style="list-style-type: none"> • スイッチのコンソール ポートを介して行われる設定には、console キーワードを使用します。 • 同期ログイングをイネーブルにする vty 回線を指定するには、line vty line-number コマンドを使用します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ~ 15 です。 <p>16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。</p> <p>line vty 0 15</p> <p>また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。</p> <p>line vty 2</p> <p>このコマンドを入力すると、ライン コンフィギュレーション モードになります。</p>
ステップ 3 logging synchronous [level [severity-level all] limit number-of-buffers]	<p>メッセージの同期ログイングをイネーブルにします。</p> <ul style="list-style-type: none"> • (任意) level severity-level には、メッセージの重大度を指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルト値は 2 です。 • (任意) level all を指定すると、重大度に関係なく、すべてのメッセージが非同期に出力されます。 • (任意) limit number-of-buffers には、キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ~ 2147483647 です。デフォルト値は 20 です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、**no logging synchronous [level severity-level | all] [limit number-of-buffers]** ライン コンフィギュレーション コマンドを使用します。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

ログ メッセージのタイム スタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service timestamps log uptime または service timestamps log datetime [msec] [localtime] [show-timezone]	ログのタイム スタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動したあとの経過時間が表示されます。 2 番目のコマンドを実行すると、ログ メッセージのタイム スタンプがイネーブルになります。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間 (ミリ秒)、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デバッグ メッセージとログ メッセージの両方のタイム スタンプをディセーブルにするには、**no service timestamps** グローバル コンフィギュレーション コマンドを使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
(Switch-2)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

ログ メッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service sequence-numbers	シーケンス番号をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

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

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のログイング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)
```

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します (表 32-3 を参照)。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>logging console level</code>	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 32-3 (P.32-10) を参照)。
ステップ 3	<code>logging monitor level</code>	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 32-3 (P.32-10) を参照)。
ステップ 4	<code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します (表 32-3 (P.32-10) を参照)。 Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.32-12) を参照してください。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code> または <code>show logging</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) *level* を指定すると、このレベルのメッセージ、および数値的により低いレベルのメッセージが宛先に表示されます。

コンソールへのログングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのログングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。**Syslog** サーバへのログングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 32-3 に *level* キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 32-3 メッセージ ログング level キーワード

level キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	ただちに対処が必要な状態	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー	LOG_ERR
warnings	4	警告	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	通知メッセージ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ~ **emergencies** の重大度で表示されます。このタイプのメッセージは、スイッチの機能に影響があることを示します。この誤動作からの回復手順については、このリリースに対応するシステム メッセージ ガイドを参照してください。
- debug** コマンドの出力：**debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center (TAC) でのみ使用されます。
- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。
- リロード要求および下位プロセス スタックのメッセージ。**informational** レベルで表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP Network Management Station (NMS; ネットワーク管理ステーション) に送信されるように Syslog メッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッセージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもできます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ (表 32-3 (P.32-10) を参照) が、履歴テーブルに 1 つ格納されます。

重大度および履歴テーブル サイズのデフォルト値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>logging history level¹</code>	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。 <i>level</i> キーワードのリストについては、表 32-3 (P.32-10) を参照してください。 デフォルトでは、 warnings 、 errors 、 critical 、 alerts 、および emergencies のメッセージが送信されます。
ステップ 3	<code>logging history size number</code>	履歴テーブルに格納できる Syslog メッセージ数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定できる範囲は 0 ~ 500 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

1. 表 32-3 に、*level* キーワードおよび重大度を示しています。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、*emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合 (`logging history size` グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合) は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのログングをデフォルトの重大度に戻すには、`no logging history` グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、`no logging history size` グローバル コンフィギュレーション コマンドを使用します。

設定変更ロガーのイネーブル化

CLI (コマンドライン インターフェイス) で行った設定変更をトラッキングするために設定ロガーをイネーブルにすることができます。`logging enable` 設定変更ロガー コンフィギュレーション コマンドを入力すると、設定変更用に入力されたセッション、ユーザおよびコマンドがログに記録されます。設定ログのサイズは 1 ~ 1000 エントリの間で設定することができます (デフォルトは 100)。`no logging enable` コマンドの後に `logging enable` コマンドを入力してログングをディセーブルにして再びイネーブルにすることで、いつでもログをクリアすることができます。

`show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning]` 特権 EXEC コマンドを使用して、設定ログ全体または指定したパラメータのログを表示します。

デフォルトで設定ログングはディセーブルになっています。

コマンドの詳細については、次の URL にある『Cisco IOS Configuration Fundamentals and Network Management Command Reference』Release 12.3 T を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

設定ログをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3	log config	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 4	logging enable	設定変更ログをイネーブルにします。
ステップ 5	logging size entries	(任意) 設定ログで取得するエン트리数を設定します。指定できる範囲は 1 ~ 1000 です。デフォルト値は 100 です。 (注) 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show archive log config	設定ログを表示することでエントリを確認します。

次に、設定変更ロガーをイネーブルにして、ログのエン트리数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

設定ログの出力例は次のとおりです。

```
Switch# show archive log config all
idx  sess      user@line      Logged command
 38   11   unknown user@vty3  |no aaa authorization config-commands
 39   12   unknown user@vty3  |no aaa authorization network default group radius
 40   12   unknown user@vty3  |no aaa accounting dot1x default start-stop group
radius
 41   13   unknown user@vty3  |no aaa accounting system default
 42   14           temi@vty4      |interface GigabitEthernet4/0/1
 43   14           temi@vty4      | switchport mode trunk
 44   14           temi@vty4      | exit
 45   16           temi@vty5      |interface FastEthernet5/0/1
 46   16           temi@vty5      | switchport mode trunk
 47   16           temi@vty5      | exit
```

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ログング ファシリティを定義する手順について説明します。

UNIX Syslog デーモンへのログ メッセージ

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。この手順は任意です。

root としてログインし、次のステップを実行します。



(注) 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ログイングをイネーブルにするには、Syslog コマンドラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

ステップ 1 /etc/syslog.conf ファイルに次のような行を 1 行追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

local7 キーワードは、使用するログイング ファシリティを指定します。ファシリティの詳細については、表 32-4 (P.32-14) を参照してください。**debug** キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 32-3 (P.32-10) を参照してください。Syslog デーモンは、これ以上の重大度の場合に、次のフィールドで指定されたファイルにメッセージを送信します。このファイルは、Syslog デーモンに書き込み権限がある既存ファイルでなければなりません。

ステップ 2 UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

ステップ 3 Syslog デーモンに新しい設定を認識させます。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

UNIX システム ログイング ファシリティの設定

システム ログ メッセージを外部デバイスに送信する場合は、メッセージを UNIX Syslog ファシリティから送信されたメッセージとして特定するようにシステムを設定できます。

UNIX システム ファシリティ メッセージ ログイングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging host	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを記録します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。

コマンド	目的
ステップ 3 <code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれ以下のメッセージを受信します。 <code>level</code> キーワードについては、表 32-3 (P.32-10) を参照してください。
ステップ 4 <code>logging facility facility-type</code>	Syslog ファシリティを設定します。 <code>facility-type</code> キーワードについては、表 32-4 (P.32-14) を参照してください。 デフォルトは <code>local7</code> です。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、`no logging host` グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのログイングをディセーブルにするには、`no logging trap` グローバル コンフィギュレーション コマンドを入力します。

表 32-4 に、ソフトウェアでサポートされている UNIX システム ファシリティを示します。これらのファシリティの詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 32-4 ログイング facility-type キーワード

facility-type キーワード	説明
<code>auth</code>	許可システム
<code>cron</code>	<code>cron</code> ファシリティ
<code>daemon</code>	システム デーモン
<code>kern</code>	カーネル
<code>local0 ~ local7</code>	ローカルに定義されたメッセージ
<code>lpr</code>	ライン プリンタ システム
<code>mail</code>	メール システム
<code>news</code>	USENET ニュース
<code>sys9 ~ sys14</code>	システムで使用
<code>syslog</code>	システム ログ
<code>user</code>	ユーザ プロセス
<code>uucp</code>	UNIX から UNIX へのコピー システム

ログイング設定の表示

ログイング設定およびログ バッファの内容を表示するには、`show logging` 特権 EXEC コマンドを使用します。この表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。



CHAPTER 33

SNMP の設定

この章では、Catalyst 3750 スイッチに Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスおよび次の URL の Cisco.com ホームページにある『Cisco IOS Network Management Command Reference, Release 12.4』を参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

- 「SNMP の概要」 (P.33-1)
- 「SNMP の設定」 (P.33-6)
- 「SNMP ステータスの表示」 (P.33-20)

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージフォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB (管理情報ベース) で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System (NMS; ネットワーク管理システム) に統合できます。エージェントおよび MIB は、スイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワークデータの保存場所である MIB から値を収集します。エージェントはマネージャからのデータ取得要求または設定要求に応答します。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンクステータス (アップまたはダウン)、MAC (メディアアクセス制御) アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

スタック マスターは、スイッチ スタック全体の SNMP 要求およびトラップを処理します。スタック マスターは、すべてのスタック メンバーに関連する要求またはトラップをトランスペアレントに管理します。新しいスタック マスターが選択されると、新しいマスターが以前のスタック マスターの設定に従って SNMP 要求およびトラップの処理を継続します。SNMP 管理ステーションとの IP 接続は、新しいマスターが制御を引き継いだあとも、有効であると見なされます。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

ここでは、次の概要について説明します。

- 「SNMP バージョン」 (P.33-2)
- 「SNMP マネージャ機能」 (P.33-3)
- 「SNMP エージェント機能」 (P.33-4)
- 「SNMP コミュニティストリング」 (P.33-4)
- 「SNMP を使用して MIB 変数にアクセスする方法」 (P.33-4)
- 「SNMP 通知」 (P.33-5)
- 「SNMP ifIndex MIB オブジェクト値」 (P.33-6)

SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1 : RFC1157 に定められた SNMP (完全インターネット標準)
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティベースの管理およびセキュリティフレームワークをコミュニティストリングベースの管理フレームワークに置き換えたものです。次の機能があります。
 - SNMPv2 : RFC 1902 ~ 1907 に定められた SNMP バージョン 2 (ドラフト版インターネット標準)
 - SNMPv2C : RFC 1901 に定められた SNMPv2 のコミュニティストリングベースの管理フレームワーク (試験版インターネットプロトコル)
- SNMPv3 : SNMP のバージョン 3 は、RFC 2273 から 2275 で定義された相互運用可能な標準ベースのプロトコルです。SNMPv3 は、ネットワーク上のパケットの認証と暗号化によりデバイスへの安全なアクセスを提供し、次のセキュリティ機能を備えています。
 - メッセージの完全性 : パケットが伝送中に改ざんされないようにします。
 - 認証 : メッセージの送信元が有効かどうかを判別します。
 - 暗号化 : パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。



(注) 暗号化を選択するには、**priv** キーワードを入力します。このキーワードを使用できるのは、暗号化ソフトウェア イメージがインストールされている場合だけです。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス Access Control List (ACL; アクセスコントロールリスト) およびパスワードによって定義されます。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラーメッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラーコードが使用されています。これらのエラーは、SNMPv1 では単一のエラーコードで報告されます。SNMPv2 では、エラーリターンコードでエラータイプが報告されるようになりました。

SNMPv3 は、セキュリティモデルとセキュリティレベルの両方を提供します。セキュリティモデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティレベルは、セキュリティモデル内で許可されたセキュリティのレベルです。セキュリティレベルとセキュリティモデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティメカニズムが決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

表 33-1 に、セキュリティ モデルとセキュリティ レベルのさまざまな組み合わせについて、その特性を示します。

表 33-1 SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv (暗号化ソフトウェア イメージが必要)	MD5 または SHA	Data Encryption Standard (DES; データ暗号化規格) または Advanced Encryption Standard (AES; 高度暗号規格)	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。次の暗号化アルゴリズムを使用する User-Based Security Model (USM; ユーザベースセキュリティ モデル) を指定できます。 <ul style="list-style-type: none"> Cipher Block Chaining (CBC; 暗号ブロック連鎖) DES (DES-56) 標準に基づいた認証のほか、DES の 56 ビット暗号化 3DES の 168 ビット データ暗号化 AES の 128 ビット、192 ビット、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 33-2 に示す動作を実行します。

表 33-2 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 ¹
get-bulk-request ²	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

- この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
- get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップメッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパンニング ツリー トポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ スtring

SNMP コミュニティ スtring は、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ スtring 定義が、スイッチ上の 3 つのコミュニティ スtring 定義の少なくとも 1 つと一致していなければなりません。

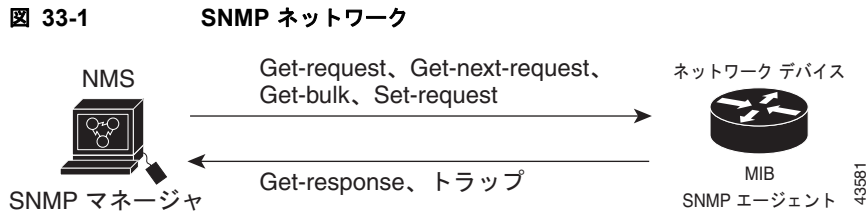
コミュニティ スtring のアトリビュートは、次の 3 つのいずれかです。

- Read-Only (RO)：許可された管理ステーションに、コミュニティ スtring を除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write (RW)：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ スtring に対するアクセスは許可しません。
- クラスタを作成すると、コマンドスイッチがメンバー スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に設定された RW および RO コミュニティ スtring にメンバー スイッチ番号 (@esN、N はスイッチ番号) を追加し、これらのスtring をメンバー スイッチに伝播します。詳細は、第 6 章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 33-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリーに応答します。



サポート対象の MIB の詳細、およびアクセス手順については、付録 B「サポート対象 MIB」を参照してください。

SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにないかぎり、キーワード *traps* はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。



(注) SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうか送信側にわからないからです。通知要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) でメッセージを確認します。送信側が応答を受信しなかった場合は、再び通知要求を送信できます。再送信できるので、通知の方がトラップより意図した宛先に届く可能性が高くなります。

通知の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、通知要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信（再試行）が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。したがって、トラップにするか通知にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、通知要求を使用してください。ネットワークまたはスイッチ メモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である **interface index** (ifIndex) オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチのソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、表 33-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 33-3 ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI ¹	1 ~ 4999
EtherChannel	5000 ~ 5012
ループバック	5013 ~ 5077
トンネル	5078 ~ 5142
物理 (ギガビット イーサネットまたは SFP ² モジュール インターフェイス)	10000 ~ 14500
ヌル	14501

1. SVI = Switch Virtual Interface

2. SFP = Small Form-Factor Pluggable



(注) スイッチは、範囲内の連続した値を使用しない場合があります。

SNMP の設定

- 「SNMP のデフォルト設定」(P.33-7)
- 「SNMP 設定時の注意事項」(P.33-7)
- 「SNMP エージェントのディセーブル化」(P.33-8)
- 「コミュニティ スtring の設定」(P.33-8)
- 「SNMP グループおよびユーザの設定」(P.33-10)
- 「SNMP 通知の設定」(P.33-13)
- 「CPU しきい値通知のタイプと値の設定」(P.33-17)
- 「エージェント コンタクトおよびロケーションの設定」(P.33-17)
- 「SNMP を通して使用する TFTP サーバの制限」(P.33-18)
- 「SNMP の例」(P.33-19)

SNMP のデフォルト設定

表 33-4 に、SNMP のデフォルト設定を示します。

表 33-4 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル ¹
SNMP トラップ レシーバー	未設定
SNMP トラップ	TCP 接続のトラップ (tty) 以外は、イネーブルではありません。
SNMP バージョン	version キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで noauth (noAuthNoPriv) になります。
SNMP 通知タイプ	タイプを指定しなかった場合、すべての通知が送信されます。

1. これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバーです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン ID は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザに対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。通知ビューの設定が必要な状況については、『*Cisco IOS Network Management Command Reference*』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモート エージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカル ユーザとリモート ホストに関連がない場合、スイッチは、**auth** (**authNoPriv**) および **priv** (**authPriv**) 認証レベルの通知を送信しません。

- SNMP エンジン ID の値を変更すると、重大な影響が生じます。コマンドラインで入力されたユーザのパスワードは、パスワードおよびエンジン ID に基づいて、MD5 または SHA セキュリティダイジェストに変換されます。その後、コマンドラインパスワードは RFC 2274 で要求されているように破棄されます。このように削除されるため、エンジン ID の値が変化した場合、SNMPv3 ユーザのセキュリティダイジェストは無効になり、`snmp-server user username` グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要があります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no snmp-server</code>	SNMP エージェントの動作をディセーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`no snmp-server` グローバル コンフィギュレーション コマンドを使用すると、デバイス上で稼動しているすべてのバージョン (バージョン 1、バージョン 2C、バージョン 3) がディセーブルになります。SNMP をイネーブルにする特定の Cisco IOS コマンドは存在しません。最初に入力する `snmp-server` グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server community string</code> [<code>view view-name</code>] [<code>ro</code> <code>rw</code>] [<code>access-list-number</code>]	コミュニティ ストリングを設定します。 (注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 <ul style="list-style-type: none"> <code>string</code> には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 (任意) <code>view</code> には、コミュニティがアクセスできるビュー レコードを指定します。 (任意) 許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用 (<code>ro</code>)、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き (<code>rw</code>) を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 (任意) <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	(任意) ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します (コミュニティ ストリングに値を入力しないでください)。

特定のコミュニティ ストリングを削除するには、`no snmp-server community string` グローバル コンフィギュレーション コマンドを使用します。

次に、ストリング *comaccess* を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト 4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名 (エンジン ID) を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上で SNMP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID { <i>local engineid-string</i> <i>remote ip-address [udp-port port-number] engineid-string</i> }	SNMP のローカル コピーまたはリモート コピーの名前を設定します。 <ul style="list-style-type: none"> <i>engineid-string</i> は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロだけが続く箇所を除いた部分に限ります。たとえば、123400000000000000000000 というエンジン ID を設定する場合、snmp-server engineID local 1234 のように入力できます。 remote を指定した場合、SNMP のリモート コピーが置かれているデバイスの <i>ip-address</i> を指定し、任意でリモート デバイスの UDP ポートを指定します。デフォルト値は 162 です。

コマンド	目的
ステップ 3 snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	<p>リモート デバイスに新規 SNMP グループを設定します。</p> <ul style="list-style-type: none"> • <i>groupname</i> には、グループを指定します。 • セキュリティ モデルを指定します。 <ul style="list-style-type: none"> – v1 は、最も安全性の低いセキュリティ モデルです。 – v2c は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を伝送できます。 – 最も安全な v3 の場合、認証レベルを選択する必要があります。 <p>auth : MD5 および SHA によるパケット認証が可能です。</p> <p>noauth : noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、これがデフォルトです。</p> <p>priv : DES によるパケット暗号化をイネーブルにします (<i>privacy</i> と呼ばれます)。</p> <p>(注) priv キーワードを使用できるのは、暗号化ソフトウェア イメージがインストールされている場合だけです。</p> <ul style="list-style-type: none"> • (任意) read <i>readview</i> とともに、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) write <i>writeview</i> とともに、データを入力し、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) notify <i>notifyview</i> とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) access <i>access-list</i> とともに、アクセス リスト名のストリング (64 文字以下) を入力します。

コマンド	目的
ステップ 4 snmp-server user <i>username</i> <i>groupname</i> { remote <i>host</i> [udp-port <i>port</i>]} { v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted] [access <i>access-list</i>] [auth { md5 sha } <i>auth-password</i>]} [priv { des 3des aes { 128 192 256 }} <i>priv-password</i>]	SNMP グループに対して新規ユーザを追加します。 <ul style="list-style-type: none"> • <i>username</i> は、エージェントに接続するホスト上のユーザ名です。 • <i>groupname</i> は、ユーザが対応付けられるグループの名前です。 • remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルト値は 162 です。 • SNMP バージョン番号 (v1、v2c、または v3) を入力します。v3 を入力する場合は、次のオプションを追加します。 <ul style="list-style-type: none"> – encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードを使用できるのは、v3 キーワードが指定されている場合だけです。 – auth は認証レベル設定セッションで、HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。パスワードストリング <i>auth-password</i> (64 文字以下) が必要です。 • v3 を入力し、スイッチで暗号化ソフトウェアイメージが実行されている場合は、プライベートな (priv) 暗号化アルゴリズムおよびパスワードストリング <i>priv-password</i> (64 文字以下) を設定することもできます。 <ul style="list-style-type: none"> – priv は、ユーザベース セキュリティ モデル (USM) を指定します。 – des は、56 ビットの DES 暗号化を使用するように指定します。 – 3des は、168 ビットの DES 暗号化を使用するように指定します。 – aes は、DES 暗号化を使用するように指定します。128 ビット、192 ビット、または 256 ビットの暗号化を選択する必要があります。 • (任意) access <i>access-list</i> とともに、アクセスリスト名のストリング (64 文字以下) を入力します。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show running-config	設定を確認します。 (注) auth noauth priv モード設定に関する SNMPv3 情報を表示するには、 show snmp user 特権 EXEC コマンドを入力する必要があります。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS リリースが稼動しているスイッチでは、トラップ マネージャを無制限に設定できます。



(注)

コマンド構文で *traps* というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにないかぎり、キーワード **traps** はトラップ、情報、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

表 33-5 に、サポートされているスイッチ トラップ (通知タイプ) を示します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host host-addr informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

表 33-5 スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	Border Gateway Protocol (BGP) 状態変化トラップを生成。このオプションを使用できるのは、拡張マルチレイヤ イメージがインストールされている場合だけです。
bridge	Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
cpu threshold	CPU 関連のトラップを許可します。
envmon	環境モニタ トラップを生成します。ファン (fan)、シャットダウン (shutdown)、ステータス (status)、電源 (supply)、温度 (temperature) の環境トラップのいずれかまたはすべてをイネーブルにできます。
errdisable	ポート VLAN が errdisable ステートになった場合に、トラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 10000 です。デフォルトは 0 で、レート制限がないという意味です。
flash	SNMP FLASH 通知を生成します。オプションとして、フラッシュの追加または削除に関する通知をイネーブルにできます。このようにすると、スタックからスイッチを削除するか、またはスタックにスイッチを追加した場合に (物理的な取り外し、電源のオフ/オン、またはリロードの場合に)、トラップが発行されます。
fru-ctrl	エンティティ Field-Replaceable Unit (FRU) 制御トラップを生成します。スイッチ スタックでは、このトラップはスタックに対するスイッチの追加または削除を意味します。
hsrp	Hot Standby Router Protocol (HSRP) が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャストルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol (MSDP) が変更された場合に、トラップを生成します。

表 33-5 スイッチの通知タイプ (続き)

通知タイプのキーワード	説明
ospf	Open Shortest Path First (OSPF) が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステートアドバタイズメント、レート制限、再送信、ステート変更の各トラップのいずれかまたはすべてをイネーブルにできます。
pim	Protocol-Independent Multicast (PIM) が変更された場合に、トラップを生成します。無効 PIM メッセージ、ネイバー変更、ランデブー ポイント (RP) マッピング変更の各トラップのいずれかまたはすべてをイネーブルにできます。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 (注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 <ul style="list-style-type: none">snmp-server enable traps port-securitysnmp-server enable traps port-security trap-rate rate
rtr	SNMP Response Time Reporter (RTR) のトラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 に設定されています (制限なしの状態では、発生ごとにトラップが送信されます)。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) が変更された場合に、トラップを生成します。

表 33-5 に示す通知タイプを受信する場合は、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID remote ip-address engineid-string	リモート ホスト用のエンジン ID を指定します。

コマンド	目的
ステップ 3 snmp-server user <i>username</i> <i>groupname</i> { remote <i>host</i> [udp-port <i>port</i>]} { v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted [access <i>access-list</i>] [auth { md5 sha } <i>auth-password</i>]}]}	ステップ 2 で設定したリモート ホストと対応付ける SNMP ユーザを設定します。 (注) アドレスに対応するリモート ユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラー メッセージが表示され、コマンドが実行されません。
ステップ 4 snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	SNMP グループを設定します。
ステップ 5 snmp-server host <i>host-addr</i> [informs traps] [version { 1 2c 3 { auth noauth priv }}] <i>community-string</i> [<i>notification-type</i>]	SNMP トラップ動作の受信側を指定します。 <ul style="list-style-type: none"> • <i>host-addr</i> には、ホスト (対象となる受信側) の名前またはインターネット アドレスを指定します。 • (任意) SNMP 情報をホストに送信するには、informs を指定します。 • (任意) SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。 • (任意) SNMP version (1、2c、または 3) を指定します。SNMPv1 は informs をサポートしていません。 • (任意) バージョン 3 の場合、認証レベルとして auth、noauth、または priv を選択します。 (注) priv キーワードを使用できるのは、暗号化ソフトウェア イメージがインストールされている場合だけです。 <ul style="list-style-type: none"> • <i>community-string</i> には、version 1 または version 2c が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティ スtring を入力します。version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。 (注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ スtring の一部として @ 記号を使用しないでください。 <ul style="list-style-type: none"> • (任意) <i>notification-type</i> には、表 33-5 (P.33-13) に記載されているキーワードを使用します。タイプを指定しなかった場合、すべての通知が送信されます。

	コマンド	目的
ステップ 6	snmp-server enable traps notification-types	<p>スイッチがトラップまたは情報を送信できるようにし、送信する通知のタイプを指定します。通知タイプの一覧については、表 33-5 (P.33-13) を参照するか、snmp-server enable traps ? と入力してください。</p> <p>複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに snmp-server enable traps コマンドを個別に入力する必要があります。</p> <p>(注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。</p> <ul style="list-style-type: none"> snmp-server enable traps port-security snmp-server enable traps port-security trap-rate rate
ステップ 7	snmp-server trap-source interface-id	(任意) 送信元インターフェイスを指定します。そこからトラップ メッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 8	snmp-server queue-length length	(任意) 各トラップ ホストのメッセージ キュー長を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 10 です。
ステップ 9	snmp-server trap-timeout seconds	(任意) トラップ メッセージを再送信する間隔を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show running-config	設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

snmp-server host コマンドでは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドによって、指定された通知メカニズム (トラップおよび情報) がグローバルでイネーブルになります。ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host host** グローバル コンフィギュレーション コマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** グローバル コンフィギュレーション コマンドを使用してください。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps notification-types** グローバル コンフィギュレーション コマンドを使用します。

CPU しきい値通知のタイプと値の設定

CPU しきい値通知のタイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>process cpu threshold type {total process interrupt} rising percentage interval seconds [falling fall-percentage interval seconds]</code>	<p>CPU しきい値通知のタイプと値を設定します。</p> <ul style="list-style-type: none"> total : 通知タイプを合計 CPU 使用率に設定します。 process : 通知タイプを CPU プロセス使用率に設定します。 interrupt : 通知タイプを CPU 割り込み使用率に設定します。 rising percentage : 設定されている期間この値を超えたときに CPU しきい値通知を送信する CPU リソースのパーセンテージ (1 ~ 100) です。 interval seconds : CPU しきい値通知を送信するために満たす必要のある CPU しきい値違反の継続時間を示す秒数 (5 ~ 86400) です。 falling fall-percentage : 設定されている期間、使用率がこのレベルより低くなると CPU しきい値通知を送信する CPU リソースのパーセンテージ (1 ~ 100) です。 <p>この値は、rising percentage の値以下である必要があります。指定しないと、falling fall-percentage の値は rising percentage の値と同じになります。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server contact text</code>	<p>システム コンタクトを表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server contact Dial System Operator at beeper 21555.</pre>
ステップ 3	<code>snmp-server location text</code>	<p>システム ロケーションを表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server location Building 3/Room 222</pre>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

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

SNMP を通して使用する TFTP サーバの制限

SNMP を通してコンフィギュレーション ファイルを保存およびロードするために使用する TFTP (簡易ファイル転送プロトコル) サーバを、アクセス リストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server tftp-server-list access-list-number</code>	SNMP を通してコンフィギュレーション ファイルをコピーするために使用する TFTP サーバを、アクセス リスト内のサーバに限定します。 <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>source</i> には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

```
Switch(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33 (SNMPv1 を使用) や、ホスト 192.180.1.27 (SNMPv2C を使用) へ VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバーに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行めはこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の *snmp-server host* コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードの時に *auth* (*authNoPriv*) 認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、表 33-6 に記載されたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。この場合に表示されるフィールドの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

表 33-6 SNMP 情報を表示するためのコマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID [local remote]	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドを使用して auth noauth priv モードの SNMPv3 設定情報を表示する必要があります。この情報は、 show running-config の出力には表示されません。



CHAPTER 34

組み込みイベント マネージャの設定

Embedded Event Manager (EEM; 組み込みイベント マネージャ) は、Cisco IOS デバイス内でイベントを検出しリカバリーするための分散型でカスタマイズされた手法です。EEM はイベントをモニタして、モニタ対象のイベントが発生するかしきい値に達したときに、情報提供、修正、およびその他の EEM アクションを行うことができます。EEM ポリシーは、イベントおよびイベントが発生したときに実行する操作を定義します。

この章では、EEM の使用方法および Catalyst 3750 スイッチ上で設定する方法について説明します。この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチのコマンドリファレンスおよび『Cisco IOS Network Management Command Reference』を参照してください。完全な EEM マニュアルセットについては、『Cisco IOS Network Management Configuration Guide』の次のドキュメントを参照してください。

- *Embedded Event Manager Overview*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- *Writing Embedded Event Manager Policies Using the Cisco IOS CLI*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html
- *Writing Embedded Event Manager Policies Using Tcl*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html



(注)

この機能は、IP サービス イメージが稼動しているスイッチでだけサポートされます。

この章で説明する内容は、次のとおりです。

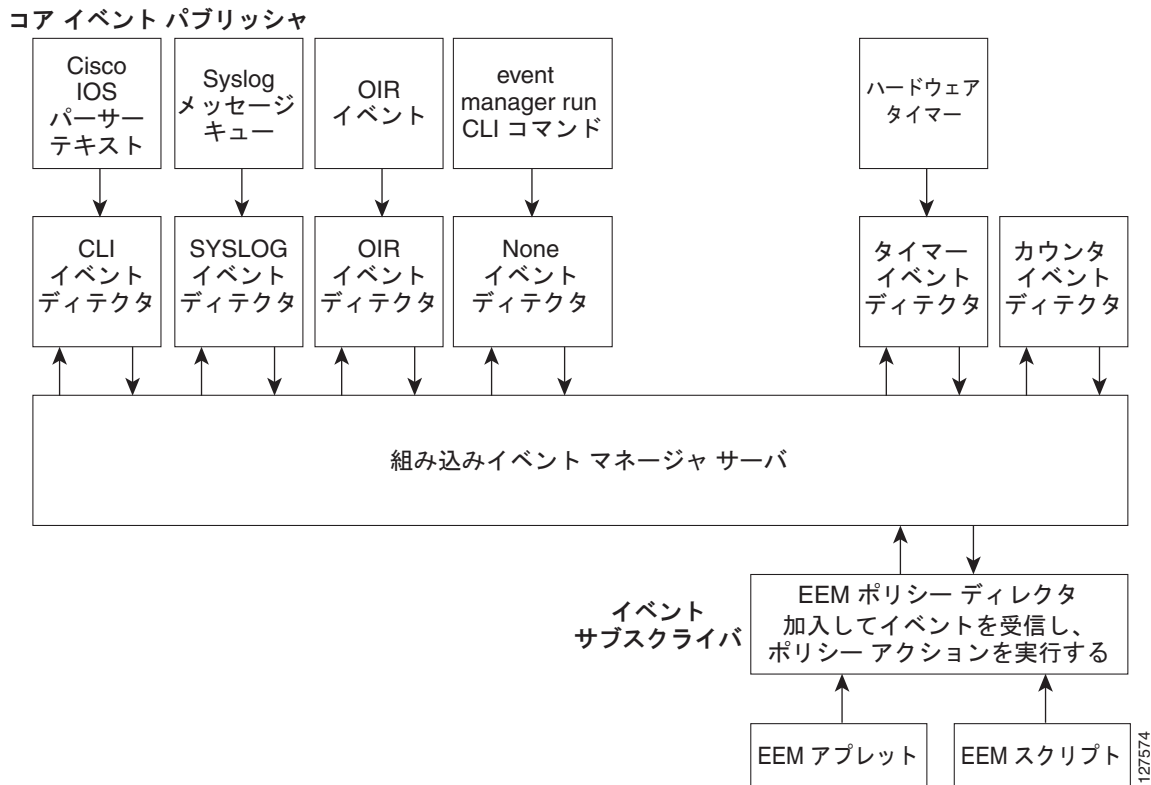
- 「組み込みイベント マネージャの概要」 (P.34-2)
- 「組み込みイベント マネージャの設定」 (P.34-6)
- 「組み込みイベント マネージャ情報の表示」 (P.34-8)

組み込みイベント マネージャの概要

EEM は、主要なシステム イベントをモニタして、セット ポリシーによってこれらに対する処理を行います。このポリシーはプログラミングされたスクリプトで、スクリプトをカスタマイズするために使用でき、発生するイベントセットに基づいて操作を呼び出します。スクリプトによって、カスタム Syslog または Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップの生成、CLI コマンドの呼び出し、フェールオーバーの強制などの操作が行われます。イベント管理の中にはスイッチから実行できないものがあり、問題によってはスイッチと外部ネットワーク管理デバイスの間で信頼のおけないコミュニケーションが行われることがあるので、EEM のイベント管理機能は便利です。スイッチをリブートしなくても自動回復処理を実行できれば、ネットワークの可用性が向上します。

図 34-1 に、EEM サーバ、コア イベント パブリッシャ (イベント ディテクタ)、およびイベント サブスクリイバ (ポリシー) 間の関係を示します。イベント パブリッシャは、イベント サブスクリイバによって示されるイベント指定と一致した場合、イベントをスクリーニングしてパブリッシュします。イベント ディテクタは、イベントが発生すると EEM サーバに通知します。そして EEM ポリシーは、システムと、指定のイベントについてポリシーに指定されている操作の現在の状態に基づいて回復を行います。

図 34-1 組み込みイベント マネージャのコア イベント ディテクタ



EEM 配置の例については、『[EEM Configuration for Cisco Integrated Services Router Platforms Guide](#)』を参照してください。

- 「イベント ディテクタ」 (P.34-3)
- 「組み込みイベント マネージャの操作」 (P.34-4)
- 「組み込みイベント マネージャ ポリシー」 (P.34-5)

- 「組み込みイベント マネージャの環境変数」 (P.34-5)
- 「EEM 3.2」 (P.34-6)

イベント ディテクタ

イベント ディテクタは EEM ソフトウェア プログラムであり、EEM イベントの発生を検知します。イベント ディテクタは独立したシステムであり、モニタ対象のエージェント（たとえば SNMP）とアクションが実行される EEM ポリシーとの間のインターフェイスとなります。イベント ディテクタはマスター スイッチによってのみ生成されます。また、CLI およびルーティング処理もマスター スイッチからのみ実行されます。



(注)

スタック メンバー スイッチはイベントを生成せず、メモリしきい値の通知および IOSWdSysmon イベント ディテクタをサポートしません。

- アプリケーション固有のイベント ディテクタ：どの EEM ポリシーでもイベントをパブリッシュできます。
- IOS CLI イベント ディテクタ：CLI を使用して入力されたコマンドに基づいてポリシーを生成します。
- Generic Online Diagnostics (GOLD; 汎用オンライン診断) イベント ディテクタ：特定のカードおよびサブカードで GOLD 障害イベントが検出されると、イベントをパブリッシュします。
- カウンタ イベント ディテクタ：特定のカウンタが特定のしきい値を超えると、イベントをパブリッシュします。
- インターフェイス カウンタ イベント ディテクタ：特定のインターフェイスの汎用 Cisco IOS インターフェイス カウンタが定義されたしきい値を超えると、イベントをパブリッシュします。しきい値は絶対値または差分値として指定できます。たとえば、差分値を 50 に設定すると、インターフェイス カウンタが 50 増えるとイベントがパブリッシュされます。
このディテクタは、エントリ値と終了値に対する変更の比率に基づいて、インターフェイスに関するイベントもパブリッシュします。
- None イベント ディテクタ：**event manager run** CLI コマンドが EEM ポリシーを実行すると、イベントをパブリッシュします。EEM は、ポリシー自身でのイベント指定に基づいてポリシーをスケジューリングして実行します。**event manager run** コマンドを実行する前に、EEM ポリシーを手動で指定し、登録する必要があります。
- Online Insertion and Removal (OIR; ホットスワップ) イベント ディテクタ：ハードウェアの OIR イベントが発生すると、イベントをパブリッシュします。
- リソースしきい値イベント ディテクタ：グローバル プラットフォーム値およびしきい値に基づいてポリシーを生成します。リソースには CPU 使用率および残りのバッファ容量などがあります。これはマスター スイッチにだけ適用されます。
- Remote Procedure Call (RPC; リモートプロシージャコール) イベント ディテクタ：Secure Shell (SSH; セキュア シェル) を使用する暗号化された接続を介してスイッチの外部から EEM ポリシーを呼び出し、Simple Object Access Protocol (SOAP) データ符号化を使用して XML ベースのメッセージを交換します。また、EEM ポリシーを実行した後、SOAP XML 形式の応答で出力を取得します。

- SNMP イベント デテクタ：標準 SNMP Management Information Base (MIB; 管理情報ベース) オブジェクトがモニタされ、次の場合にイベントが生成されます。
 - オブジェクトが、指定された値と一致するか指定されたしきい値を超えている場合。
 - SNMP デルタ値 (期間の開始時にモニタされた Object Identifier (OID; オブジェクト識別子) 値とイベントがパブリッシュされた時点での実際の OID 値の差異) が、指定された値と一致する場合。
 - SNMP 通知イベント デテクタ：SNMP トラップを代行受信し、スイッチが受信したメッセージを通知します。着信メッセージが指定されている値と一致するか、定義されているしきい値を超えると、イベントが生成されます。
 - Syslog イベント デテクタ：正規表現のパターン マッチにより Syslog メッセージがスクリーニングされます。選択されたメッセージにはさらに条件を設定して、特定の時間内に特定の回数の発生が記録されることを必要とするようにできます。特定のイベント条件での一致により、設定されたポリシー アクションがトリガーされます。
 - タイマー イベント デテクタ：次のタイマーによってイベントがパブリッシュされます。
 - absolute-time-of-day タイマーは、特定の絶対日時の場合にイベントをパブリッシュします。
 - カウントダウン タイマーは、タイマーがゼロになるとイベントをパブリッシュします。
 - Watchdog タイマーは、タイマーがゼロになるとイベントをパブリッシュします。タイマーは自動的に初期値にリセットされ、再度カウントダウンを開始します。
 - CRON タイマーは、イベントをパブリッシュする時間を定義するために UNIX 標準 CRON 仕様を使用してイベントをパブリッシュします。CRON タイマーは 1 秒に 1 つしかイベントをパブリッシュしません。
 - Watchdog イベント デテクタ (IOSWDSysMon)：マスター スイッチが次のときにだけイベントをパブリッシュします。
 - Cisco IOS 処理の CPU 使用率がしきい値を超える場合。
 - Cisco IOS 処理のメモリ使用率がしきい値を超える場合。
- 2 つのイベントを同時にモニタできます。イベントのパブリッシング条件では、1 つまたは両方のイベントが特定のしきい値を超える必要があります。

組み込みイベント マネージャの操作

イベントに応じて次のアクションが発生します。

- 特定のカウンタの変更
- アプリケーション固有のイベントのパブリッシュ
- SNMP トラップの生成
- 優先 Syslog メッセージの生成
- Cisco IOS ソフトウェアのリロード
- スイッチ スタックのリロード
- マスター スイッチオーバー発生時のマスター スイッチのリロード。これが行われると、新しいマスター スイッチが選択されます。

組み込みイベント マネージャ ポリシー

EEM はイベントをモニタして情報を提供したり、モニタ対象のイベントが発生するかしきい値に到達したときに修正操作を行ったりすることができます。EEM ポリシーは、イベントおよびイベントが発生したときに実行する操作を定義するエンティティです。

EEM ポリシーにはアプレットとスクリプトの 2 種類があります。アプレットは CLI コンフィギュレーションで定義される単純なポリシーで、イベントのスクリーニング条件およびイベント発生時に実行する操作を定義する簡単な方法です。スクリプトは ASCII エディタを使用してネットワーク装置に定義されます。スクリプトにはバイトコード (.tbc) スクリプトとテキスト (.tcl) スクリプトがあり、ネットワーク装置にコピーされて EEM に登録されます。1 つの .tcl ファイルで複数のイベントを登録することもできます。

EEM は、EEM ポリシーのツール コマンド言語 (TCL) スクリプトを使用して独自のポリシーを作成および実装します。マスター スイッチ上で TCL スクリプトを設定すると、スクリプト ファイルがメンバー スイッチに自動的に送信されます。マスター スイッチが変わっても TCL スクリプト ポリシーが引き続き動作するようにするためには、ユーザが定義した TCL スクリプトは、メンバー スイッチで利用可能である必要があります。

シスコはキーワード拡張の形で TCL を拡張したため、EEM ポリシーの開発は容易になっています。これらのキーワードを使用して、検出されたイベント、その後の操作、ユーティリティ情報、カウンタ値、およびシステム情報を特定します。

EEM ポリシーおよびスクリプトの設定の詳細については、『Cisco IOS Network Management Configuration Guide』 Release 12.4T を参照してください。

組み込みイベント マネージャの環境変数

EEM は、EEM ポリシーで環境変数を使用します。環境変数は、EEM ポリシーの TCL スクリプトで CLI コマンドおよび **event manager environment** コマンドを実行して定義します。

- ユーザ定義の変数

ユーザがユーザ定義のポリシー用に定義します。

- シスコ定義の変数

シスコが特定のサンプル ポリシー用に定義します。

- シスコの組み込み変数 (EEM アプレットで使用可能)

シスコが定義する読み取り専用または読み取りと書き込みが可能な変数です。読み取り専用変数は、アプレットが実行を開始する前にシステムによって設定されます。_exit_status という読み取りと書き込み変数を使用すると、同期イベントによってトリガーされるポリシーの終了ステータスを設定できます。

シスコ定義の環境変数およびシスコのシステム定義の環境変数は、1 つの特定のイベント ディテクタまたはすべてのイベント ディテクタに適用されます。ユーザ定義の環境変数またはサンプル ポリシーでシスコが定義する環境変数は、**event manager environment** グローバル コンフィギュレーション コマンドを使用して設定されます。ポリシーを登録する前に、EEM ポリシーで変数を定義する必要があります。

EEM がサポートする環境変数の詳細については、『Cisco IOS Network Management Configuration Guide』 Release 12.4T を参照してください。

EEM 3.2

EEM 3.2 は Cisco IOS Release 12.2(52)SE 以降でサポートされ、次のイベント ディテクタを導入します。

- 近隣探索：近隣探索イベント ディテクタは、次の場合に、ポリシーをパブリッシュして自動近隣探索に応答できます。
 - Cisco Discovery Protocol (CDP; シスコ検出プロトコル) キャッシュ エントリの追加、削除、または更新。
 - Link Layer Discovery Protocol (LLDP) キャッシュ エントリの追加、削除、または更新。
 - インターフェイス リンク ステータスの変更。
 - インターフェイス ライン ステータスの変更。
- ID：ID イベント ディテクタは、AAA 許可および認証が成功したとき、失敗したとき、または、ポート上の通常のユーザ トラフィックのフローが許可された後に、イベントを生成します。
- Mac アドレス テーブル：Mac アドレス テーブル イベント ディテクタは、MAC アドレス テーブルで MAC アドレスが学習されたときにイベントを生成します。



(注) Mac アドレス テーブル イベント ディテクタは、スイッチ プラットフォーム上でだけサポートされ、MAC アドレスが学習されるレイヤ 2 インターフェイスでだけ使用できます。レイヤ 3 インターフェイスはアドレスを学習せず、ルータは通常、学習された MAC アドレスを EFM に通知するために必要な MAC アドレス テーブル インフラストラクチャをサポートしません。

EEM 3.2 では、新しいイベント ディテクタと共に動作するアプレットをサポートする CLI コマンドも導入されます。

EEM 3.2 の機能の詳細については、『Embedded Event Manager 3.2』マニュアルを参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

組み込みイベント マネージャの設定

- 「組み込みイベント マネージャのアプレットの登録および定義」(P.34-6)
- 「組み込みイベント マネージャの TCL スクリプトの登録および定義」(P.34-7)

組み込みイベント マネージャの設定の詳細については、『Cisco IOS Network Management Configuration Guide』Release 12.4T を参照してください。

組み込みイベント マネージャのアプレットの登録および定義

EEM にアプレットを登録して、イベント アプレットおよびアクション アプレット コンフィギュレーション コマンドを使用して EEM アプレットを定義するには、特権 EXEC モードで次のコマンドを実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 event manager applet <i>applet-name</i>	EEM にアプレットを登録してアプレット コンフィギュレーション モードを開始します。
ステップ 3 event snmp oid <i>oid-value</i> get-type {exact next} entry-op {gt ge eq ne lt le} entry-val <i>entry-val</i> [exit-comb {or and}] [exit-op {gt ge eq ne lt le}] [exit-val <i>exit-val</i>] [exit-time <i>exit-time-val</i>] poll-interval <i>poll-int-val</i>	EEM アプレットが起動するイベント条件を指定します。 (任意) 終了条件。終了条件を指定しないと、イベントのモニタリングが即時に再度イネーブルになります。
ステップ 4 action label syslog [priority <i>priority-level</i>] msg <i>msg-text</i>	EEM アプレットをトリガーする操作を指定します。この操作を繰り返して、アプレットに他の CLI コマンドを追加します。 <ul style="list-style-type: none"> • (任意) priority キーワードは、Syslog メッセージの優先レベルを指定します。選択する場合は、priority-level 引数を定義する必要があります。 • msg-text については、この引数は文字テキスト、環境変数、またはこれら 2 つの組み合わせで指定できます。
ステップ 5 end	アプレット コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、SNMP オブジェクト ID によって指定されたフィールドのいずれかが、定義されたしきい値を超える場合の EEM の出力例を示します。

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

次に、EEM イベントに応じて実行されるアクションの例を示します。

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"
Switch (config-applet)# action 2.0 force-switchover
```

組み込みイベント マネージャの TCL スクリプトの登録および定義

EEM に TCL スクリプトを登録して、TCL スクリプトおよびポリシー コマンドを定義するには、特権 EXEC モードで次のコマンドを実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 1 show event manager environment [all <i>variable-name</i>]	(任意) show event manager environment コマンドは、EEM 環境変数の名前および値を表示します。 (任意) all キーワードは、EEM 環境変数を表示します。 (任意) variable-name 引数は、特定の環境変数の情報を表示します。
ステップ 2 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3 event manager environment <i>variable-name</i> string	特定の EEM 環境変数の値を設定します。必要な環境変数すべてについて、これを繰り返します。

	コマンド	目的
ステップ 4	<code>event manager policy</code> <code>policy-file-name</code> [<code>type</code> <code>system</code>] [<code>trap</code>]	ポリシー内に定義された特定のイベントが発生するときに実行する EEM ポリシーを登録します。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次に、`show event manager environment` コマンドの出力例を示します。

```
Switch# show event manager environment all
No.  Name                               Value
1    _cron_entry                          0-59/2 0-23/1 * * 0-6
2    _show_cmd                            show ver
3    _syslog_pattern                      .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                        interface Ethernet1/0
5    _config_cmd2                        no shut
```

次に、ソフトウェアによって指定される、毎日毎時間、毎分毎秒設定される CRON タイマー環境変数の例を示します。

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

この例では、システム ポリシーとして登録された `tm_cli_cmd.tcl` という名前のサンプル EEM ポリシーを示します。システム ポリシーは Cisco IOS イメージの一部です。最初にユーザ定義の TCL スクリプトをフラッシュ メモリにコピーする必要があります。

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

組み込みイベント マネージャ情報の表示

EEM の登録済みポリシーおよび EEM 履歴データなどの EEM の情報を表示するには、『*Cisco IOS Configuration Fundamentals and Network Management Command Reference*』を参照してください。



CHAPTER 35

ACL によるネットワーク セキュリティの設定

この章では、Access Control List (ACL; アクセス コントロール リスト) を使用して、Catalyst 3750 スイッチ上でネットワーク セキュリティを設定する方法について説明します。ACL の意味でアクセス リストという言葉を使用しています。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

この章では、IP ACL に関する記述は、IP Version 4 (IPv4) ACL のものです。IPv6 ACL の詳細については、[第 41 章「IPv6 ACL の設定」](#)を参照してください。

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide*』 Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』 Release 12.2 を参照してください。Cisco IOS のマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または、[Command References] からアクセスできます。

この章で説明する内容は、次のとおりです。

- 「ACL の概要」 (P.35-1)
- 「IPv4 ACL の設定」 (P.35-7)
- 「名前付き MAC 拡張 ACL の作成」 (P.35-28)
- 「VLAN マップの設定」 (P.35-31)
- 「ルータ ACL を VLAN マップと組み合わせて使用する方法」 (P.35-38)
- 「IPv4 ACL の設定の表示」 (P.35-42)

ACL の概要

パケット フィルタリングによって、ネットワーク トラフィックを限定し、さらに特定のユーザまたはデバイスに使用させるネットワークを制限できます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN (仮想 LAN) でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件を集めて順番に並べたものです。パケットがインターフェイスに着信すると、スイッチはパケットのフィールドと適用される ACL を比較し、アクセス リストに指定されている条件に基づいて、転送に必要な許可がパケットに与えられているかどうかを調べます。スイッチはパケットをアクセス リスト内の条件に対して 1 つずつテストします。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。制限がない場合、スイッチはパケットを転送し、制限がある場合はパケットを廃棄します。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセスリストを設定します。ACL を設定しないと、スイッチを通過するパケットはすべて、ネットワークのすべての部分に伝送される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定できます。たとえば、電子メールトラフィックの転送は許可し、Telnet トラフィックは許可しないといったことが可能です。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

ACL には Access Control Entry (ACE; アクセス コントロール エントリ) を順番に指定したリストが含まれます。ACE ごとに、*permit* または *deny*、および ACE と一致するためにパケットが満たさなければならない一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって異なります。

スイッチは、次の IP ACL およびイーサネット (MAC (メディア アクセス制御)) ACL をサポートします。

- IP ACL は、TCP、User Datagram Protocol (UDP)、Internet Group Management Protocol (IGMP)、Internet Control Message Protocol (ICMP) などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は、非 IP トラフィックをフィルタリングします。

このスイッチでは、Quality of Service (QoS) 分類 ACL もサポートされています。詳細については、「[QoS ACL に基づく分類](#)」(P.36-7) を参照してください。

ここでは、次の概要について説明します。

- 「[サポートされる ACL](#)」(P.35-2)
- 「[分割トラフィックおよび非分割トラフィックの処理](#)」(P.35-6)
- 「[ACL およびスイッチ スタック](#)」(P.35-7)

サポートされる ACL

トラフィックをフィルタリングするため、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス制御します。スイッチでは、発信方向のポート ACL はサポートしません。1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセスリスト 1 つと MAC アクセスリスト 1 つだけです。詳細については、「[ポート ACL](#)」(P.35-3) を参照してください。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向 (着信または発信) に適用されます。詳細については、「[ルータ ACL](#)」(P.35-4) を参照してください。
- VLAN ACL または VLAN マップは、すべてのパケット (ブリッジドパケットおよびルーテッドパケット) をアクセス制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット (ルーテッドパケットまたはブリッジドパケット) が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッドポートを介して、VLAN に入ることができます。詳細については、「[VLAN マップ](#)」(P.35-5) を参照してください。

同じスイッチ上で入力ポート ACL、ルータ ACL、VLAN マップを併用できます。ただし、ポート ACL はルータ ACL または VLAN マップよりも優先されます。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。その他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信されるルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。その他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってのみフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、VLAN マップおよびルータ ACL の両方によってフィルタリングされます。その他のパケットは、VLAN マップによってのみフィルタリングされます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってのみフィルタリングされます。発信されるルーテッド IP パケットは、VLAN マップおよびルータ ACL の両方によってフィルタリングされます。その他のパケットは、VLAN マップによってのみフィルタリングされます。

インターフェイスで IEEE 802.1Q トンネリングを設定している場合、トンネルポートで受信した IEEE 802.1Q カプセル化 IP パケットは、MAC ACL によってフィルタリングされますが、IP ACL ではフィルタリングされません。これは、IEEE 802.1Q ヘッダー内のプロトコルをスイッチが認識しないからです。この制限事項は、ルータ ACL、ポート ACL、VLAN マップに適用されます。IEEE 802.1Q トンネリングの詳細については、第 18 章「IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

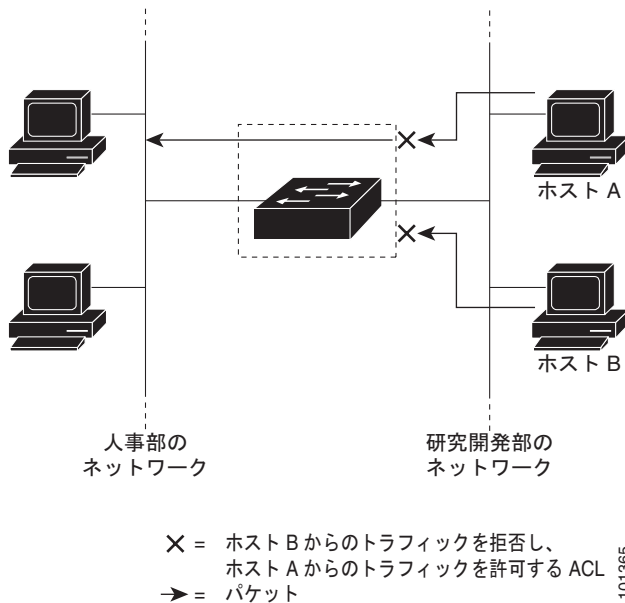
ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は、物理インターフェイス上でのみサポートされるため、EtherChannel インターフェイスではサポートされません。また、ポート ACL は着信方向のインターフェイス上でのみ適用できます。次のアクセスリストがサポートされています。

- 送信元アドレスを使用する標準 IP アクセス リスト
- 送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレス、宛先 MAC アドレス、およびオプションのプロトコル タイプ情報を使用する MAC 拡張アクセス リスト

スイッチは、特定のインターフェイス上に設定されている着信方向のすべての機能に関連した ACL をテストし、パケットが ACL 内のエン트리と一致するかどうかによって、パケットの転送を許可または拒否します。この方法の場合、ACL は、ネットワークまたは一部のネットワークへのアクセスを制御します。図 35-1 に、ポート ACL を使用して、すべてのワークステーションが同一の VLAN にある場合のネットワーク アクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A が人事部のネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2 インターフェイスにのみ適用されます。

図 35-1 ACL を使用したネットワーク トラフィックの制御



ポート ACL をトランク ポートに適用すると、そのトランク ポートにあるすべての VLAN で ACL によるトラフィックのフィルタリングが実行されます。音声 VLAN のあるポートにポート ACL を適用すると、データ VLAN と音声 VLAN の両方でその ACL によるトラフィックのフィルタリングが実行されます。

ポート ACL を使用すると、IP アクセス リストを使用して IP トラフィックをフィルタリングし、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用すると、そのレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックをフィルタリングできます。



(注)

1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストと MAC アクセス リストが 1 つずつ設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換えられます。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスである SVI、物理レイヤ 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

1 つの ACL をある特定インターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回、照合されます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、送信元アドレスを使用して照合します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。しかし、ルータ ACL は双方向でサポートされています。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクスト ホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセスを制御できます。図 35-1 では、ルータへの入力に適用されている ACL により、ホスト A は人事部のネットワークへのアクセスが許可されますが、ホスト B は拒否されます。

VLAN マップ

VLAN ACL または VLAN マップを使用して、すべてのトラフィックのアクセスを制御できます。VLAN との間でルーティングされる、またはスタックの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

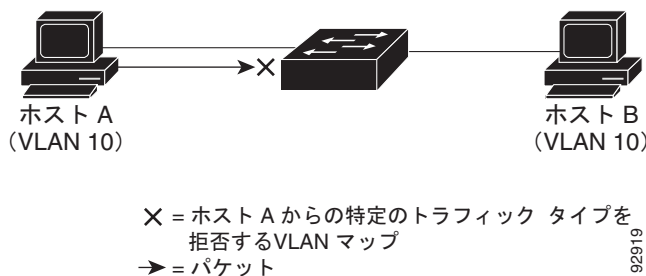
VLAN マップはセキュリティ パケット フィルタリングに使用してください。VLAN マップで方向（着信または発信）は定義されません。

VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックには、MAC VLAN マップによるアクセス コントロールができません）。VLAN マップはスイッチを通過するパケットだけに適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用することができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。図 35-2 に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 35-2 VLAN マップによるトラフィックの制御



分割トラフィックおよび非分割トラフィックの処理

IP パケットは、ネットワークを通過中に分割されることがあります。分割された場合、TCP または UDP ポート番号、ICMP タイプ、コードなどのレイヤ 4 情報が格納されているのは、パケットの先頭部分が含まれるフラグメントだけです。他のいずれのフラグメントにも、この情報は格納されません。

一部の ACE はレイヤ 4 情報を調べないため、すべてのパケット フラグメントに適用できます。ただし、通常の方法では、レイヤ 4 情報をテストする ACE は分割された IP パケットのほとんどのフラグメントに適用できません。フラグメントにレイヤ 4 情報が含まれず、ACE が一部のレイヤ 4 情報を調べる場合には、一致規則が次のように変更されます。

- フラグメント内のレイヤ 3 情報 (TCP、UDP などのプロトコル タイプを含む) を調べる許可 ACE は、格納されていないレイヤ 4 情報に関係なく、フラグメントに一致するとみなされます。
- レイヤ 4 情報を調べる拒否 ACE は、フラグメントにレイヤ 4 情報が格納されていないかぎり、フラグメントと一致することはありません。

次のコマンドで設定されたアクセス リスト 102 が 3 つのフラグメント パケットに適用されたとします。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```



(注)

この例の 1 番めおよび 2 番めの ACE で、宛先アドレスの後ろに *eq* キーワードが指定されています。これは、TCP 宛先ポートのうち、それぞれ Simple Mail Transfer Protocol (SMTP) および Telnet に対応する well-known 番号の有無をテストするという意味です。

- パケット A は、ホスト 10.2.2.2 のポート 65000 から SMTP ポート上のホスト 10.1.1.1 へ送信される TCP パケットです。このパケットが分割される場合、最初のフラグメントは、すべてのレイヤ 4 情報が格納されているので、完全なパケットの場合と同様、最初の ACE (許可) と一致します。最初の ACE はフラグメント適用時にレイヤ 3 情報だけを調べるため、SMTP ポート情報の有無にかかわらず残りのフラグメントも最初の ACE と一致します。この例の情報は、パケットが TCP で宛先が 10.1.1.1 ということです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 から Telnet ポート上のホスト 10.1.1.2 へ送信される TCP パケットです。このパケットが分割される場合、すべてのレイヤ 3 情報とレイヤ 4 情報が存在するため、最初のフラグメントは 2 番めの ACE (拒否) と一致します。パケットの残りのフラグメントは、レイヤ 4 情報がないので、2 番めの ACE と一致しません。残りのフラグメントは 3 番めの ACE (許可) に一致します。

最初のフラグメントが拒否されたので、ホスト 10.1.1.2 は完全なパケットを再び組み立てることができず、パケット B は事実上、拒否されます。ただし、許可されたあとのフラグメントがパケットを再び組み立てるときに、ネットワーク帯域幅とホスト 10.1.1.2 のリソースが消費されます。

- 分割パケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットが分割される場合、最初のフラグメントは 4 番めの ACE (拒否) と一致します。他のフラグメントもすべて、4 番めの ACE と一致します。この ACE はレイヤ 4 情報を調べず、すべてのフラグメントに含まれているレイヤ 3 情報から、ホスト 10.1.1.3 に送信中であったことが認識され、前の許可 ACE は別のホストをチェックしていたということがわかるためです。

ACL およびスイッチ スタック

スイッチ スタックの ACL サポート機能は、スタンドアロン スイッチの場合と同じです。ACL の設定情報は、スタック内のすべてのスイッチに伝播されます。スタック マスターを含むスタック内のすべてのスイッチは、情報を処理し、ハードウェアをプログラミングします（スイッチ スタックの詳細については、第 5 章「スイッチ スタックの設定」を参照）。

スタック マスターは、次に示す ACL 機能を実行します。

- ACL 設定を処理し、情報をすべてのスタック メンバーに伝播します。
- ACL 情報を、スタックに加入しているすべてのスイッチに配信します。
- 何らかの理由でパケットをソフトウェアで転送する必要がある場合（ハードウェア リソースが不足している場合など）、マスター スイッチはパケットに ACL を適用したあとにのみ、パケットを転送します。
- 処理する ACL 情報を使用して、ハードウェアをプログラミングします。

スタック メンバーは、次に示す ACL 機能を実行します。

- マスター スイッチから ACL 情報を受け取り、ハードウェアをプログラミングします。
- スタンバイ スイッチとして機能します。既存のマスター スイッチに障害が発生した場合、新規スタック マスターに選択されたスタック メンバーは、スタック マスターの役割を引き継ぐことができます。

スタック マスターに障害が発生し、新規スタック マスターが選択された場合、新規に選択されたマスターはバックアップされた実行コンフィギュレーションを解析し直します（第 5 章「スイッチ スタックの設定」を参照）。実行コンフィギュレーションの一部である ACL 設定も、この時に解析し直されます。新規スタック マスターは、ACL 情報をスタック内のすべてのスイッチに配信します。

IPv4 ACL の設定

スイッチに IPv4 ACL を設定する手順は、他のシスコ製スイッチおよびルータに IPv4 ACL を設定する場合と同じです。ここでは、手順を簡単に説明します。ACL の設定に関する詳細は、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。コマンドの詳細については、『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』 Release 12.2 を参照してください。Cisco IOS のマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または、[Command References] からアクセスできます。

スイッチがサポートしない Cisco IOS ルータ ACL 関連の機能は、次のとおりです。

- 非 IP プロトコル ACL（表 35-1 (P.35-9) を参照）またはブリッジグループ ACL
- IP アカウンティング
- 着信および発信レート制限（QoS ACL は除く）
- 再帰 ACL またはダイナミック ACL（スイッチ クラスタリング機能が使用する一部の特殊なダイナミック ACL は除く）
- ポート ACL および VLAN マップに関する ACL ロギング

スイッチ上で IP ACL を使用する手順は、次のとおりです。

-
- ステップ 1** アクセス リストの番号または名前およびアクセス条件を指定して、ACL を作成します。
- ステップ 2** ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。
-

ここでは、次の設定情報について説明します。

- 「標準および拡張 IPv4 ACL の作成」 (P.35-8)
- 「端末回線への IPv4 ACL の適用」 (P.35-19)
- 「インターフェイスへの IPv4 ACL の適用」 (P.35-20)
- 「IP ACL のハードウェアおよびソフトウェアの処理」 (P.35-22)
- 「ACL のトラブルシューティング」 (P.35-22)
- 「IPv4 ACL の設定例」 (P.35-23)

標準および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL は許可条件と拒否条件を集めて順番に並べたものです。スイッチはパケットをアクセス リスト内の条件に対して 1 つずつテストします。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは最初に一致した時点でテストを中止するので、条件の指定順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。

ソフトウェアは IPv4 用に、次に示すタイプの ACL、つまりアクセス リストをサポートします。

- 標準 IP アクセス リストでは、送信元アドレスを使用して照合します。
- 拡張 IP アクセス リストでは、送信元アドレスおよび宛先アドレスを使用して照合し、オプションとしてプロトコル タイプ情報を使用して、より細かな制御を行います。

ここでは、アクセス リストの概要、およびアクセス リストの作成方法について説明します。

- 「アクセス リスト番号」 (P.35-9)
- 「ACL のロギング」 (P.35-9)
- 「番号制標準 ACL の作成」 (P.35-10)
- 「番号制拡張 ACL の作成」 (P.35-11)
- 「ACL 内の ACE シーケンスの再編集」 (P.35-15)
- 「名前付き標準および拡張 ACL の作成」 (P.35-15)
- 「ACL での時間範囲の使用法」 (P.35-17)
- 「ACL へのコメントの挿入」 (P.35-19)

アクセス リスト番号

ACL を表すために使用する番号は、作成するアクセス リストのタイプを示します。表 35-1 に、アクセス リスト番号と対応するアクセス リストタイプ、およびスイッチがサポートするかどうかを示します。スイッチは、IPv4 標準および IPv4 拡張アクセス リスト（番号 1 ～ 199 および 1300 ～ 2699）をサポートします。

表 35-1 アクセス リスト番号

アクセス リスト番号	Type	サポート
1 ～ 99	IP 標準アクセス リスト	あり
100 ～ 199	IP 拡張アクセス リスト	あり
200 ～ 299	プロトコル タイプ コード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト (拡張範囲)	あり
2000 ～ 2699	IP 拡張アクセス リスト (拡張範囲)	あり



(注) 番号制標準および拡張 ACL のほかに、サポートされている番号を使用することによって、名前付き標準および拡張 IP ACL を作成することもできます。標準 IP ACL の名前は 1 ～ 99、拡張 IP ACL の名前は 100 ～ 199 にできます。番号制リストの代わりに名前付き ACL を使用した場合、名前付きリストからエントリを個別に削除できるという利点があります。

ACL のロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。



(注) ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log キーワードを含む許可 (permit) または拒否 (deny) ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

番号制標準 ACL の作成

番号制標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard] [log]</code>	送信元アドレスおよびワイルドカードを使用して、標準 IPv4 アクセス リストを定義します。 <i>access-list-number</i> は、1 ~ 99 または 1300 ~ 1999 の 10 進数です。 deny または permit を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。 <i>source</i> は、パケットが送られてくるネットワークまたはホストの送信元アドレスです。次のように指定されます。 <ul style="list-style-type: none"> ドット付き 10 進表記で 32 ビットの値 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード any。 <i>source-wildcard</i> の入力は不要です。 <i>source</i> 0.0.0.0 という <i>source</i> および <i>source-wildcard</i> の省略形を表すキーワード host (任意) <i>source-wildcard</i> によって、ワイルドカード ビットが <i>source</i> に適用されます。 (任意) log を指定すると、エン트리と一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除する場合は、**no access-list access-list-number** グローバル コンフィギュレーション コマンドを使用します。番号制アクセス リストから ACE を個別に削除することはできません。



(注)

ACL を作成するときは、ACL の末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストで、対応する IP ホストアドレスの ACL 仕様からマスクを省略した場合、0.0.0.0 がマスクとして使用されます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、それ以外のすべてのホストへのアクセスを許可する標準 ACL を作成し、その結果を表示する例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
```

```
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
 10 deny 171.69.198.102
 20 permit any
```

host 一致条件を指定されたエントリ、および 0.0.0.0 の無視 (*don't care* マスク) を指定されたエントリが、リストの先頭 (ゼロ以外の無視 [*don't care*] マスクを指定されたすべてのエントリの上) に来るように、標準アクセス リストの順序に常にかき換えられます。したがって、**show** コマンドの出力およびコンフィギュレーション ファイルでは、ACE は必ずしも入力した順番に表示されません。

作成した番号制標準 IPv4 ACL は、端末回線 (「[端末回線への IPv4 ACL の適用](#)」(P.35-19) を参照)、インターフェイス (「[インターフェイスへの IPv4 ACL の適用](#)」(P.35-20) を参照)、または VLAN (「[VLAN マップの設定](#)」(P.35-31) を参照) に適用できます。

番号制拡張 ACL の作成

標準 ACL の場合、一致基準には送信元アドレスだけが使用されますが、拡張 ACL では送信元および宛先アドレスとともに、オプションとしてプロトコル タイプ情報を使用して照合できるので、より細かな制御が可能です。番号制拡張アクセス リストで ACE を作成する場合、ACL の作成後に追加したものは、リストの末尾に組み込まれることに注意してください。番号制リストの場合、リストを並べ替えたり、ACE を選択して追加したり削除したりはできません。

プロトコルによっては、そのプロトコルに適用される特定のパラメータおよびキーワードもあります。

次の IP プロトコルがサポートされています (プロトコル キーワードはカッコ内の太字)。

Authentication Header Protocol (**ahp**)、Enhanced Interior Gateway Routing Protocol (**eigrp**)、Encapsulation Security Payload (**esp**)、Generic Routing Encapsulation (**gre**)、ICMP (**icmp**)、IGMP (**igmp**)、任意の Interior Protocol (**ip**)、IP in IP トンネリング (**ipinip**)、KA9Q NOS 互換 IP over IP トンネリング (**nos**)、Open Shortest Path First ルーティング (**ospf**)、Payload Compression Protocol (**pcp**)、Protocol Independent Multicast (**pim**)、TCP (**tcp**)、または UDP (**udp**)



(注) ICMP エコー応答はフィルタリングできません。他のすべての ICMP コードまたはタイプはフィルタリングできます。

各プロトコルの特定のキーワードに関する詳細は、次のコマンドリファレンスを参照してください。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』 Release 12.2
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』 Release 12.2

これらのマニュアルは、Cisco.com ホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) にあります。



(注) スイッチは、動的アクセス リストまたは再帰アクセス リストをサポートしていません。また、**minimize-monetary-cost** Type of Service (ToS; サービス タイプ) ビットに基づくフィルタリングもサポートしていません。

サポートされているパラメータは、TCP、UDP、ICMP、IGMP、または他の IP のカテゴリにグループ化できます。

拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2a access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] (注) dscp 値を入力した場合は、 tos または precedence を入力できません。 dscp を入力しない場合は、 tos と precedence を両方とも入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 access-list-number は、100 ~ 199 または 2000 ~ 2699 の 10 進数です。 deny または permit を入力し、条件と一致した場合にパケットを拒否するか、または許可するかを指定します。 protocol には、IP プロトコルの名前または番号を入力します。指定には、 ahp 、 eigrp 、 esp 、 gre 、 icmp 、 igmp 、 igrp 、 ip 、 ipinip 、 nos 、 ospf 、 pcp 、 pim 、 tcp 、 udp 、または IP プロトコル番号を表す 0 ~ 255 の整数を使用できます。すべての IP (ICMP、TCP、および UDP を含む) と照合する場合は、キーワード ip を使用します。 (注) このステップでは、ほとんどの IP プロトコルに対応するオプションを指定します。TCP、UDP、ICMP、および IGMP の具体的なパラメータについては、ステップ 2b ~ 2e を参照してください。 source は、パケットの送信元であるネットワークまたはホストの番号です。 source-wildcard によって、ワイルドカード ビットが source に適用されます。 destination は、パケットの宛先ネットワークまたはホストの番号です。 destination-wildcard によって、ワイルドカード ビットが destination に適用されます。 source 、 source-wildcard 、 destination 、および destination-wildcard は、次の 3 つの方法で指定できます。 <ul style="list-style-type: none"> • ドット付き 10 進表記で 32 ビットの値 • 0.0.0.0 255.255.255.255 を表すキーワード any (任意のホスト) • 単一のホスト 0.0.0.0 を表すキーワード host その他のキーワードは任意であり、次の意味があります。 <ul style="list-style-type: none"> • precedence : 0 ~ 7 の番号または名前で指定された優先順位を使用して、パケットを照合します。使用できる名前および番号は、routine (0)、priority (1)、immediate (2)、flash (3)、flash-override (4)、critical (5)、internet (6)、network (7) です。 • fragments : 先頭以外のフラグメントをチェックします。 • tos : 0 ~ 15 の番号または名前で指定された ToS レベルを使用して照合します。使用できる名前および番号は、normal (0)、max-reliability (2)、max-throughput (4)、min-delay (8) です。 • log : エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。 • time-range : このキーワードの説明については、「ACL での時間範囲の使用法」(P.35-17) を参照してください。 • dscp : 0 ~ 63 の番号で指定された DSCP 値を使用してパケットを比較します。疑問符 (?) を使用すると、使用可能な値のリストが表示されます。

コマンド	目的
または access-list <i>access-list-number</i> { deny permit } <i>protocol</i> any any [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	アクセス リスト コンフィギュレーション モードで、 source と source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用するか、または destination と destination-wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよびワイルドカードの代わりに、 any キーワードを使用できます。
または access-list <i>access-list-number</i> { deny permit } <i>protocol</i> host <i>source</i> host <i>destination</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	source と source-wildcard ワイルドカードの値 <i>source</i> 0.0.0.0 の省略形を使用するか、または destination と destination-wildcard の値 <i>destination</i> 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに、 host キーワードを使用できます。
ステップ 2b access-list <i>access-list-number</i> { deny permit } tcp <i>source</i> <i>source-wildcard</i> [<i>operator</i> <i>port</i>] <i>destination</i> <i>destination-wildcard</i> [<i>operator</i> <i>port</i>] [established] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>] [<i>flag</i>]	(任意) 拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。 次に示す例外を除き、ステップ 2a の説明にあるパラメータと同じパラメータを使用します。 (任意) <i>operator</i> および <i>port</i> を入力すると、送信元ポート (<i>source source-wildcard</i> の後ろに入力した場合) または宛先ポート (<i>destination destination-wildcard</i> の後ろに入力した場合) が比較されます。使用可能な演算子は eq (等しい)、 gt (より大きい)、 lt (より小さい)、 neq (等しくない)、 range (包含範囲) などです。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。 <i>port</i> にポート番号を 10 進数 (0 ~ 65535) として入力するか、または TCP ポート名を入力します。TCP ポート名を参照する場合は、? を使用するか、『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときは、TCP ポートの番号または名前のみを使用します。 他のオプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • established : 確立された接続と照合します。このキーワードは、ack または rst フラグを指定した場合の一致検索機能と同じです。 • flag : 指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、ack (確認応答)、fin (終了)、psh (プッシュ)、rst (リセット)、syn (同期)、または urg (緊急) です。
ステップ 2c access-list <i>access-list-number</i> { deny permit } udp <i>source</i> <i>source-wildcard</i> [<i>operator</i> <i>port</i>] <i>destination</i> <i>destination-wildcard</i> [<i>operator</i> <i>port</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	(任意) 拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、 udp を入力します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[<i>operator</i> [<i>port</i>]] ポート番号またはポート名は、UDP ポートの番号または名前であればなりません。また、UDP の場合、 flag および established パラメータは無効です。

コマンド	目的
ステップ 2d access-list <i>access-list-number</i> {deny permit} icmp <i>source</i> <i>source-wildcard destination</i> <i>destination-wildcard</i> [<i>icmp-type</i> [[<i>icmp-type icmp-code</i>] <i>icmp-message</i>]] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	(任意) 拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、 icmp を入力します。 ICMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <i>icmp-type</i> : ICMP メッセージタイプを基準にしてフィルタリングします。0 ~ 255 の値を使用できます。 <i>icmp-code</i> : ICMP メッセージコードタイプを基準にしてフィルタリングします。0 ~ 255 の値を使用できます。 <i>icmp-message</i> : ICMP メッセージタイプ名または ICMP メッセージのタイプ名およびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージタイプ名およびコード名のリストを参照する場合は、? を使用するか、『Cisco IOS IP Configuration Guide』Release 12.2 の「Configuring IP Services」を参照してください。
ステップ 2e access-list <i>access-list-number</i> {deny permit} igmp <i>source</i> <i>source-wildcard destination</i> <i>destination-wildcard</i> [<i>igmp-type</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [log-input] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	(任意) 拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP の場合は、 igmp を入力します。 IGMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 <i>igmp-type</i> : IGMP メッセージタイプと照合するには、0 ~ 15 の番号またはメッセージ名 (dvmrp 、 host-query 、 host-report 、 pim 、または trace) を入力します。
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show access-lists [<i>number</i> <i>name</i>]	アクセス リストの設定を確認します。
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リスト全体を削除する場合は、**no access-list access-list-number** グローバル コンフィギュレーション コマンドを使用します。番号制アクセス リストから ACE を個別に削除することはできません。

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを禁止し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します (**eq** キーワードを宛先アドレスのあとに指定すると、Telnet に対応する TCP 宛先ポート番号がテストされます)。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
  10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
  20 permit tcp any any
```

ACL の作成後に (端末から入力するなどして) 追加したものは、リストの末尾に組み込まれます。番号制アクセス リストの特定の場所に ACE を追加または削除することはできません。



(注)

ACL を作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号制拡張 ACL は、端末回線（「[端末回線への IPv4 ACL の適用](#)」(P.35-19) を参照）、インターフェイス（「[インターフェイスへの IPv4 ACL の適用](#)」(P.35-20) を参照）、または VLAN（「[VLAN マップの設定](#)」(P.35-31) を参照）に適用できます。

ACL 内の ACE シーケンスの再編集

新しく ACL を作成すると、アクセス リスト内のエントリのシーケンス番号が自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、ACL のシーケンス番号を編集したり、適用する ACE の順番を変更したりできます。たとえば、ACL に新規 ACE を追加した場合、その ACE はリストの一番下に配置されます。その場合、シーケンス番号を変更することで、ACL 内の ACE を異なる場所に移動できます。

ip access-list resequence コマンドの詳細については、次の URL にアクセスしてください。

http://preview.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a60.html

名前付き標準および拡張 ACL の作成

番号ではなく英数字のストリング（名前）で、IPv4 ACL を特定できます。名前付き ACL を使用すると、番号制アクセス リストの場合より多くの IPv4 アクセス リストをスイッチ上で設定できます。番号ではなく名前でアクセス リストを指定する場合、モードとコマンド構文が多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドが名前付きアクセス リストを受け入れるわけではありません。



(注)

標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ~ 99、拡張 IP ACL の名前は 100 ~ 199 にできます。番号制リストの代わりに名前付き ACL を使用した場合、名前付きリストからエントリを個別に削除できるという利点があります。

名前付き ACL を設定する前に、次の注意事項と制限事項を考慮してください。

- 番号制 ACL を受け入れるすべてのコマンドが、名前付き ACL を受け入れるわけではありません。インターフェイスの packets フィルタおよびルート フィルタ用の ACL では、名前を使用できません。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前を使用することはできません。
- 「[標準および拡張 IPv4 ACL の作成](#)」(P.35-8) で説明したとおり、番号制 ACL を使用することもできます。
- VLAN マップには、標準 ACL および拡張 ACL（名前付きまたは番号制）を使用できます。

名前付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list standard name</code>	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前は、1 ~ 99 の番号にできます。
ステップ 3	<code>deny {source [source-wildcard] host source any} [log]</code> または <code>permit {source [source-wildcard] host source any} [log]</code>	アクセス リスト コンフィギュレーション モードで、パケットを転送するの否を決定する、拒否条件または許可条件を 1 つまたは複数指定します。 <ul style="list-style-type: none"> • host source : source と source-wildcard の値 source 0.0.0.0 • any : source と source-wildcard の値 0.0.0.0 255.255.255.255
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

名前付き標準 ACL を削除するには、`no ip access-list standard name` グローバル コンフィギュレーション コマンドを使用します。

名前付き拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list extended name</code>	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前は、100 ~ 199 の番号にできます。
ステップ 3	<code>{deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host destination any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</code>	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。 <code>log</code> キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 プロトコルおよび他のキーワードの定義については、「 番号制拡張 ACL の作成 」(P.35-11) を参照してください。 <ul style="list-style-type: none"> • host source : source と source-wildcard の値 source 0.0.0.0 • host destination : destination と destination-wildcard の値 destination 0.0.0.0 • any : source と source-wildcard の値、または destination と destination-wildcard の値である 0.0.0.0 255.255.255.255
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

名前付き拡張 ACL を削除するには、`no ip access-list extended name` グローバル コンフィギュレーション コマンドを使用します。

標準または拡張 ACL を作成するときは、ACL の末尾に暗黙的な拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL で、対応する IP ホストアドレスのアクセスリスト仕様に基づくマスクを指定しなかった場合、0.0.0.0 がマスクとみなされます。

ACL の作成後に行った追加は、リストの末尾に組み込まれます。ACE を選択的に特定の ACL に追加することはできません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセスリスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号制 ACL ではなく名前付き ACL を使用する理由の 1 つは、名前付き ACL から行を選択して削除できるためです。

作成した名前付き ACL は、インターフェイス（「[インターフェイスへの IPv4 ACL の適用](#)」(P.35-20) を参照）または VLAN（「[VLAN マップの設定](#)」(P.35-31) を参照）に適用できます。

ACL での時間範囲の使用法

time-range グローバル コンフィギュレーション コマンドを使用することによって、曜日および時刻に基づいて拡張 ACL を選択的に適用できます。最初に時間範囲の名前を定義して、時間範囲の時刻および日付、または曜日を設定します。この時間範囲名は、ACL を適用してアクセスリストに制限を設定するときに入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内、指定曜日など）を定義できます。**time-range** キーワードおよび引数については、「[標準および拡張 IPv4 ACL の作成](#)」(P.35-8) および「[名前付き標準および拡張 ACL の作成](#)」(P.35-15) に記載されている、名前付きおよび番号制拡張 ACL の手順を参照してください。

時間範囲を使用する利点の一部を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザアクセスをより厳密に許可または拒否できます。
- ログメッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセスリストを使用すると、CPU に負荷が生じます。これは、アクセスリストの新規設定を他の機能や、Ternary CAM (TCAM) にロードされた結合済みの設定とマージする必要があるためです。このため、複数のアクセスリストが短期間に連続して（互いに数分以内に）有効となるような設定を行わないように注意する必要があります。



(注)

時間範囲には、スイッチのシステムクロックが使用されます。したがって、信頼できるクロックソースが必要です。Network Time Protocol (NTP) を使用してスイッチクロックを同期させることを推奨します。詳細については、「[システム日時の管理](#)」(P.7-1) を参照してください。

ACL の時間範囲パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	time-range <i>time-range-name</i>	作成する時間範囲には意味のある名前 (<i>workhours</i> など) を割り当て、 time-range コンフィギュレーション モードを開始します。名前にスペースまたは疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 3	absolute [start time date] [end time date] または periodic <i>day-of-the-week hh:mm to [day-of-the-week] hh:mm</i> または periodic {weekdays weekend daily} <i>hh:mm to hh:mm</i>	適用する機能がいつ動作可能になるかを指定します。 <ul style="list-style-type: none">時間範囲には、absolute ステートメントを 1 つのみ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。複数の periodic ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show time-range	時間範囲の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

複数の項目を別々の時間で有効にする場合は、上記の手順を繰り返してください。

設定した時間範囲の制限を削除するには、**no time-range *time-range-name*** グローバル コンフィギュレーション コマンドを使用します。

次に、*workhours* (営業時間) の時間範囲および会社の休日 (2006 年 1 月 1 日) を設定し、設定確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に、時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
    10 deny tcp any any time-range new_year_day_2006 (inactive)
    20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して、同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
 10 permit ip any any
Extended IP access list deny_access
 10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
 10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入

remark キーワードを使用すると、エントリに関するコメント（注釈）を任意の IP 標準または拡張 ACL に組み込むことができます。コメントを使用すると、ACL エントリの理解とスキャンが容易になります。1 つのコメント行は 100 文字までです。

コメントは許可 (**permit**) ステートメントまたは拒否 (**deny**) ステートメントの前後どちらにでも配置できます。コメントがどの許可ステートメントまたは拒否ステートメントの説明であるのかが明白になるように、コメントの位置には一貫性が必要です。たとえば、一部のコメントは対応する許可または拒否ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあるという状況は、混乱の原因となります。

番号制の IP 標準または拡張 ACL にコメントを挿入するには、**access-list access-list number remark remark** グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、**no** 形式のコマンドを使用します。

次の例では、Jones のワークステーションにアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリに関しては、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、**no** 形式のコマンドを使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されていません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

端末回線への IPv4 ACL の適用

番号制 ACL を使用すると、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

インターフェイスへの ACL の適用の手順については、「[インターフェイスへの IPv4 ACL の適用](#)」(P.35-20) を参照してください。VLAN への ACL の適用については、「[VLAN マップの設定](#)」(P.35-31) を参照してください。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>line [console vty] line-number</code>	設定する回線を特定し、インライン コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> console : コンソール端末回線を指定します。コンソール ポートは Data Communications Equipment (DCE; データ通信装置) です。 vty : リモート コンソール アクセス用の仮想端末を指定します。 <i>line-number</i> は、回線タイプを指定する場合、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ~ 16 です。
ステップ 3	<code>access-class access-list-number {in out}</code>	(デバイスに対する) 特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信および発信接続を制限します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

端末回線から ACL を削除するには、`no access-class access-list-number {in | out}` ライン コンフィギュレーション コマンドを使用します。

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。以下の注意事項に留意してください。

- ACL は着信レイヤ 2 ポートにだけ適用してください。
- レイヤ 3 インターフェイスの場合は、ACL を着信または発信のいずれかの方向に適用します。
- インターフェイスへのアクセスを制御する場合、名前付きまたは番号制 ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットのみがフィルタリングされます。レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にのみルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。



(注) パケットがアクセス グループによって拒否された場合、デフォルトでは、ルータは ICMP 到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアで廃棄されず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定する特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス (ポート ACL) またはレイヤ 3 インターフェイス (ルータ ACL) を指定できます。
ステップ 3	<code>ip access-group {access-list-number name} {in out}</code>	指定したインターフェイスへのアクセスを制御します。 out キーワードはレイヤ 2 インターフェイス (ポート ACL) ではサポートされません。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定されたアクセス グループを削除するには、**no ip access-group {access-list-number | name} {in | out}** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートにアクセス リスト 2 を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config)# interface gigabitethernet0/1Switch(config-if)# ip access-group 2 in
```



(注) **ip access-group** インターフェイス コンフィギュレーション コマンドをレイヤ 3 インターフェイス (SVI、レイヤ 3 EtherChannel、またはルーテッド ポート) に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ 3 アクセス グループは、CPU のレイヤ 3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

着信 ACL の場合、パケットの受信後に、スイッチはパケットを ACL と照合します。ACL がパケットを許可していると、スイッチはパケットの処理を継続します。ACL がパケットを拒否していると、スイッチはパケットを廃棄します。

発信 ACL の場合、パケットを受信し、制御対象インターフェイスに送信したあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可していると、スイッチはパケットを送信します。ACL がパケットを拒否していると、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または出力インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断して処理を行い、すべてのパケットが許可されてしまいます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

IP ACL のハードウェアおよびソフトウェアの処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には CPU に転送してソフトウェア処理を行う必要があるものもあります。ハードウェアで ACL コンフィギュレーションを保存する容量がいっぱいになると、パケットは転送のために CPU に送信されます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックより大幅に低くなります。



(注)

スタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受ける (ソフトウェアで転送される) のは、スイッチに着信した該当 VLAN 内のトラフィックのみです。パケットのソフトウェア転送が発生すると、消費される CPU サイクル数に応じて、スイッチ スタックのパフォーマンスが低下することがあります。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー (許可フローと拒否フロー) の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

ルータ ACL の設定をハードウェアに適用できない場合、VLAN に着信したルーティング対象パケットはソフトウェアでルーティングされますが、ブリッジングはハードウェアで行われます。ACL により多数のパケットが CPU へ送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドを入力しても、表示される一致カウントはハードウェアで制御されるアクセスのパケットを表示しません。スイッチドおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

ACL のトラブルシューティング

この ACL マネージャのメッセージが表示され、[chars] がアクセス リスト名の場合、次のようなメッセージが表示されます。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

スイッチには、ACL をハードウェアで表現するのに十分なリソースがありません。リソースには、ハードウェア メモリとラベル スペースが含まれていますが、CPU メモリは含まれていません。この問題は、使用可能な LOU または特定のハードウェア リソースの不足によって発生します。LOU は TCP によるフラグ照合、または、TCP、UDP、SCTP ポート番号での **eq** 以外のテスト (**ne**、**gt**、**lt**、または **range**) で必要になります。

回避策として、次のいずれかの方法を使用します。

- ACL 設定を変更して使用するリソースを減らす。
- ACL 名に付加された英数字を、その英数字に先行する英数字に置き換えて ACL 名を変更する。

特定のハードウェア リソースを使用するには、**show platform layer4 acl map** 特権 EXEC コマンドを使用します。スイッチに使用可能なリソースがない場合、**index 0 ~ index 15** は使用できないと出力されます。

リソースが不足した状態で ACL を設定する方法の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

たとえば、この ACL を次のようにインターフェイスに適用します。

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

そして、次のメッセージが表示された場合、

```
ACL MGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグに関連する演算子は使用できません。この問題は、次のように回避します。

- **ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、4 番目の ACE を 1 番目の ACE の前に移動する。

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

または

- ACL 名を、他の ACL 名に付加された英数字よりも先行する英数字に置き換えて変更する（たとえば、ACL 79 を ACL 1 に変更する）。

これで、ACL の 1 番目の ACE をインターフェイスに適用できます。スイッチは ACE を Opselect index の利用可能なマッピング ビットに割り当て、次に、TCAM で同じビット数を使用するためにフラグに関連する演算子を割り当てます。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- **ip unreachable** がディセーブルの場合、log を指定しないと、セキュリティ ACL の拒否ステートメントと一致するフローがハードウェアによって廃棄されます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングのみが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

IPv4 ACL の設定例

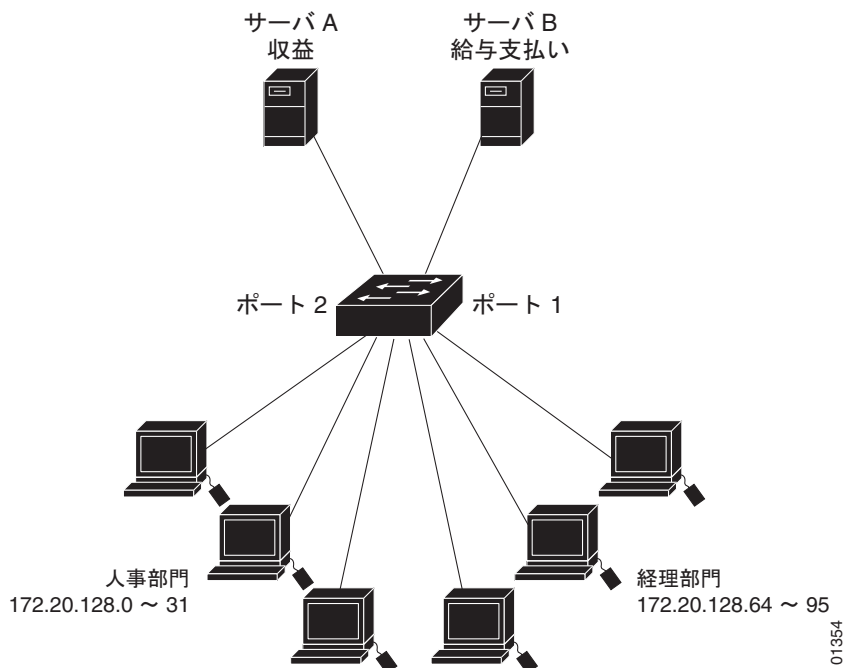
ここでは、IPv4 ACL の設定および適用例を示します。ACL のコンパイルに関する詳細については、『Cisco IOS Security Configuration Guide』Release 12.2、および『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。

図 35-3 に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングする。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングする。

図 35-3 ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ~ 172.20.128.95 から送信されるトラフィックのみを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
 10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ~ 172.20.128.95 に送信されるトラフィックのみを許可する例を示します。この ACL は、ルーテッド ポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックのみを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル (IP) を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
 10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 106 in
```


番号制 ACL

次の例のネットワーク 36.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネットマスクは 255.255.0.0 です。ネットワーク アドレス 36.0.0.0 の 3 番めおよび 4 番目のオクテットは、特定のホストを指定します。アクセスリスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセスリストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。ACL はポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番目の行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番目の行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

この例では、インターネットに接続されたネットワークがあり、ネットワーク上の任意のホストが、インターネット上の任意のホストと TCP 接続を確立できるようにする場合を考えます。ただし、IP ホストには、専用メール ホストのメール (SMTP) ポート接続を除いて、ネットワーク上のホストへの TCP 接続は設定しないものとします。

SMTP は、接続の一端では TCP ポート 25、もう一方ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できません。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致とみなされます。スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL

次に、*internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスと宛先ワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ~ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL に適用される時間範囲

次の例では、月曜日から金曜日までの午前 8 時～午後 6 時（18 時）の間、IP 上の HTTP トラフィックを拒否します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。（20:00）。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリ

次に示す番号指定 ACL の例では、Jones のワークステーションにアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号制 ACL の例では、Winter および Smith のワークステーションでの Web 閲覧が禁止されます。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにはアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットには発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL のロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged
```

Log Buffer (4096 bytes):

```
00:00:48: NTP: authentication delay calculation problems
```

<output truncated>

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOGDP で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1
0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が追加されません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0),
1 packet
```

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。手順については、他の名前付き拡張 ACL を設定する場合と同様です。



(注)

レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

mac access-list extended コマンドでサポートされている非 IP プロトコルの詳細については、このリリースのコマンド リファレンスを参照してください。



(注)

appletalk はコマンドラインのヘルプに表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

名前付き MAC 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 mac access-list extended name	名前を使用して拡張 MAC アクセス リストを定義します。
ステップ 3 {deny permit} {any host source MAC address source MAC address mask} {any host destination MAC address destination MAC address mask} [type mask lsap lsap mask aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos cos]	<p>拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての (any) 送信元 MAC アドレス、マスク付きの送信元 MAC アドレス、または特定のホスト (host) 送信元 MAC アドレス、およびすべての (any) 宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、permit または deny を指定します。</p> <p>(任意) 次のオプションを入力することもできます。</p> <ul style="list-style-type: none"> type mask : Ethernet II または SNAP でカプセル化されたパケットの任意の Ethertype 番号。10 進数、16 進数、または 8 進数で表記できます。Ethertype に適用される <i>don't care</i> ビットの任意のマスクが付加されて、一致検査が行われます。 lsap lsap mask : IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。 <i>don't care</i> ビットの任意のマスクが付加されます。 aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp : 非 IP プロトコル cos cos : プライオリティを設定するために使用される、0 ~ 7 の IEEE 802.1Q CoS 番号
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show access-lists [number name]	アクセス リストの設定を表示します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除する場合は、**no mac access-list extended name** グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、他のすべてのタイプのトラフィックを許可する、*mac1* という名前のアクセス リストを作成して表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny any any decnet-iv
    20 permit any any
```

レイヤ 2 インターフェイスへの MAC ACL の適用

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用する場合は、次の注意事項を考慮してください。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- 同じレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。IP アクセス リストは IP パケットのみをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換えられます。

レイヤ 2 インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイス (ポート ACL) でなければなりません。
ステップ 3	<code>mac access-group {name} {in}</code>	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は、着信方向のみサポートします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mac access-group [interface interface-id]</code>	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定したアクセス グループを削除するには、`no mac access-group {name}` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートにアクセス リスト `mac1` を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Router(config-if)# mac access-group mac1 in
```



(注)

`mac access-group` インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用された場合のみ有効となります。このコマンドを EtherChannel ポート チャネルには使用できません。


パケットの受信後に、スイッチは着信 ACL とパケットを照合します。ACL がパケットを許可すると、スイッチはパケットの処理を継続します。ACL がパケットを拒否すると、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断して処理を行い、すべてのパケットが許可されてしまいます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

VLAN マップの設定

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケットタイプ (IP または MAC) に対する **match** コマンドがある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットは廃棄されます。該当パケットタイプに対する **match** コマンドがない場合、デフォルトでは、パケットが転送されます。

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

-
- ステップ 1** VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。「標準および拡張 IPv4 ACL の作成」(P.35-8) および「VLAN マップの作成」(P.35-33) を参照してください。
- ステップ 2** VLAN ACL マップ エントリを作成するには、**vlan access-map** グローバル コンフィギュレーション コマンドを入力します。
- ステップ 3** アクセス マップ コンフィギュレーション モードでは、**action** として、**forward** (デフォルト) または **drop** を入力することもできます。また、**match** コマンドを入力して、既知の MAC アドレスのみが格納された IP パケットまたは非 IP パケットを指定したり、1 つまたは複数の ACL (標準または拡張) とパケットを照合したりすることもできます。
-
-  **(注)** パケットタイプ (IP または MAC) に対する **match** コマンドが VLAN マップにあつてマップアクションが廃棄された場合、タイプが一致するすべてのパケットが廃棄されます。VLAN マップに **match** コマンドがなく、設定されたアクションが廃棄された場合、すべての IP および レイヤ 2 パケットが廃棄されます。
-
- ステップ 4** VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** グローバル コンフィギュレーション コマンドを使用します。
-

ここでは、次の設定情報について説明します。

- 「VLAN マップの設定時の注意事項」(P.35-32)
- 「VLAN マップの作成」(P.35-33)
- 「VLAN への VLAN マップの適用」(P.35-35)
- 「ネットワークでの VLAN マップの使用法」(P.35-36)

VLAN マップの設定時の注意事項

VLAN マップを設定するときには、次の注意事項に従ってください。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケットタイプ (IP または MAC) に対する match コマンドが VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match コマンドに一致しない場合、デフォルトではパケットが廃棄されます。該当パケットタイプに対する match コマンドが VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまたは MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットをソフトウェアでブリッジングおよびルーティングする必要があります。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
 - ホスト ポートから混合ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
 - 混合ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN の両方に適用します。プライベート VLAN の詳細については、[第 17 章「プライベート VLAN の設定」](#)を参照してください。

設定例については、「[ネットワークでの VLAN マップの使用法](#)」(P.35-36) を参照してください。

ルータ ACL および VLAN マップを組み合わせて使用方法については、「[VLAN マップとルータ ACL の設定時の注意事項](#)」(P.35-38) を参照してください。

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>vlan access-map name [number]</code>	VLAN マップを作成し、名前および番号（任意）を指定します。番号は、マップ内のエントリの順序を表す数字です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、目的のマップ エントリの番号を入力できます。 このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。
ステップ 3	<code>action {drop forward}</code>	(任意) マップ エントリに対するアクションを設定します。デフォルトは転送 (forward) です。
ステップ 4	<code>match {ip mac} address {name number} [name number]</code>	1 つまたは複数の標準または拡張アクセス リストに対してパケットを照合します (IP または MAC アドレスを使用)。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してのみ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してのみ照合されません。
ステップ 5	<code>end</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マップを削除するには、`no vlan access-map name` グローバル コンフィギュレーション コマンドを使用します。マップ内のシーケンス エントリを 1 つ削除するには、`no vlan access-map name number` グローバル コンフィギュレーション コマンドを使用します。

デフォルトのアクションである転送を行うには、`no action` アクセス マップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の `permit` または `deny` キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションを廃棄に設定します。ACL 内の `permit` は、一致するという意味です。ACL 内の `deny` は、一致しないという意味です。

ACL および VLAN マップの例

次に、特定の目的のための ACL および VLAN マップを作成する例を示します。

例 1

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、`ip1` ACL (TCP パケット) に一致するすべてのパケットが廃棄されます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する `ip1ACL` を作成します。VLAN マップには IP パケットに対する `match` コマンドが存在するため、デフォルトのアクションでは、どの `match` コマンドとも一致しない IP パケットがすべて廃棄されます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL と一致しないすべての IP パケット (TCP でも UDP でもないパケット) が廃棄されます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

例 2

次の例の VLAN マップでは、デフォルトで IP パケットが廃棄され、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットが廃棄されます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットが廃棄されます。
- すべての非 IP パケットが転送されます。

```
Switch(config)# access-list 101 permit tcp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例 3

次の例の VLAN マップでは、デフォルトで MAC パケットが廃棄され、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットが廃棄されます。

- すべての IP パケットが転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例 4

次の例の VLAN マップでは、デフォルトですべてのパケット (IP および非 IP) が廃棄されます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットが廃棄されます。
- その他のすべての MAC パケットが廃棄されます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan filter mapname vlan-list list	VLAN マップを 1 つまたは複数の VLAN ID に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12, 22, 30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 3	show running-config	アクセス リストの設定を表示します。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN マップを削除するには、**no vlan filter mapname vlan-list list** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN マップ 1 を VLAN 20 ~ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

ネットワークでの VLAN マップの使用法

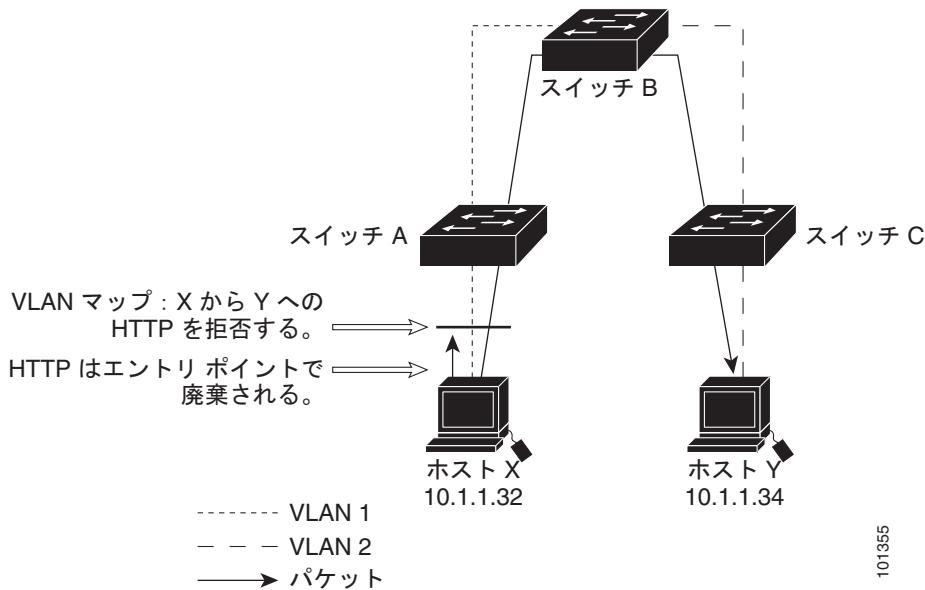
ここでは、一般的な VLAN マップの使用法について一部説明します。

- 「ワイヤリング クローゼットの設定」(P.35-36)
- 「別の VLAN にあるサーバへのアクセスの拒否」(P.35-37)

ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成におけるスイッチでは、ルーティングがイネーブルでない可能性があります。ただし、この構成でも、VLAN マップおよび QoS 分類 ACL はサポートされています。
 図 35-4 では、ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリング クローゼット スイッチ A およびスイッチ C に接続されていると想定しています。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。

図 35-4 ワイヤリング クローゼットの設定



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) に向かうすべての HTTP トラフィックがスイッチ A で廃棄され、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可 (一致) する IP アクセス リスト *http* を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックが廃棄され、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

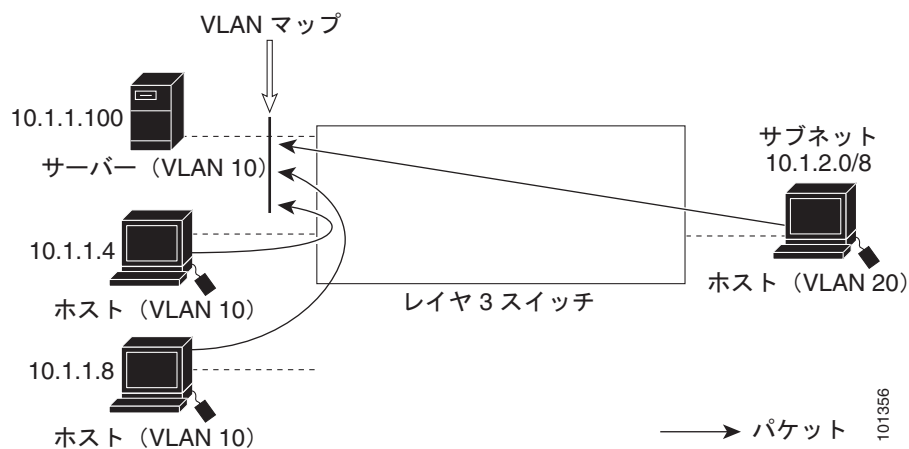
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセスの拒否

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります (図 35-5 を参照)。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 35-5 他 VLAN 上のサーバへのアクセス拒否



次に、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ *SERVER1_ACL* を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップ *SERVER1* を VLAN 10 に適用します。

ステップ 1 正しいパケットと一致する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

- ステップ 2** SERVER1_ACL と一致する IP パケットを廃棄して、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

- ステップ 3** VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

ルータ ACL を VLAN マップと組み合わせて使用する方法

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセス コントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスを制御する VLAN マップを定義できます。

パケットフローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケットフローは拒否されます。



(注)

ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケットタイプ (IP または MAC) に対する match コマンドが VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットが廃棄されます。VLAN マップ内に match ステートメントがなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

ここでは、ルータ ACL を VLAN マップと組み合わせて使用する方法について説明します。

- 「VLAN マップとルータ ACL の設定時の注意事項」 (P.35-38)
- 「VLAN に適用されるルータ ACL と VLAN マップの例」 (P.35-39)

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

スイッチ ハードウェアは、方向 (入力および出力) ごとにセキュリティ ACL を 1 回検索します。したがって、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL と VLAN マップを統合すると、ACE の数が膨大になる場合があります。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイスの方向 (入力および出力) ごとに、設定できる VLAN マップおよびルータ ACL は 1 つのみです。

- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルト アクションのみが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

```
permit...
permit...
permit...
deny ip any any
```

または

```
deny...
deny...
deny...
permit ip any any
```

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

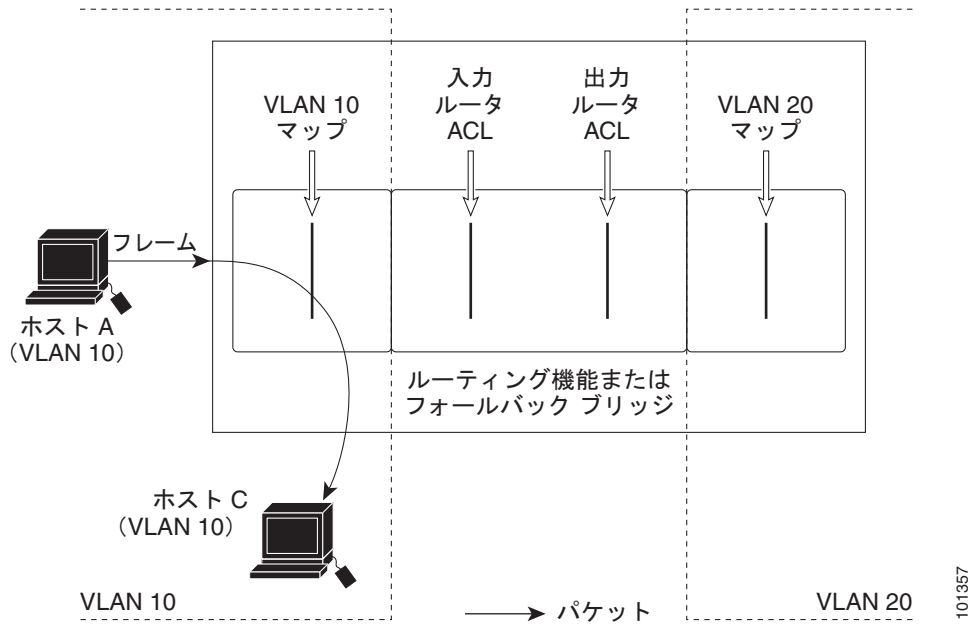
VLAN に適用されるルータ ACL と VLAN マップの例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずに廃棄する可能性もあります。

ACL およびスイッチド パケット

図 35-6 に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。フォールバック ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップのみが適用されます。

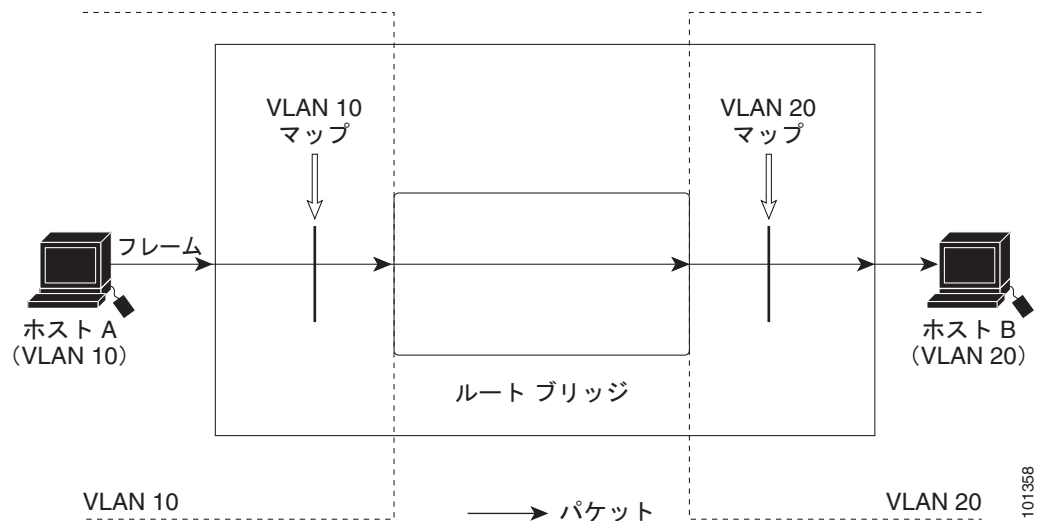
図 35-6 スイッチド パケットへの ACL の適用



ACL およびブリッジド パケット

図 35-7 に、代替ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL のみが適用されます。また、非 IP および非 ARP パケットのみが代替ブリッジド パケットとなります。

図 35-7 ブリッジド パケットへの ACL の適用

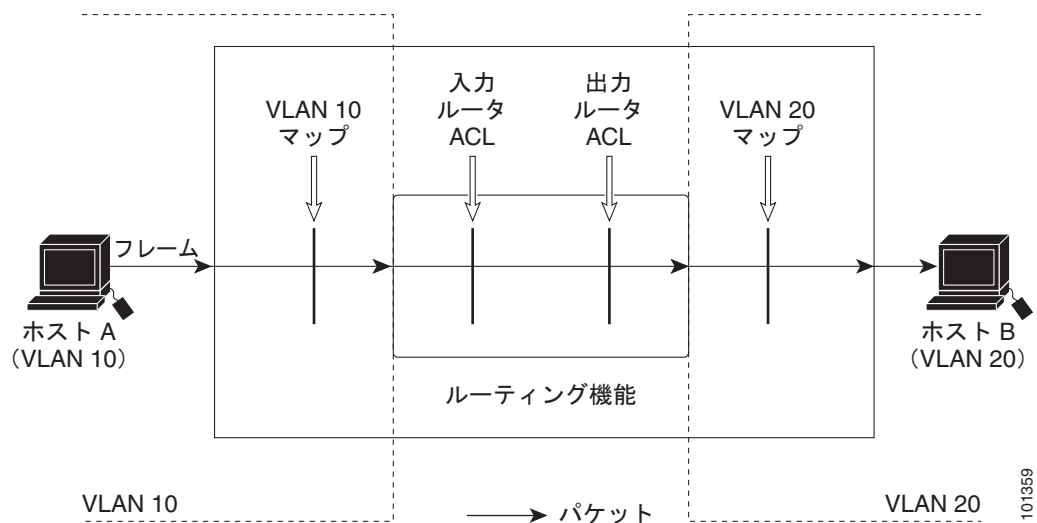


ACL およびルーテッド パケット

図 35-8 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

図 35-8 ルーテッド パケットへの ACL の適用

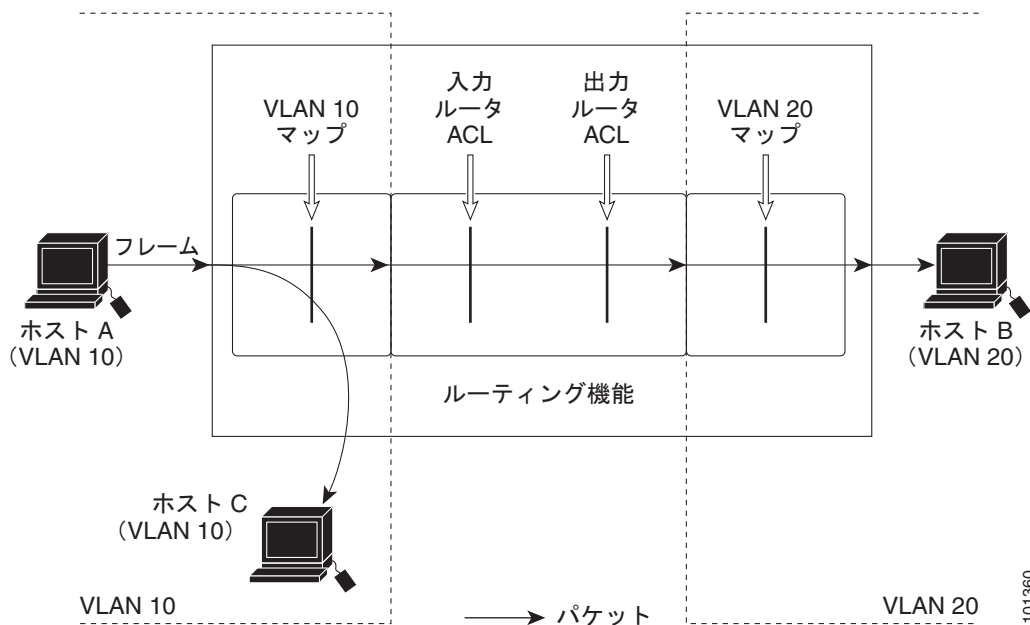


ACL およびマルチキャスト パケット

図 35-9 に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされる場合がありますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。

最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップ (図 35-9 の VLAN 10 マップ) によってパケットが廃棄される場合、パケットのコピーは宛先に送信されません。

図 35-9 マルチキャスト パケットへの ACL の適用



IPv4 ACL の設定の表示

スイッチ上に設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示できます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、特権 EXEC コマンドを使用します (表 35-2 を参照)。

表 35-2 アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
<code>show access-lists [number name]</code>	現在の IP および MAC アドレス アクセス リストの 1 つまたは全体の内容、または特定のアクセス リスト (番号制または名前付き) の内容を表示します。
<code>show ip access-lists [number name]</code>	現在の IP アクセス リスト全体、または特定の IP アクセス リスト (番号制または名前付き) の内容を表示します。
<code>show ip interface interface-id</code>	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、 ip access-group インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
<code>show running-config [interface interface-id]</code>	スイッチまたは特定のインターフェイスのコンフィギュレーション ファイルの内容 (設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたなど) を表示します。
<code>show mac access-group [interface interface-id]</code>	すべてのレイヤ 2 インターフェイスまたは特定のレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

VLAN アクセスマップまたは VLAN フィルタに関する情報も表示できます。VLAN マップ情報を表示するには、表 35-3 に記載された特権 EXEC コマンドを使用します。

表 35-3 VLAN マップ情報を表示するコマンド

コマンド	目的
<code>show vlan access-map [mapname]</code>	すべての VLAN アクセス マップまたは指定されたアクセス マップに関する情報を表示します。
<code>show vlan filter [access-map name vlan vlan-id]</code>	すべての VLAN フィルタに関する情報、または指定された VLAN や VLAN アクセス マップに関する情報を表示します。



CHAPTER 36

QoS の設定

この章では、標準の QoS (Quality of Service) コマンドまたは自動 QoS コマンドを使用して Catalyst 3750 スイッチ上で QoS を設定する方法について説明します。QoS を使用すると、特定のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

QoS は物理ポートおよび Switch Virtual Interfaces (SVI; スイッチ仮想インターフェイス) に設定できます。ポリシー マップを適用するほかに、分類、キューイング、およびスケジューリングなどの QoS を同じ方法で物理ポートおよび SVI に設定します。物理ポートに QoS を設定すると、非階層型のポリシー マップがポートに適用されます。SVI に QoS を設定すると、非階層型、または階層型のポリシー マップが適用されます。Catalyst 3750 Metro スイッチのマニュアルでは、非階層型のポリシー マップは非階層型単一レベルのポリシー マップと呼ばれ、階層型のポリシー マップは階層型デュアル レベルのポリシー マップと呼ばれます。



(注)

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

この章で説明する内容は、次のとおりです。

- 「QoS の概要」 (P.36-2)
- 「自動 QoS の設定」 (P.36-20)
- 「自動 QoS 情報の表示」 (P.36-30)
- 「標準 QoS の設定」 (P.36-31)
- 「標準 QoS 情報の表示」 (P.36-80)

スイッチは、Modular QoS Command Line Interface (MQC; モジュラ QoS コマンドライン インターフェイス) コマンドの一部をサポートします。MQC コマンドの詳細については、次の URL にアクセスし「Modular Quality of Service Command-Line Interface Overview」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd908.html

QoS の概要

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生した場合に、廃棄される可能性についても、すべてのトラフィックで同じです。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、Internet Engineering Task Force (IETF) の新しい規格である Differentiated Services (DiffServ) アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP Type of Service (ToS; サービス タイプ) フィールドの 6 ビットを使用して、分類 (クラス) 情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します (図 36-1 を参照)。

- レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 の ISL (スイッチ間リンク) フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p Class of Service (CoS; サービス クラス) 値を伝達する 1 バイトのユーザ フィールドがあります。レイヤ 2 ISL トランクとして設定されたポートでは、すべてのトラフィックが ISL フレームに取められます。

レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット (ユーザ プライオリティ ビット) で CoS 値が伝達されます。レイヤ 2 IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除くすべてのトラフィックが IEEE 802.1Q フレームに取められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ) です。

- レイヤ 3 パケットのプライオリティ ビット

レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point (DSCP) 値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

IP precedence 値の範囲は 0 ~ 7 です。

DSCP 値の範囲は 0 ~ 63 です。



(注)

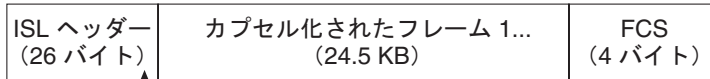
Cisco IOS Release 12.2(52)SE 以降は、デュアル IPv4/IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートとの IPv6 ポートベースの信頼をサポートします。IPv6 が稼動するスイッチの場合は、スイッチにデュアル IPv4/IPv6 テンプレートをリロードする必要があります。詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

図 36-1 フレームおよびパケットにおける QoS 分類レイヤ

カプセル化されたパケット

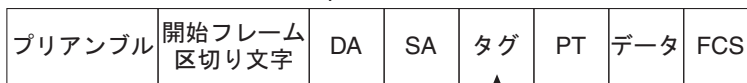


レイヤ 2 ISL フレーム



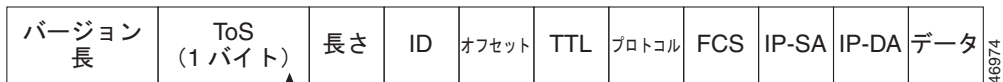
↑ 3 ビットを CoS に使用

レイヤ 2 802.1Q および 802.1p フレーム



↑ 3 ビット (ユーザプライオリティ ビット) を CoS に使用

レイヤ 3 IPv4 パケット



↑ IP precedence または DSCP

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てられるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コアスイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィッククラスに割り当てるリソースの容量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィックタイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

QoS の基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し (分類)、パケットがスイッチを通過するとき所定の QoS を指定するラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ (ポリシングおよびマーキング)、リソース競合が発生する状況に応じて異なる処理 (キューイングおよびスケジューリング) を行う必要があります。また、スイッチから送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります (シェーピング)。

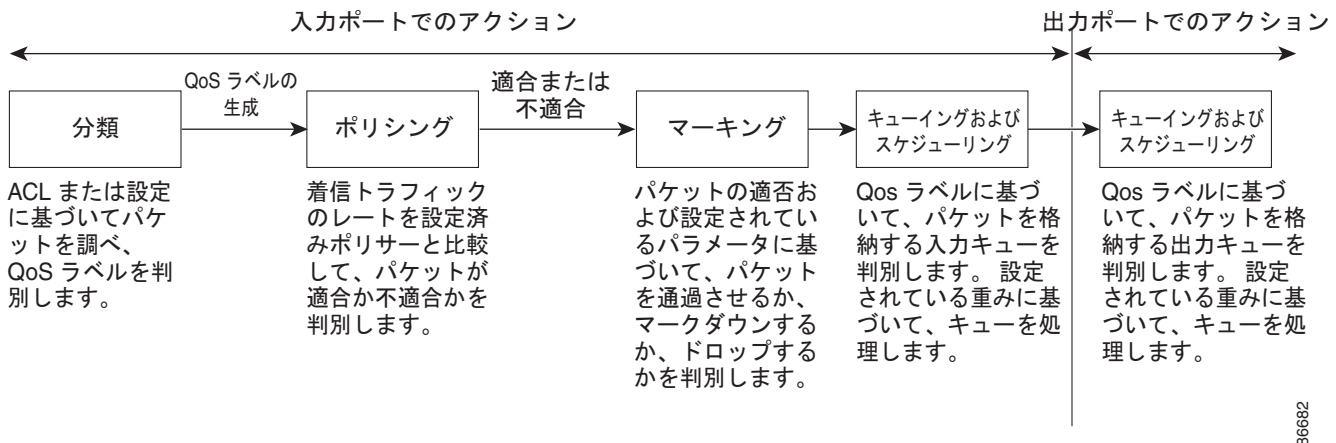
図 36-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。詳細については、「[分類](#)」(P.36-5) を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。詳細については、「[ポリシングおよびマーキング](#)」(P.36-8) を参照してください。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットを廃棄するか）を決定します。詳細については、「[ポリシングおよびマーキング](#)」(P.36-8) を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを 2 つの入力キューのどちらに格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail-Drop (WTD) アルゴリズムによって拡張されます。しきい値を超過している場合、パケットは廃棄されます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.36-13) を参照してください。
- スケジューリングでは、設定されている Shaped Round Robin (SRR) の重みに基づいて、キューを処理します。入力キューの 1 つがプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから他のキューを処理します。詳細については、「[SRR のシェーピングおよび共有](#)」(P.36-14) を参照してください。

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットは廃棄されます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.36-13) を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

図 36-2 QoS の基本モデル



2668

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを決定します。QoS ラベルは信頼設定およびパケットタイプに従ってマッピングされます (図 36-3 (P.36-6) を参照)。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。非 IP トラフィックには、次の分類オプションを使用できます (図 36-3 を参照)。

- 着信フレームの CoS 値を信頼します (ポートが CoS を信頼するように設定します)。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ 2 の ISL フレームヘッダーは、1 バイトのユーザフィールドの下位 3 ビットで CoS 値を伝達します。レイヤ 2 IEEE 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0 (ロープライオリティ) ~ 7 (ハイプライオリティ) です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
- 設定されたレイヤ 2 の MAC (メディア アクセス制御) Access Control List (ACL; アクセスコントロールリスト) に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

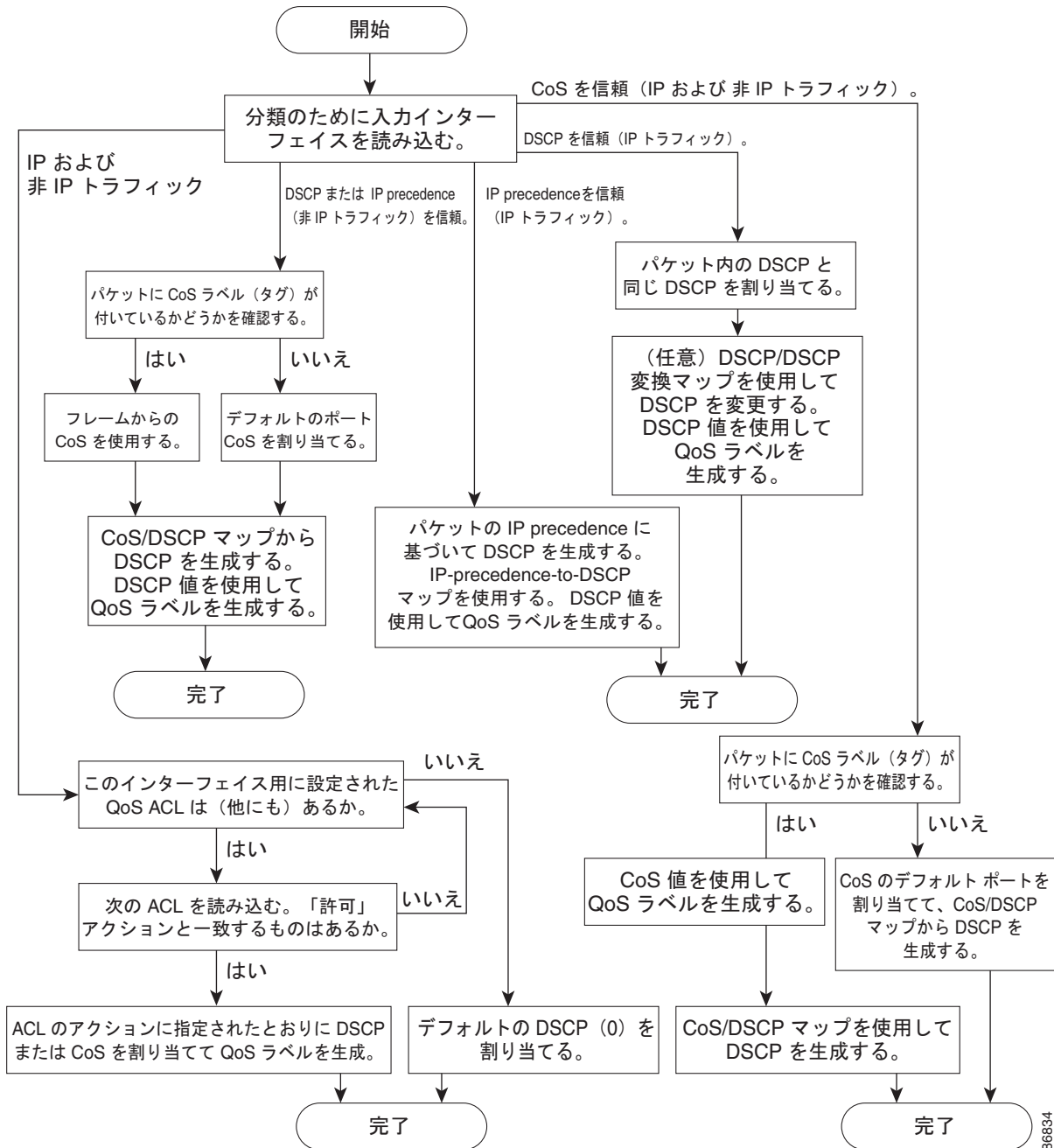
IP トラフィックには、次の分類オプションを使用できます (図 36-3 を参照)。

- 着信パケットの DSCP 値を信頼し (DSCP を信頼するようにポートを設定し)、同じ DSCP 値をパケットに割り当てます。IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ~ 63 です。
2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。
- 着信パケットの IP precedence 値を信頼し (IP precedence を信頼するようにポートを設定し)、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。IP precedence 値の範囲は 0 (ロープライオリティ) ~ 7 (ハイプライオリティ) です。
- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
- 設定された IP 標準 ACL または IP 拡張 ACL (IP ヘッダーの各フィールドを調べる) に基づいて、分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」(P.36-12) を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態による分類の設定」(P.36-37) を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 36-3 分類フローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケットグループ（クラス）を定義できます。QoS のコンテキストでは、Access Control Entry (ACE; アクセスコントロール エントリ) の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかり、それ以降の検索処理は中止され、QoS 処理が開始されます。



(注)

アクセスリストを作成するときは、アクセスリストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義したあとで、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。設定手順については、「[QoS ポリシーの設定](#)」(P.36-43) を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセスグループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合したあとで、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適切な場合の対処法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合しなければなりません。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

ポリシー マップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

非階層型ポリシー マップは、物理ポートまたは SVI の着信トラフィックに適用できます。ただし、階層型のポリシー マップに関しては、SVI に対してのみしか適用できません。階層型のポリシー マップには 2 つのレベルがあります。1 番めは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 番めはインターフェイス レベルで、SVI の物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイス レベルのアクションはインターフェイス レベルのポリシー マップで指定されます。

詳細については、「[ポリシングおよびマーキング](#)」(P.36-8) を参照してください。設定手順については、「[QoS ポリシーの設定](#)」(P.36-43) を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てたあとで、ポリシングおよびマーキング プロセスを開始できます (図 36-4 を参照)。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットを廃棄するアクション、またはパケットに割り当てられた DSCP 値を変更 (マークダウン) してパケットの通過を許可するアクションなどがあります。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。ポリシング済み DSCP マップの詳細については、「[マッピング テーブル](#)」(P.36-12) を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。



(注)

すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます (ポリサーが設定されている場合)。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときに廃棄されたり、DSCP または CoS フィールドが変更されたりすることがあります。

物理ポートまたは SVI に対してポリシングを設定できます。物理ポートに対しては、信頼状態を設定したり、パケットに新規に DSCP または IP precedence 値を設定したり、個別のポリサーまたは集約ポリサーを定義できます。物理ポートのポリシング設定の詳細については、「[物理ポートのポリシング](#)」(P.36-9) を参照してください。SVI にポリシー マップを設定する場合、階層型のポリシー マップを作成して、ポリシー マップの 2 番めのインターフェイス レベルにのみ個別にポリサーを定義します。詳細については、「[SVI のポリシング](#)」(P.36-10) を参照してください。

ポリシー マップおよびポリシング アクションを設定したあとで、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシーを統合します。設定情報については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-49)、「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-53)、および「[集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-60) を参照してください。



(注)

10 ギガビット イーサネット インターフェイスはポリシングをサポートしません。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

- **Individual** : QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- **Aggregate** : QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。ポリサーの帯域幅限度を指定するには、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用します。このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。



(注)

個別のポリサーのみを SVI で設定できます。

ポリシングは、トークン バケット アルゴリズムを使用します。各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート (ビット/秒) で送信されます。バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション (廃棄またはマークダウン) が実行されます。

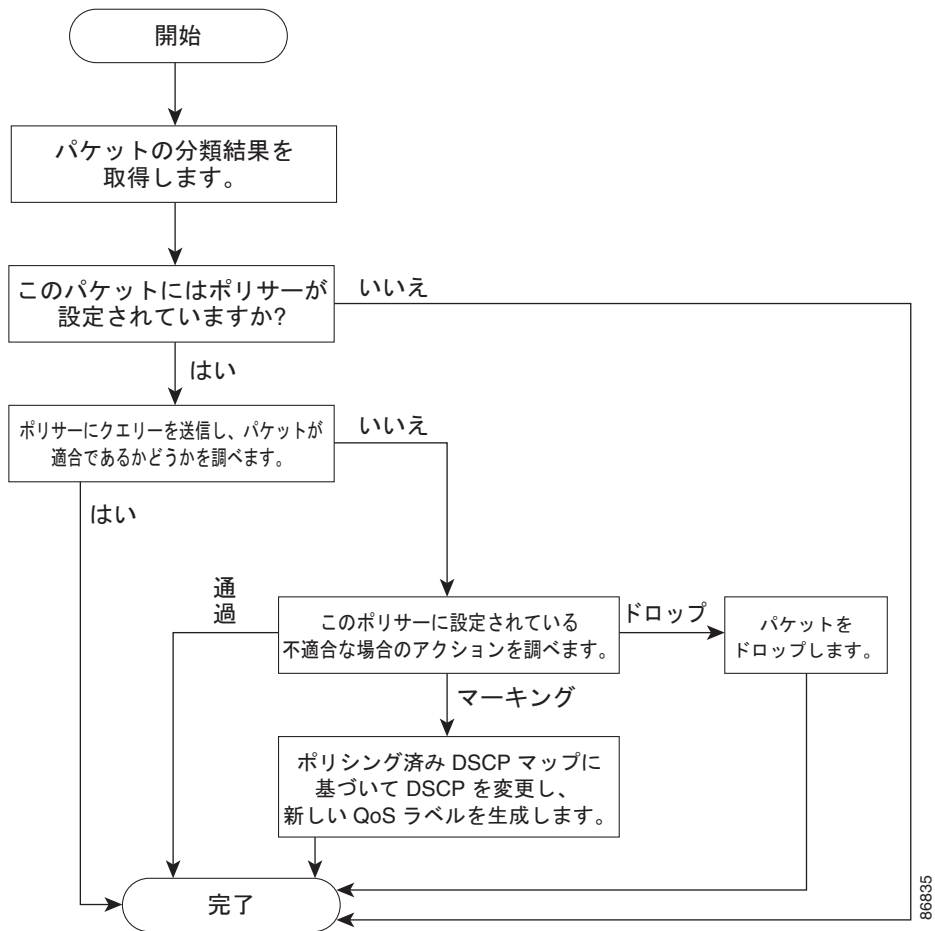
バケットが満たされる速度は、バケット深度 (**burst-byte**)、トークンが削除されるレート (**rate-bps**)、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシングアクションが実行されます。

バケット深度 (バケットがオーバーフローするまでに許容される最大バースト) を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドの **burst-byte** オプションを使用します。トークンがバケットから削除されるレート (平均レート) を設定するには、**police** ポリシーマップ クラス コンフィギュレーション コマンドまたは **mls qos aggregate-policer** グローバル コンフィギュレーション コマンドの **rate-bps** オプションを使用します。

[図 36-4](#) に、ポリシングおよびマーキングのプロセスを示します。次のタイプのポリシー マップが設定されます。

- 物理ポートの非階層型ポリシー マップ。
- SVI に適用されたインターフェイス レベルの階層型ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップに指定します。

図 36-4 物理ポートのポリシングおよびマーキング フローチャート



SVI のポリシング



(注)

SVI に個別のポリサーで階層型のポリシー マップを設定する前に、SVI の物理ポートに対して VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップが SVI に適用されますが、個々のポリサーは、階層型のポリシー マップの 2 番目のインターフェイス レベルで指定した物理ポートのトラフィックに対してのみ影響します。

階層型のポリシー マップには 2 つのレベルがあります。1 番めは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 番めはインターフェイス レベルで、SVI の物理ポートのトラフィックに対して実行するアクションを指定します (インターフェイス レベルのポリシー マップで指定されます)。

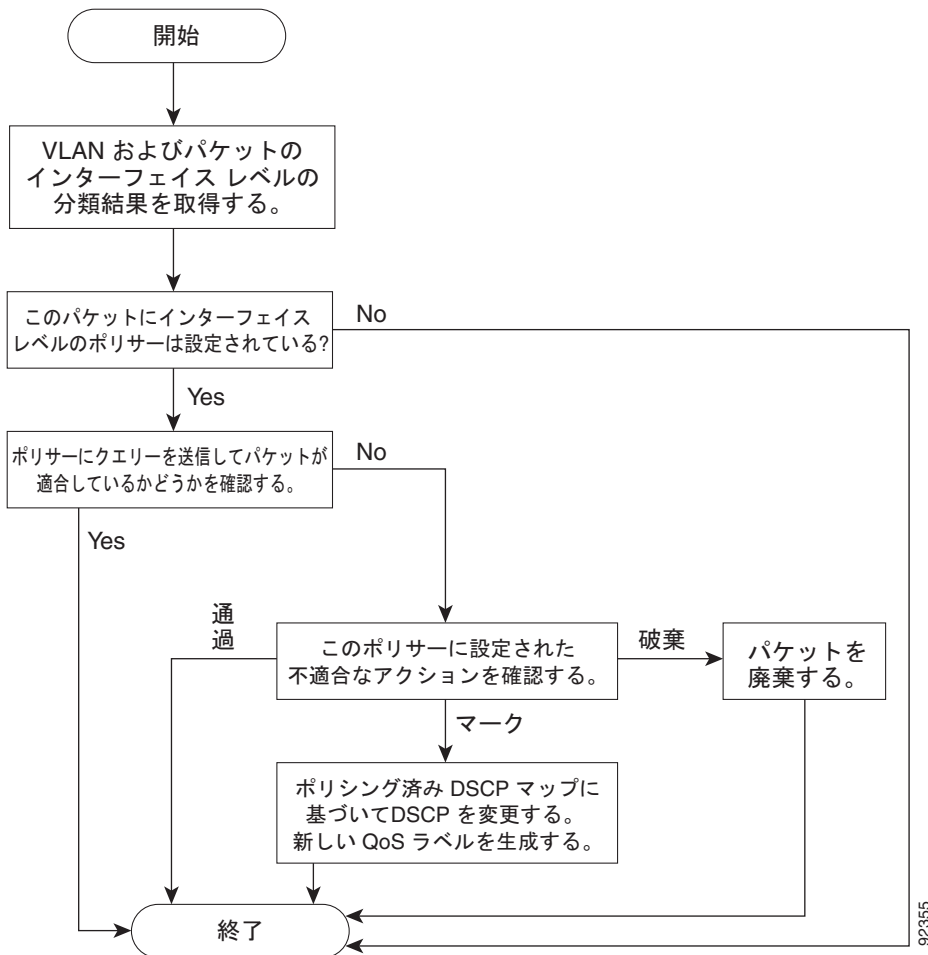
SVI にポリシーを設定する場合、次の 2 つのレベルの階層型ポリシー マップを作成および設定できます。

- VLAN レベル：クラス マップおよびポートの信頼状態を指定するクラスを設定することで、またはパケットに新規に DSCP や IP precedence 値を設定することでプライマリ レベルを作成します。VLAN レベルのポリシー マップは SVI の VLAN に対してのみ適用可能で、ポリサーはサポートしません。
- インターフェイス レベル：クラス マップおよび SVI の物理ポートに個別にポリサーを指定するクラスを設定することで、セカンダリ レベルを作成します。インターフェイス レベルのポリシー マップは個別のポリサーのみサポートし、集約ポリサーをサポートしません。VLAN レベルのポリシー マップで定義されたクラスごとに、異なるインターフェイス レベル ポリシー マップを設定できます。

階層型のポリシー マップの例は、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシー、およびマーキング」(P.36-53) を参照してください。

図 36-5 に、SVI に階層型のポリシー マップが設定されている場合のポリシーおよびマーキングのプロセスを示します。

図 36-5 SVI のポリシーおよびマーキング フローチャート



92355

マッピング テーブル

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用してキューを選択します。また、QoS ラベルによって入力/出力キューだけでなく、WTD しきい値も特定されます。これらのマップを設定するには、**mls qos srr-queue {input | output} dscp-map** および **mls qos srr-queue {input | output} cos-map** グローバル コンフィギュレーション コマンドを使用します。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。

DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。その他のすべてのマップはスイッチ全体に適用されます。

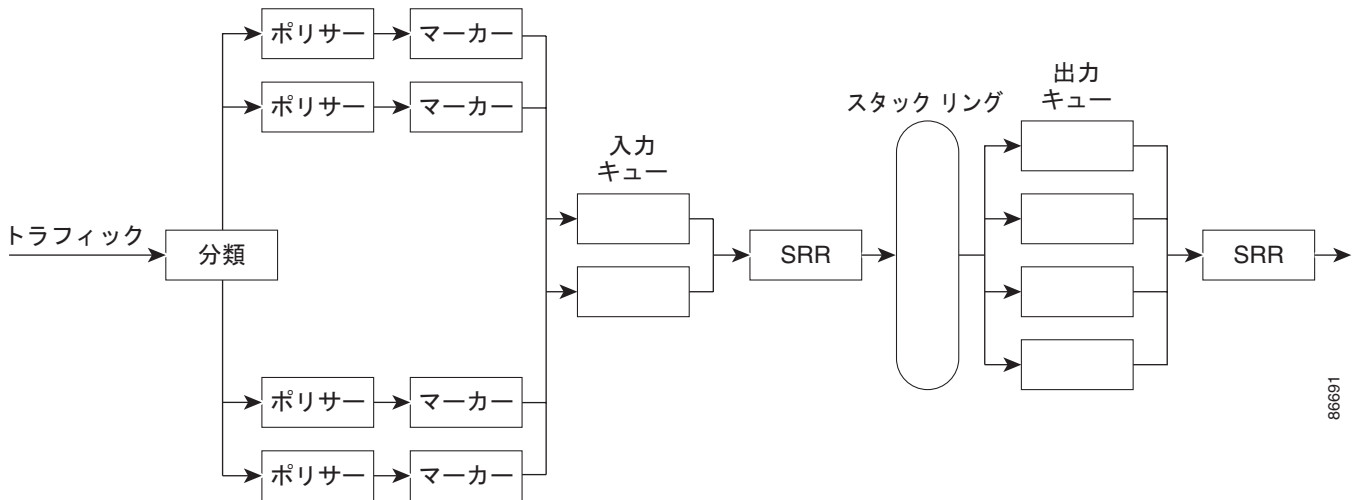
設定手順については、「[DSCP マップの設定](#)」(P.36-62) を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「[入力キューでのキューイングおよびスケジューリング](#)」(P.36-15) を参照してください。DSCP および CoS 出力キューしきい値マップの詳細については、「[出力キューでのキューイングおよびスケジューリング](#)」(P.36-17) を参照してください。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立ってます（図 36-6 を参照）。

図 36-6 入力および出力キューの位置



すべてのポートの入力帯域幅の合計がスタック リングの帯域幅を超えることがあるため、入力キューはパケットの分類、ポリシング、およびマーキングのあと、パケットがスイッチ ファブリックに転送される前の位置に配置されています。複数の入力ポートから 1 つの出力ポートに同時にパケットが送信されて、輻輳が発生することがあるため、出力キューはスタック リングのあとに配置されています。

WTD

入力および出力キューは両方とも、WTD と呼ばれるテール ドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとに廃棄優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームは廃棄されます。

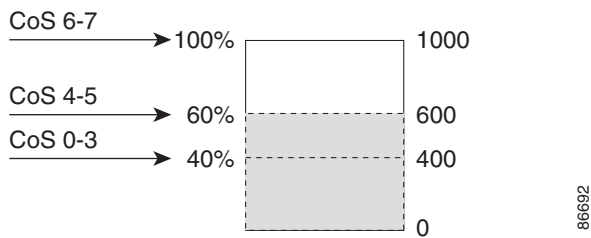
各キューには 3 つのしきい値があります。QoS ラベルは 3 つのしきい値のどれがフレームの対象となるかを決定します。3 つのしきい値のうち 2 つが設定可能（明示的）であり 1 つが設定可能ではありません（暗黙的）。

図 36-7 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます（キューフル ステート）。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0～3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

図 36-7 WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.36-68)、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」(P.36-73)、および「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.36-75) を参照してください。

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットがスタック リングに送信されます。出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有がデフォルト モードであり、これ以外のモードはサポートされていません。

シェーピング モードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。シェーピングされたトラフィックの場合は、リンクがアイドルの場合も、割り当てを超える帯域幅は使用されません。シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バースト トラフィックの最高時と最低時を削減します。シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

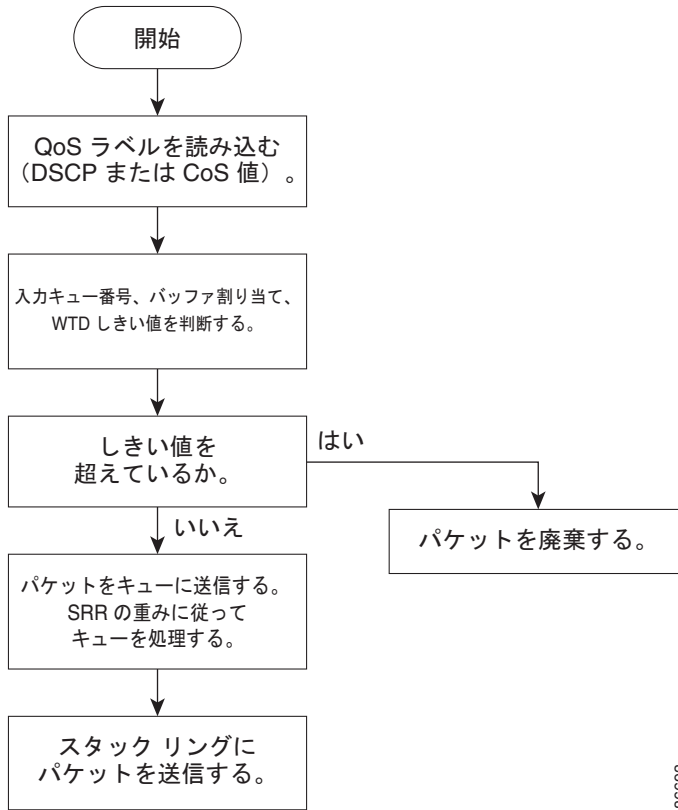
共有モードでは、各キューは設定された重みに従って帯域幅を共有します。帯域幅に対してはこのレベルが保証されますが、このレベルに限定されるわけではありません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。シェーピングおよび共有はインターフェイス単位で設定されます。各インターフェイスを一意に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」(P.36-70)、「出力キューでの SRR シェーピング 重みの設定」(P.36-76)、および「出力キューでの SRR 共有重みの設定」(P.36-78) を参照してください。

入力キューでのキューイングおよびスケジューリング

図 36-8 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

図 36-8 入力ポートのキューイングおよびスケジューリング フローチャート



(注) 共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってのみ処理される、設定可能な入力キューを 2 つサポートしています。表 36-1 にこれらのキューの説明を示します。

表 36-1 入力キューのタイプ

キュー タイプ ¹	機能
標準	標準プライオリティと見なされるユーザ トラフィック。各フローを区別するために、3 つの異なるしきい値を設定できます。 mls qos srr-queue input threshold 、 mls qos srr-queue input dscp-map 、および mls qos srr-queue input cos-map グローバル コンフィギュレーション コマンドを使用できます。
緊急	Differentiated Services (DF) 緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラフィック。このトラフィックに必要な帯域幅は、 mls qos srr-queue input priority-queue グローバル コンフィギュレーション コマンドを使用して、合計スタック トラフィックの割合として設定できます。緊急キューには帯域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークおよびスタックを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}** または **mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}** グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能 (明示的) な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能 (暗示的) なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合 (しきい値 ID 1 および ID 2 用) を割り当てるには、**mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2** グローバル コンフィギュレーション コマンドを使用します。各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。WTD の仕組みの詳細については、「[WTD](#)」(P.36-13) を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する (スペース量を割り当てる) には、**mls qos srr-queue input buffers percentage1 percentage2** グローバル コンフィギュレーション コマンドを使用します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットが廃棄される前にバッファに格納して送信できるデータ量が制御されます。1 帯域幅を割合として割り当てるには、**mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドを使用します。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、**mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューはスタック リングの負荷に関わらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック (音声など) に使用する必要があります。

SRR は **mls qos srr-queue input priority-queue queue-id bandwidth weight** グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は **mls qos srr-queue input bandwidth weight1 weight2** グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットが廃棄されるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定手順については、「[入力キューの特性の設定](#)」(P.36-68) を参照してください。

出力キューでのキューイングおよびスケジューリング

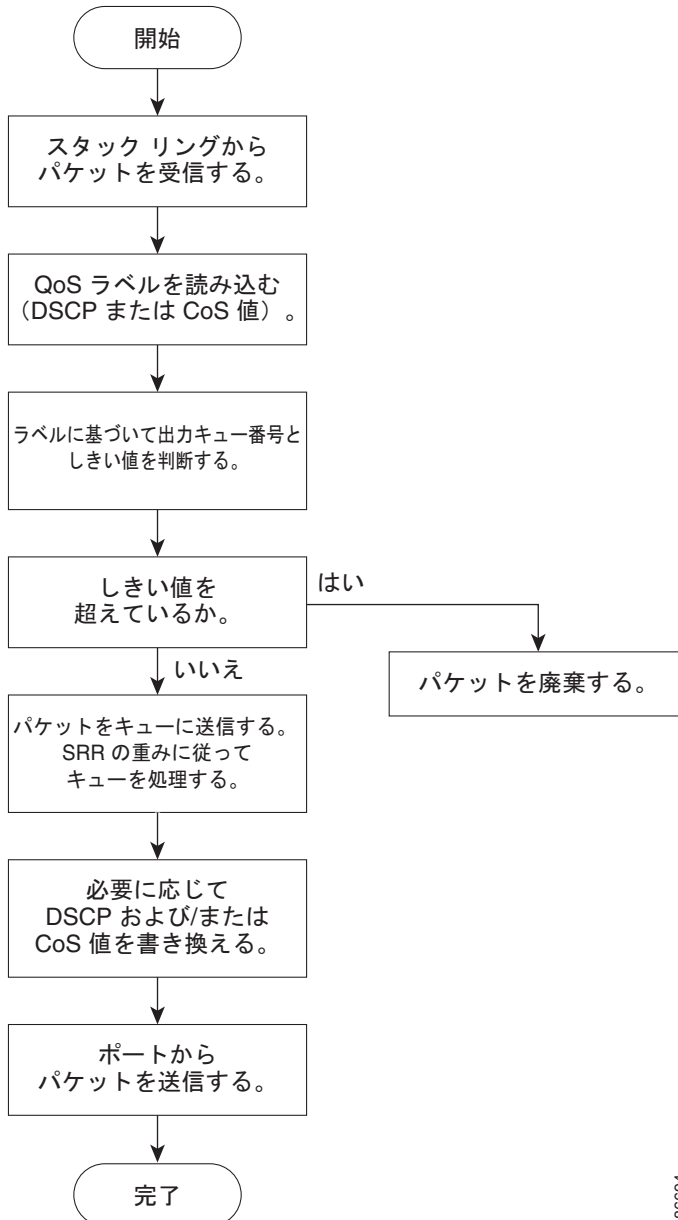
図 36-9 に、出力ポートのキューイングおよびスケジューリング フローチャートを示します。



(注)

緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の 3 つのキューが処理されます。

図 36-9 出力ポートのキューイングおよびスケジューリング フローチャート

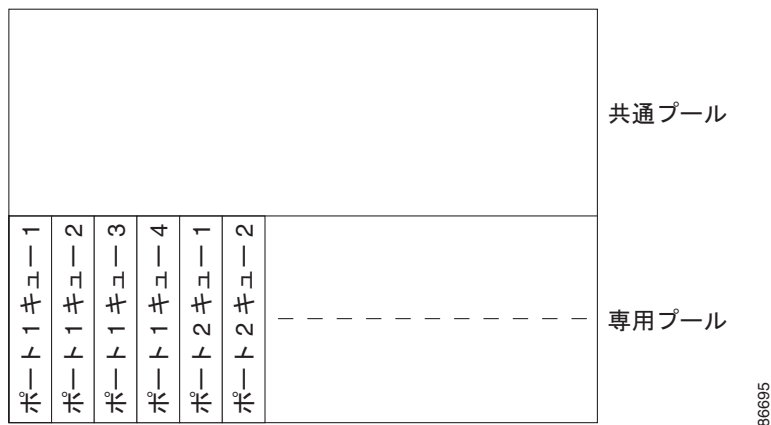


86694

各ポートは、4 つの出力キューをサポートし、そのうち 1 つ（キュー 1）を出力緊急キューにできます。これらのキューはキューセットで設定します。出力ポートから送出されるすべてのトラフィックは、これらの 4 つのキューのいずれかを通過し、パケットに割り当てられた QoS ラベルに基づいてしきい値に影響されます。

図 36-10 に出力キュー バッファを示します。バッファ スペースは共通プールと専用プールからなります。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかを制御されます。スイッチは、目的のキューが確保された量（限度内）を超えるバッファを消費していないかどうか、最大バッファ（限度超）をすべて消費しているかどうか、および共通プールが空である（空きバッファなし）か、または空でない（空きバッファあり）かを検出します。キューが限度を超えていない場合、スイッチは専用プールまたは共通プール（空でない場合）からバッファ スペースを割り当てます。共通プールに空きバッファがない場合、またはキューが限度を超えている場合は、フレームが廃棄されます。

図 36-10 出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。各しきい値はキューに割り当てられたメモリの割合です。パーセンテージを指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティ トラフィックを確実にバッファに格納できます。たとえば、バッファ スペースが 400 の場合、バッファ スペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ~ 4 に割り当てることができます。キュー 1 には 280 のバッファが割り当てられ、キュー 2 ~ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。たとえば、キュー用として 100 バッファがある場合、50% (50 バッファ) を確保できます。残りの 50 バッファは共通プールに戻されます。また、最大しきい値を設定することにより、一杯になったキューが確保量を超えるバッファを取得できるようにすることもできます。共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 `mpls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}` または `mpls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}` グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、`show mpls qos maps` 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能 (明示的) な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能 (暗示的) なしきい値です。しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。キューセットにポートをマッピングするには、`queue-set qset-id` インターフェイス コンフィギュレーション コマンドを使用します。キューセットの設定を変更して WTD しきい値の割合を変更します。WTD の仕組みの詳細については、「WTD」(P.36-13) を参照してください。

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。ポートに共有重みまたはシェーピング重みを割り当てするには、`srr-queue bandwidth share weight1 weight2 weight3 weight4` または `srr-queue bandwidth shape weight1 weight2 weight3 weight4` インターフェイス コンフィギュレーション コマンドを使用します。シェーピングと共有の違いについては、「SRR のシェーピングおよび共有」(P.36-14) を参照してください。



(注)

10 ギガビット インターフェイスにシェーピング重みを割り当てられません。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットが廃棄される前にバッファに格納して送信できるデータ量が制御されます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルでないかぎり、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域幅重みは無視されて比率計算に使用されません。緊急キューはプライオリティ キューであり、処理されて空になってから、他のキューが処理されます。緊急キューをイネーブルにするには、`priority-queue out` インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットが廃棄されるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定手順については、「出力キューの特性の設定」(P.36-72) を参照してください。



(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、次のようにパケットが変更されることがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、このあとの段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されずに、DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されずに、CoS/DSCP マップに従って DSCP が変更されることがあります。

入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。ポリサーマップの設定アクションによっても、DSCP が書き換えられます。

自動 QoS の設定

自動 QoS 機能を使用して、既存の QoS 機能の配置を容易にできます。自動 QoS では、ネットワーク設計について前提条件を設定し、その結果スイッチは、デフォルトの QoS 動作を使用せずに、各トラフィック フローについて優先度を指定して入力および出力キューを適切に使用できるようになります（デフォルトで自動 QoS はディセーブルになっています。したがって、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します）。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

自動 QoS コマンドを使用して Cisco IP Phone、および Cisco SoftPhone アプリケーションを実行するデバイスに接続するポートを指定します。また、アップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。自動 QoS は以下の機能を実行します。

- Cisco IP Phone の有無の検出
- QoS 分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- 「生成される自動 QoS 設定」 (P.36-21)
- 「コンフィギュレーションにおける自動 QoS の影響」 (P.36-26)
- 「自動 QoS 設定時の注意事項」 (P.36-26)
- 「Cisco IOS Release 12.2(20)SE 以前のリリースからのアップグレード」 (P.36-27)
- 「VoIP 用自動 QoS のイネーブル化」 (P.36-27)

- 「自動 QoS 設定例」 (P.36-29)

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。

自動 QoS がイネーブルの場合、入力パケット ラベルを使用してトラフィックを分類し、パケット ラベルを割り当て、入力および出力キューを設定します (表 36-2 を参照)。

表 36-2 トラフィック タイプ、パケット ラベル、キュー

	VoIP ¹ データ トラフィック	VoIP 制御 トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他のトラフィック	
DSCP	46	24, 26	48	56	34	-	
CoS	5	3	6	7	4	-	
CoS/入力キュー マップ	2, 3, 4, 5, 6, 7 (キュー 2)					0, 1 (キュー 1)	
CoS/出力キュー マップ	5 (キュー 1)	3, 6, 7 (キュー 2)			4 (キュー 3)	2 (キュー 3)	0, 1 (キュー 4)

1. VoIP = Voice over IP

表 36-3 に、入力キューに対して生成される自動 QoS 設定を示します。

表 36-3 入力キューの自動 QoS 設定

入力キュー	キュー番号	CoS/キュー マップ	キュー重み (帯域幅)	キュー (バッファ) サイズ
SRR 共有	1	0, 1	81%	67%
プライオリティ	2	2, 3, 4, 5, 6, 7	19%	33%

表 36-4 に、出力キューに対して生成される自動 QoS 設定を示します。

表 36-4 出力キューの自動 QoS 設定

出力キュー	キュー番号	CoS/キュー マップ	キュー重み (帯域幅)	ギガビット対応 ポートのキュー (バッファ) サイズ	10/100 イーサ ネット ポートの キュー (バッファ) サイズ
プライオリティ	1	5	最大 100%	16%	10%
SRR 共有	2	3, 6, 7	10%	6%	10%
SRR 共有	3	2, 4	60%	17%	26%
SRR 共有	4	0, 1	20%	61%	54%

自動 QoS 機能を最初のポートでイネーブルにすると、以下の動作が自動的に発生します。

- QoS は、グローバルにイネーブル (**mls qos** グローバル コンフィギュレーション コマンド) になり、他のグローバル コンフィギュレーション コマンドが追加されます。
- **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを Cisco IP Phone が接続されたネットワーク エッジにあるポートに入力すると、スイッチは信頼境界機能をイネーブルにします。スイッチは、Cisco Discovery Protocol (CDP) を使用して Cisco IP Phone の有無を検出します。Cisco IP Phone が検出されたら、ポートの入力分類がパケットで受信される QoS ラベルを信頼するように設定されます。またスイッチは、ポリシングを使用して、パケットがインプロファイルかアウト オブ プロファイルかを判別し、パケットに対するアクションを指定します。パケットが DSCP 値 (24、26、または 46) を持っていない、あるいはアウト オブ プロファイルである場合は、スイッチが DSCP 値を 0 に変更します。Cisco IP Phone が不在の場合、入力分類はパケットの QoS ラベルを信頼しないように設定されます。スイッチは、表 36-3 および表 36-4 の設定に従ってポート上の入力および出力キューを設定します。スイッチで信頼境界機能がイネーブルになる前に、ポリシングがポリシー マップ分類と一致するトラフィックに適用されます。
- **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼動するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッチはポリシングを使用して、パケットがプロファイルの内部または外部にいるかを判断し、パケット上のアクションを指定します。パケットが DSCP 値 (24、26、または 46) を持っていない、あるいはアウト オブ プロファイルである場合は、スイッチが DSCP 値を 0 に変更します。スイッチは、表 36-3 および表 36-4 の設定に従ってポート上の入力および出力キューを設定します。
- ネットワーク内部に接続されたポート上で **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値、ルーテッド ポートの場合は入力パケット内の DSCP 値が信頼されます (前提条件は、トラフィックがすでに他のエッジデバイスによって分類されていることです)。スイッチは、表 36-3 および表 36-4 の設定に従ってポート上の入力および出力キューを設定します。

信頼境界機能の詳細については、「[ポート セキュリティを確保するための信頼境界機能の設定 \(P.36-39\)](#)」を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone**、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにする場合、スイッチはトラフィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、表 36-5 にリストされているコマンドをポートに適用します。

表 36-5 生成される自動 QoS 設定

説明	自動的に生成されるコマンド
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ (着信パケットの CoS 値の DSCP 値へのマッピング) を設定します。	<pre>Switch(config)# mls qos Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56</pre>
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue input cos-map Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 3 0 Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 1 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 1 2 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5</pre>

表 36-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue output cos-map Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 Switch(config)# mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7 Switch(config)# mls qos srr-queue output cos-map queue 3 threshold 3 2 4 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 3 0</pre>
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue input dscp-map Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 32 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47</pre>
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue output dscp-map Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7</pre>

表 36-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
スイッチが自動的に入力キューを設定します。キュー 2 がプライオリティ キューでキュー 1 が共有モードです。また、スイッチは、入力キューの帯域幅とバッファ サイズも設定しません。	<pre>Switch(config)# no mls qos srr-queue input priority-queue 1 Switch(config)# no mls qos srr-queue input priority-queue 2 Switch(config)# mls qos srr-queue input bandwidth 90 10 Switch(config)# mls qos srr-queue input threshold 1 8 16 Switch(config)# mls qos srr-queue input threshold 2 34 66 Switch(config)# mls qos srr-queue input buffers 67 33</pre>
スイッチが自動的に出力キューのバッファ サイズを設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード (シェーピングまたは共有) を設定します。	<pre>Switch(config)# mls qos queue-set output 1 threshold 1 138 138 92 138 Switch(config)# mls qos queue-set output 1 threshold 2 138 138 92 400 Switch(config)# mls qos queue-set output 1 threshold 3 36 77 100 318 Switch(config)# mls qos queue-set output 1 threshold 4 20 50 67 400 Switch(config)# mls qos queue-set output 2 threshold 1 149 149 100 149 Switch(config)# mls qos queue-set output 2 threshold 2 118 118 100 235 Switch(config)# mls qos queue-set output 2 threshold 3 41 68 100 272 Switch(config)# mls qos queue-set output 2 threshold 4 42 72 100 242 Switch(config)# mls qos queue-set output 1 buffers 10 10 26 54 Switch(config)# mls qos queue-set output 2 buffers 16 6 17 61 Switch(config-if)# priority-que out Switch(config-if)# srr-queue bandwidth share 10 10 60 20</pre>
auto qos voip trust コマンドを入力した場合、 mls qos trust cos コマンドを使用することによって、スイッチは非ルーテッドポートで受信したパケットの CoS 値を信頼するように、または mls qos trust dscp コマンドを使用することによって、ルーテッドポートで受信したパケットの DSCP 値を信頼するように、自動的に入力分類を設定します。	<pre>Switch(config-if)# mls qos trust cos Switch(config-if)# mls qos trust dscp</pre>
auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。	<pre>Switch(config-if)# mls qos trust device cisco-phone</pre>

表 36-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
<p>auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。</p>	<pre>Switch(config)# mls qos map policed-dscp 24 26 46 to 0 Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap)# match ip dscp ef Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap)# match ip dscp cs3 af31 Switch(config)# policy-map AutoQoS-Police-SoftPhone Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c)# set dscp ef Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust Switch(config-pmap-c)# set dscp cs3 Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit</pre>
<p>クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ (別名 <i>AutoQoS-Police-SoftPhone</i>) を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。</p>	<pre>Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone</pre>
<p>auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。</p>	<pre>Switch(config)# mls qos map policed-dscp 24 26 46 to 0 Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap)# match ip dscp ef Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap)# match ip dscp cs3 af31 Switch(config)# policy-map AutoQoS-Police-CiscoPhone Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c)# set dscp ef Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust Switch(config-pmap-c)# set dscp cs3 Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit</pre>
<p>クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ (別名 <i>AutoQoS-Police-CiscoPhone</i>) を、Cisco Phone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。</p>	<pre>Switch(config-if)# service-policy input AutoQoS-Police-CiscoPhone</pre>

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになると、**auto qos voip** インターフェイス コンフィギュレーション コマンド および生成された設定が実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設定により、生成コマンドのアプリケーションに障害が発生したり、生成コマンドによってユーザ設定が上書きされたりする可能性があります。これらの動作は警告なしに発生します。すべての生成コマンドが正常に適用された場合、上書きされていないユーザ入力設定が実行コンフィギュレーションに残ります。上書きされたユーザ入力設定は、現在の設定をメモリに保存することなく、スイッチをリロードすることで取得できます。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- 自動 QoS は非ルーテッドおよびルーテッド ポート上の Cisco IP Phone の VoIP 用にスイッチを設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼動するデバイスの VoIP 用にスイッチを設定します。



(注) Cisco IOS Release 12.2(20)SE より前のリリースでは、自動 QoS は Cisco IP Phone を搭載したスイッチ ポート上でのみ VoIP を設定します。

- Cisco SoftPhone を稼動するデバイスが非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つのみをサポートします。
- Cisco IOS Release 12.2(40)SE、Auto-Qos VoIP では出力インターフェイスに対して **priority-queue** インターフェイス コンフィギュレーション コマンドが使用されます。ポリシー マップおよび信頼できるデバイスを Cisco IP Phone の同一インターフェイス上に設定することも可能です。
- スイッチ ポートが **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを使用して設定されていた場合 (Cisco IOS Release 12.2(37)SE 以前)、Cisco IOS Release 12.2(40)SE で新規導入された自動 QoS 生成コマンドがポートに適用されません。このコマンドを自動的に適用するには、ポートの設定を一度削除してから再びポートに適用する必要があります。
- 10 ギガビット インターフェイスは、Cisco IP Phone を使用した VoIP、または Cisco SoftPhone 機能を稼動するデバイスを使用した VoIP では、自動 QoS 機能をサポートしません。
- 自動 QoS のデフォルト設定を利用する場合、他の QoS コマンドを実行する前に自動 QoS をイネーブルにする必要があります。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了したあとにのみ調整することを推奨します。詳細については、「[コンフィギュレーションにおける自動 QoS の影響](#)」(P.36-26) を参照してください。
- 自動 QoS をイネーブルにしたら、名前に *AutoQoS* が含まれているポリシー マップまたは集約ポリサーを変更しないでください。ポリシー マップまたは集約ポリサーを変更する必要がある場合、これらをコピーしてから、コピーしたポリシー マップまたは集約ポリサーを変更してください。生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。

- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。
- ルーテッドポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- 接続したデバイスは、Cisco Call Manager バージョン 4 以降を使用する必要があります。

Cisco IOS Release 12.2(20)SE 以前のリリースからのアップグレード

Cisco IOS Release 12.2(20)SE では、旧リリースから自動 QoS の実装が変更されています。生成した自動 QoS 設定が変更され、Cisco SoftPhone 機能のサポートと、ルーテッドポートの Cisco IP Phone が追加されました。

自動 QoS がスイッチ上に設定され、スイッチが Cisco IOS Release 12.2(20)SE より前のリリースを稼動している状態で、Cisco IOS Release 12.2(20)SE 以降のリリースにアップグレードする場合、コンフィギュレーションファイルに新しい設定が含まれないため、自動 QoS は動作しません。コンフィギュレーションファイルで自動 QoS 設定をアップグレードするには、次の手順を実行します。

1. スイッチを Cisco IOS Release 12.2(20)SE 以降のリリースにアップグレードします。
2. 自動 QoS がイネーブルであるポートすべてに対して、自動 QoS をディセーブルにします。
3. **no** コマンドを使用して、グローバル自動 QoS 設定すべてをデフォルト値に戻します。
4. ステップ 2 で自動 QoS をディセーブルにしたポートで、自動 QoS をイネーブルに戻します。その場合、前と同じ自動 QoS 設定でポートを設定します。

VoIP 用自動 QoS のイネーブル化

QoS ドメイン内で VoIP 用の自動 QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	Cisco IP Phone に接続されたポート、Cisco SoftPhone 機能を実行するデバイスに接続されたポート、またはネットワーク内部の信頼性のある他のスイッチやルータに接続されたアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3 <code>auto qos voip {cisco-phone cisco-softphone trust}</code>	自動 QoS をイネーブルにします。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cisco-phone : ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話が検出された場合にかぎり信頼されます。このキーワードは 10 ギガビット インターフェイス上ではサポートされません。 • cisco-softphone : ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。このキーワードは 10 ギガビット インターフェイス上ではサポートされません。 • trust : アップリンク ポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show auto qos interface interface-id</code>	設定を確認します。 このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示するには、 show running-config 特権 EXEC コマンドを使用します。

自動 QoS のイネーブルまたはディセーブル時に自動的に生成された QoS コマンドを表示するには、自動 QoS をイネーブルにする前に、`debug auto qos` 特権 EXEC コマンドを入力します。詳細については、このリリースに対応するコマンドリファレンスにある `debug autoqos` コマンドの項を参照してください。

ポートで自動 QoS をディセーブルにするには、`no auto qos voip` インターフェイス コンフィギュレーション コマンドを使用します。このポート用に自動 QoS が生成したインターフェイス コンフィギュレーション コマンドのみが削除されます。これが自動 QoS をイネーブルにしている最後のポートの場合に、`no auto qos voip` コマンドを入力すると、自動 QoS 生成グローバル コンフィギュレーション コマンドが残っていても、(グローバル コンフィギュレーションによって他のポートのトラフィックを中断しないように) 自動 QoS はディセーブルであると見なされます。

自動 QoS 生成グローバル コンフィギュレーション コマンドをディセーブルにするには、`no mls qos` グローバル コンフィギュレーション コマンドを使用します。QoS がディセーブルになると、パケット (パケットの CoS 値、DSCP 値、および IP precedence 値) は変更されないため、`trusted` (信頼性のある) ポート、または `untrusted` (信頼性のない) ポートの概念はありません。トラフィックはパススルー モードでスイッチングされます (書き換えられずにスイッチングされ、ポリシングを伴わないベストエフォート型として分類されます)。

次に、ポートに接続されたスイッチまたはルータが信頼性のあるデバイスである場合に、自動 QoS をイネーブルにして着信パケットで受信された QoS ラベルを信頼する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip trust
```


自動 QoS 設定例

ここでは、自動 QoS をネットワークに実装する方法について説明します (図 36-11 を参照)。QoS パフォーマンスを最適にするには、ネットワーク内部のデバイスすべてで自動 QoS をイネーブルにします。

図 36-11 ネットワークでの自動 QoS の設定例

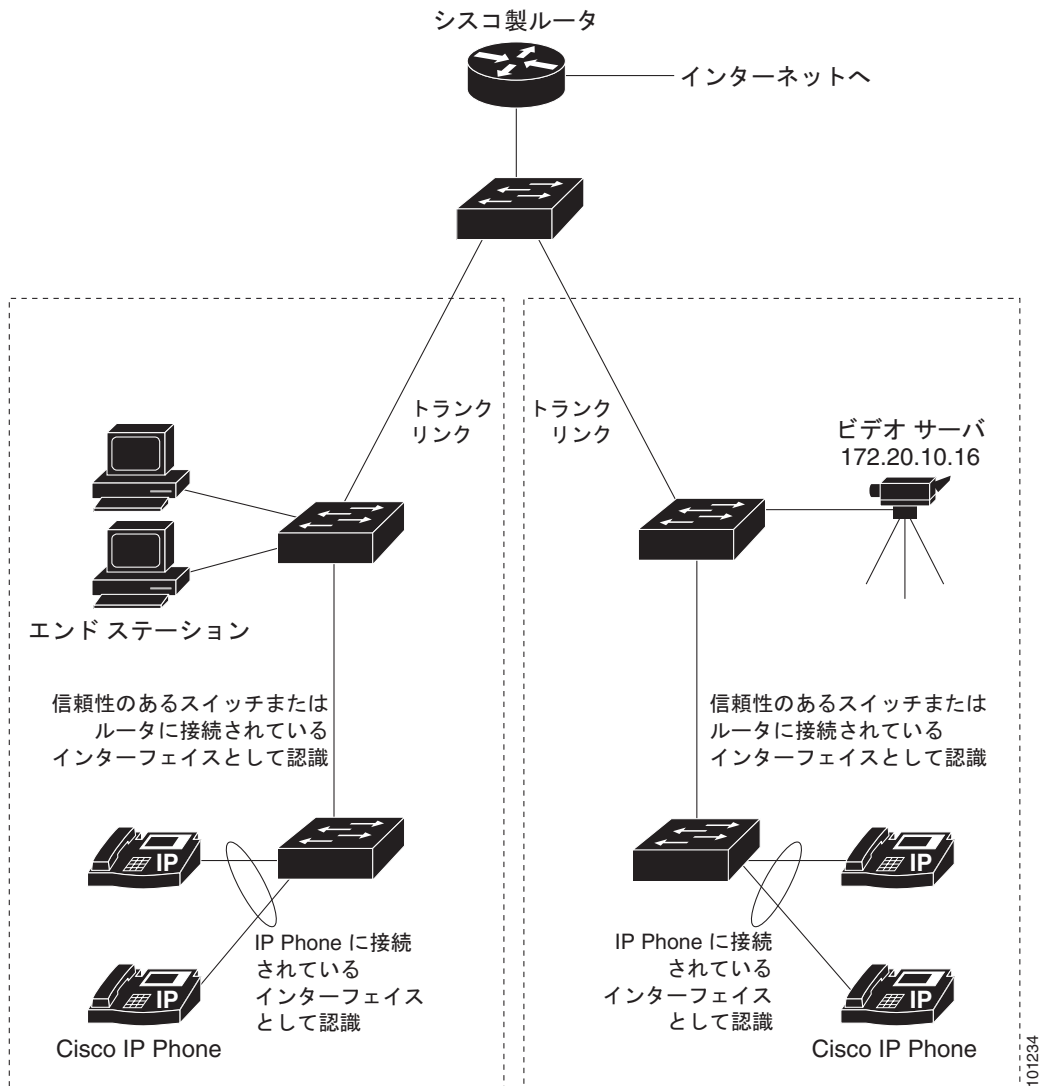


図 36-11 には、VoIP トラフィックを他のすべてのトラフィックより優先するネットワークを示しています。QoS ドメインの端にあるワイヤリングクローゼットのスイッチで、自動 QoS がイネーブルになっています。



(注)

自動 QoS コマンドを入力する前に標準 QoS コマンドを設定しないでください。QoS 設定を微調整できますが、自動 QoS が完了したあとにのみ調整することを推奨します。

QoS ドメインのエッジにあるスイッチで VoIP トラフィックを他のトラフィックより優先させるように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>debug auto qos</code>	自動 QoS のデバッグをイネーブルにします。デバッグをイネーブルにすると、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>cdp enable</code>	CDP をグローバルにイネーブルにします。デフォルトではイネーブルに設定されています。
ステップ 4	<code>interface interface-id</code>	Cisco IP Phone に接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>auto qos voip cisco-phone</code>	ポート上で自動 QoS をイネーブルにし、そのポートが Cisco IP Phone に接続されるように指定します。 着信パケットの QoS ラベルは、Cisco IP Phone が検出された場合のみ信頼されます。
ステップ 6	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 7		Cisco IP Phone に接続されているポートの数だけ、ステップ 4 ~ 6 を繰り返します。
ステップ 8	<code>interface interface-id</code>	信頼性のあるスイッチまたはルータに接続していると認識されるスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。図 36-11 を参照してください。
ステップ 9	<code>auto qos voip trust</code>	ポート上で自動 QoS をイネーブルにし、そのポートが信頼性のあるルータまたはスイッチに接続されるように指定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show auto qos</code>	設定を確認します。 このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示するには、 <code>show running-config</code> 特権 EXEC コマンドを使用します。 自動 QoS によって影響される QoS 設定の詳細については、「自動 QoS 情報の表示」(p.26-12) を参照してください。
ステップ 12	<code>copy running-config startup-config</code>	<code>auto qos voip</code> インターフェイス コンフィギュレーション コマンドおよび生成された自動 QoS 設定をコンフィギュレーション ファイル内に保存します。

自動 QoS 情報の表示

自動 QoS 設定を表示するには、`show auto qos [interface [interface-id]]` 特権 EXEC コマンドを使用します。ユーザによる設定変更を表示するには、`show running-config` 特権 EXEC コマンドを使用します。`show auto qos` コマンド出力と `show running-config` コマンド出力を比較してユーザ定義の QoS 設定を比較できます。

自動 QoS によって影響を受ける QoS 設定を表示するには、以下のいずれかのコマンドを使用します。

- `show mls qos`
- `show mls qos maps cos-dscp`
- `show mls qos interface [interface-id] [buffers | queueing]`

- `show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]`
- `show mls qos input-queue`
- `show running-config`

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

標準 QoS の設定

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

ここでは、次の設定情報について説明します。

- 「標準 QoS のデフォルト設定」(P.36-31)
- 「標準 QoS 設定時の注意事項」(P.36-34)
- 「QoS のグローバルにイネーブル化」(P.36-36) (必須)
- 「物理ポートで VLAN ベースの QoS をイネーブル化」(P.36-36) (任意)
- 「ポートの信頼状態による分類の設定」(P.36-37) (必須)
- 「QoS ポリシーの設定」(P.36-43) (必須)
- 「DSCP マップの設定」(P.36-62) (任意、DSCP/DSCP 変換マップまたはポリシング済み DSCP マップを使用する必要がない場合)
- 「入力キューの特性の設定」(P.36-68) (任意)
- 「出力キューの特性の設定」(P.36-72) (任意)

標準 QoS のデフォルト設定

QoS はディセーブルに設定されています。パケット（パケットの CoS 値、DSCP 値、および IP precedence 値）は変更されないため、**trusted**（信頼性のある）ポート、または **untrusted**（信頼性のない）ポートの概念はありません。トラフィックはパススルーモードでスイッチングされます（書き換えられずにスイッチングされ、ポリシングを伴わないベストエフォート型として分類されます）。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。ポリシー マップは設定されません。デフォルトでは、すべてのポートの信頼状態は **untrusted** です。入力および出力キューのデフォルト設定については、「入力キューのデフォルト設定」(P.36-32) および「出力キューのデフォルト設定」(P.36-32) を参照してください。

入力キューのデフォルト設定

表 36-6 に、QoS がイネーブルの場合の入力キューのデフォルト設定を示します。

表 36-6 入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て ¹	4	4
プライオリティ キューの帯域幅 ²	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみパケットを送信します。
2. キュー 2 はプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 36-7 に、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示します。

表 36-7 デフォルトの CoS 入力キューしきい値マップ

CoS 値	キュー ID-しきい値 ID
0-4	1-1
5	2-1
6, 7	1-1

表 36-8 に、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示します。

表 36-8 デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID-しきい値 ID
0-39	1-1
40-47	2-1
48-63	1-1

出力キューのデフォルト設定

表 36-9 に、QoS がイネーブルの場合における、各キューセットの出力キューのデフォルト設定を示します。すべてのポートはキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に設定され、レートは制限されません。

表 36-9 出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
専用しきい値	50%	50%	50%	50%

表 36-9 出力キューのデフォルト設定 (続き)

機能	キュー 1	キュー 2	キュー 3	キュー 4
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み (絶対) ¹	25	0	0	0
SRR 共有重み ²	25	25	25	25

1. シェーピング重みが 0 の場合、このキューはシェーピングモードで動作します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 36-10 に、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 36-10 デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID-しきい値 ID
0, 1	2-1
2, 3	3-1
4	4-1
5	1-1
6, 7	4-1

表 36-11 に、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 36-11 デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0-15	2-1
16-31	3-1
32-39	4-1
40-47	1-1
48-63	4-1

マッピング テーブルのデフォルト設定

デフォルトの CoS/DSCP マップは、表 36-12 (P.36-62) のとおりです。

デフォルトの IP precedence/DSCP マップは、表 36-13 (P.36-63) のとおりです。

デフォルトの DSCP/CoS マップは、表 36-14 (P.36-65) のとおりです。

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする (マークダウンしない) 空のマップです。

標準 QoS 設定時の注意事項

QoS の設定を始める前に、次の事項を確認してください。

- 「QoS ACL の注意事項」 (P.36-34)
- 「インターフェイスへの QoS の適用」 (P.36-34)
- 「ポリシングの注意事項」 (P.36-35)
- 「一般的な QoS の注意事項」 (P.36-35)

QoS ACL の注意事項

ACL で QoS を設定する際の注意事項は次のとおりです。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラス マップごとに使用できる ACL は 1 つだけ、使用できる **match** クラスマップ コンフィギュレーション コマンドは 1 つだけです。ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントには、ACL 行毎に複数の TCAM エントリが必要です。入力サービス ポリシー マップに ACL の信頼ステートメントが含まれている場合、利用可能な QoS TCAM に収めるにはアクセスリストが大きすぎる可能性があり、ポリシー マップをポートに適用する際にエラーが発生する場合があります。可能な限り、QoS ACL の行数を最小限に抑えてください。

インターフェイスへの QoS の適用

物理ポートで QoS を設定する際の注意事項は次のとおりです。ここでの注意事項は SVI (レイヤ 3 インターフェイス) にも当てはまります。

- QoS は物理ポートおよび SVI に設定できます。物理ポートに QoS を設定する場合は、非階層型のポリシー マップを作成し、適用してください。SVI に QoS を設定する場合は、非階層型および階層型のポリシー マップを作成し、適用できます。
- ブリッジング、ルーティング、または CPU への送信のどれを行うかに関係なく、着信トラフィックは分類、ポリシング、およびマークダウン (設定されている場合) されます。ブリッジングされたフレームを廃棄したり、DSCP および CoS 値を変更したりできます。
- 物理ポートまたは SVI でポリシー マップを設定する場合には、次の注意事項に従ってください。
 - 物理ポートと SVI に同じポリシー マップを適用できません。
 - 物理ポートで VLAN ベースの QoS を設定した場合、スイッチはそのポートにあるすべてのポートベースのポリシー マップを削除します。そうすることで、物理ポートのトラフィックは、自身のポートの SVI に適用されているポリシー マップの適用を受け入れられます。
 - SVI に適用された階層型のポリシー マップでは、物理ポートのインターフェイス レベルで個別にのみポリサーを作成でき、ポートのトラフィックの帯域幅制限を指定できます。入力ポートは、トランクまたは静的アクセス ポイントとして設定する必要があります。階層型のポリシー マップの VLAN レベルではポリサーを設定できません。
 - スイッチは、階層型のポリシー マップで集約ポリサーをサポートしません。

- SVI に階層型のポリシー マップが適用されたあとは、インターフェイス レベルのポリシー マップを変更したり、削除したりできません。新規にインターフェイス レベルのポリシー マップを階層型のポリシー マップに追加することもできません。変更するには、まず SVI から階層型ポリシー マップを削除する必要があります。また、階層型ポリシー マップで指定されたクラス マップを追加または削除できません。

ポリシングの注意事項

ポリシングの注意事項を次に示します。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 のポリサー（255 のユーザ設定可能ポリサーとシステムの内部使用のために予約された 1 つのポリサー）をサポートしています。各ポートでサポートされているポリサーの最大数は 63 です。たとえば、ギガビット イーサネット ポートに 32 のポリサー、ファスト イーサネット ポートに 8 つのポリサーを設定したり、ギガビット イーサネット ポートに 64 のポリサー、ファスト イーサネット ポートに 5 つのポリサーを設定できます。ポリサーは必要に応じてソフトウェアによって割り当てられ、ハードウェアおよび ASIC 境界の制約を受けます。ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。
- 10 ギガビット イーサネット上でポリシングを設定できません。
- 同じ非階層型のポリシー マップ内にある複数のトラフィック クラスで共有される集約ポリサーを作成できます。ただし、集約ポリサーを異なるポリシー マップにわたって使用することはできません。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランク ポートの場合、ポートを介して受信したすべての VLAN のトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- スイッチで受信された制御トラフィック（スパニング ツリー Bridge Protocol Data Unit（BPDU）；ブリッジ プロトコル データ ユニット）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。

IP サービス イメージを稼働させるスイッチは Policy-Based Routing（PBR；ポリシー ベース ルーティング）ルート マップでの QoS DSCP および IP precedence の一致をサポートしていて、次のような制限事項があります。

- QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用することができません。
- 透過的な DSCP と PBR DSCP ルート マップを同一スイッチに設定することはできません。

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。

QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos</code>	QoS をグローバルにイネーブルにします。 デフォルト設定における QoS の動作については、「標準 QoS のデフォルト設定」(P.36-31)、「入力キューでのキューイングおよびスケジューリング」(P.36-15)、および「出力キューでのキューイングおよびスケジューリング」(P.36-17)を参照してください。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

QoS をディセーブルにするには、`no mls qos` グローバル コンフィギュレーション コマンドを使用します。

物理ポートで VLAN ベースの QoS をイネーブル化

デフォルトでは、VLAN ベースの QoS はスイッチにあるすべての物理ポートでディセーブルです。スイッチは、物理ポート ベースでのみ、クラス マップおよびポリシー マップ QoS を含む QoS を適用できます。スイッチ ポートで VLAN ベースの QoS をイネーブルにできます。

VLAN ベースの QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順には、SVI にインターフェイス レベルの階層型ポリシー マップが指定されている物理ポートが必要です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>mls qos vlan-based</code>	ポートで VLAN ベースの QoS をイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface interface-id</code>	VLAN ベースの QoS が物理ポートでイネーブルかどうかを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

物理ポートで VLAN ベースの QoS をディセーブルにする場合は、`no mls qos vlan-based` インターフェイス コンフィギュレーション コマンドを使用します。

ポートの信頼状態による分類の設定

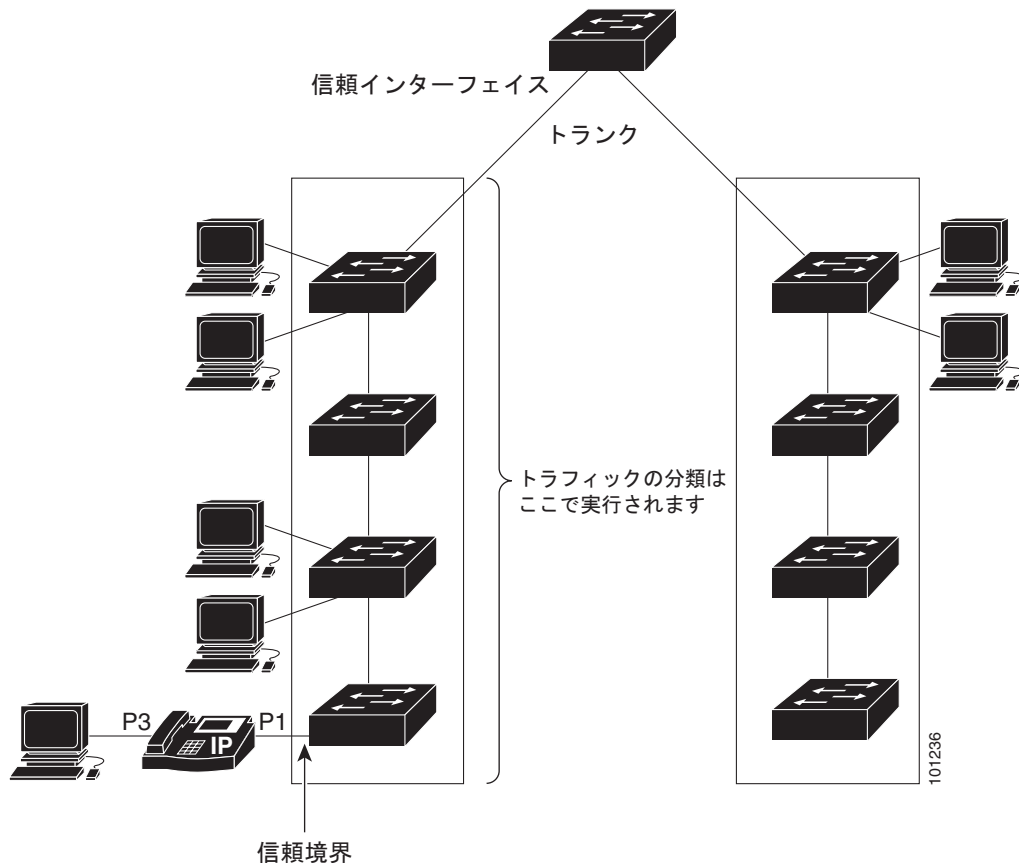
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」(P.36-43)に記載されている作業を1つまたは複数実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」(P.36-37)
- 「インターフェイスの CoS 値の設定」(P.36-39)
- 「ポートセキュリティを確保するための信頼境界機能の設定」(P.36-39)
- 「DSCP 透過モードのイネーブル化」(P.36-41)
- 「別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定」(P.36-41)

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチポートをいずれか1つの信頼状態に設定できます。図 36-12 に、ネットワークトポロジの例を示します。

図 36-12 QoS ドメイン内のポートの信頼状態



ポートが受信したトラフィックの分類を信頼するようにポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	<code>mls qos trust [cos dscp ip-precedence]</code>	ポートの信頼状態を設定します。 デフォルトでは、ポートは <code>trusted</code> ではありません。キーワードを指定しない場合、デフォルトは <code>dscp</code> です。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cos : パケットの CoS 値を使用して入力パケットを分類します。タグなしパケットの場合は、ポートのデフォルトの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。 • dscp : パケットの DSCP 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • ip-precedence : パケットの IP precedence 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`untrusted` ステートにポートを戻す場合は、`no mls qos trust` インターフェイス コンフィギュレーション コマンドを使用します。

デフォルトの CoS 値を変更する方法については、「[インターフェイスの CoS 値の設定](#)」(P.36-39) を参照してください。CoS/DSCP マップを設定する方法については、「[CoS/DSCP マップの設定](#)」(P.36-62) を参照してください。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

デフォルトのポート CoS 値を定義する場合、またはポート上のすべての着信パケットにデフォルトの CoS 値を割り当てる場合には、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	mls qos cos {default-cos override}	デフォルトのポート CoS 値を設定します。 <ul style="list-style-type: none"> <i>default-cos</i> には、ポートに割り当てるデフォルトの CoS 値を指定します。パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。CoS の範囲は 0 ~ 7 です。デフォルトは 0 です。 着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用する場合は、override キーワードを使用します。デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、 override キーワードを使用します。ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、**no mls qos cos {default-cos | override}** インターフェイス コンフィギュレーション コマンドを使用します。

ポート セキュリティを確保するための信頼境界機能の設定

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して (図 36-12 (P.36-37) を参照)、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ (CoS = 5) にマーキングし、データ パケットをロー プライオリティ (CoS = 0) にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 IEEE 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチへ送信されるトラフィックは、音声トラフィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされていることを保証するように信頼されています。**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイ プライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、(信頼性のある CoS 設定により) PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone (Cisco IP Phone 7910、7935、7940、および 7960) の存在を検出します。電話が検出されない場合、信頼境界機能がハイ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにします。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。**switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

信頼境界機能をポート上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 3	interface interface-id	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	cdp enable	ポート上で CDP をイネーブルに設定します。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	mls qos trust cos mls qos trust dscp	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	mls qos trust device cisco-phone	Cisco IP Phone が信頼性のあるデバイスであることを指定します。 信頼境界機能と自動 QoS (auto qos voip インターフェイス コンフィギュレーション コマンド) を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show mls qos interface	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

信頼境界機能をディセーブルにするには、**no mls qos trust device** インターフェイス コンフィギュレーション コマンドを使用します。

DSCP 透過モードのイネーブル化

このスイッチは透過的な DSCP 機能をサポートします。この機能は発信パケットの DSCP フィールドのみに作用します。透過的な DSCP 機能のデフォルト設定はディセーブルです。スイッチは着信パケットの DSCP フィールドを変更します。発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、および DSCP/DSCP 変換マップを含め、QoS 設定によって異なります。

no mls qos rewrite ip dscp コマンドを用いて透過的な DSCP 機能をイネーブルにした場合、スイッチは着信パケットの DSCP フィールドを変更しません。そのため、発信パケットの DSCP フィールドの内容はパケットの着信時と同じです。



(注) DSCP 透過をイネーブルにしても、IEEE 802.1Q トンネリング ポートのポート信頼設定は影響されません。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプライオリティを提示する CoS 値を生成します。また、スイッチは内部の DSCP 値を使用して、出力キューおよびしきい値も選択します。

透過的な DSCP 機能をスイッチでイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos	QoS をグローバルにイネーブルにします。
ステップ 3	no mls qos rewrite ip dscp	透過的な DSCP 機能をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

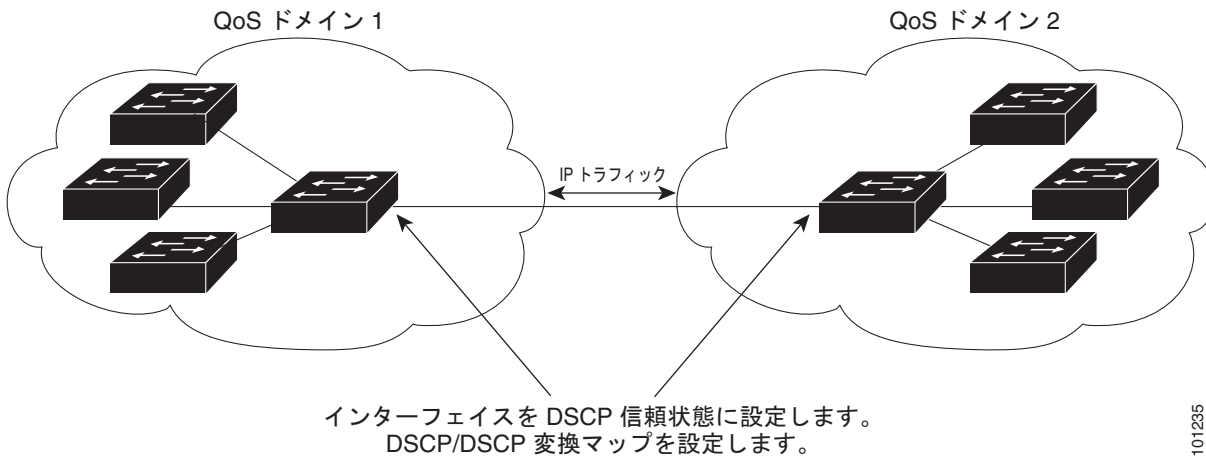
no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません (デフォルトの QoS 設定)。

no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust [cos | dscp]** インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます (図 36-13 を参照)。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 36-13 別の QoS ドメインとの境界ポートの DSCP 信頼状態



101295

ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 mls qos map dscp-mutation <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。 <ul style="list-style-type: none"> <i>dscp-mutation-name</i> には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 <i>in-dscp</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>out-dscp</i> には、DSCP 値を 1 つ入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3 interface interface-id	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4 mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5 mls qos dscp-mutation <i>dscp-mutation-name</i>	指定された DSCP trusted 入力ポートにマップを適用します。 <i>dscp-mutation-name</i> には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show mls qos maps dscp-mutation	設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートを `trusted` 以外のステータスに戻すには、`no mls qos trust` インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、`no mls qos map dscp-mutation dscp-mutation-name` グローバル コンフィギュレーション コマンドを使用します。

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ~ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ (`gi1/0/2-mutation`) を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gi1/0/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/0/2-mutation
Switch(config-if)# end
```

QoS ポリシーの設定

QoS ポリシーを設定するには、通常、トラフィックをクラス別に分類し、各トラフィック クラスに適用するポリシーを設定し、ポリシーをポートに結合する必要があります。

基本情報については、「[分類](#)」(P.36-5) および「[ポリシングおよびマーキング](#)」(P.36-8) を参照してください。設定時の注意事項については、「[標準 QoS 設定時の注意事項](#)」(P.36-34) を参照してください。

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。ネットワーク設定に応じて、次の作業を 1 つまたは複数実行する必要があります。

- 「[ACL によるトラフィックの分類](#)」(P.36-44)
- 「[クラス マップによるトラフィックの分類](#)」(P.36-47)
- 「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-49)
- 「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-53)
- 「[集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-60)

ACL によるトラフィックの分類

IP 標準 ACL または IP 拡張 ACL を使用することによって、IP トラフィックを分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用することによって分類できます。

IP トラフィック用に IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <code>access-list-number</code> には、アクセス リスト番号を入力します。有効範囲は 1 ~ 99 および 1300 ~ 1999 です。 • <code>permit</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。<code>deny</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • <code>source</code> には、パケットの送信元となるネットワークまたはホストを指定します。<code>any</code> キーワードは <code>0.0.0.0 255.255.255.255</code> の省略形として使用できます。 • (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show access-lists</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、`no access-list access-list-number` グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワーク アドレスのホスト部分にワイルドカードビットが適用されます。アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```


IP トラフィック用に IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard	<p>IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> access-list-number には、アクセス リスト番号を入力します。有効範囲は 100 ~ 199 および 2000 ~ 2699 です。 permit キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。deny キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 protocol には、IP プロトコルの名前または番号を入力します。疑問符 (?) を使用すると、使用できるプロトコル キーワードのリストが表示されます。 source には、パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、source 0.0.0.0 source-wildcard 255.255.255.255 の短縮形として any キーワードを使用したり、source 0.0.0.0 を表す host キーワードを使用します。 source-wildcard では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、source 0.00.0.0 source-wildcard 255.255.255.255 の短縮形として any キーワードを使用したり、source 0.0.0.0 を表す host キーワードを使用します。 destination には、パケットの宛先となるネットワークまたはホストを指定します。destination および destination-wildcard には、source および source-wildcard での説明と同じオプションを使用できます。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show access-lists	設定を確認します。
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no access-list access-list-number** グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック (precedence 値は 5) を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック (DSCP 値は 32) を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 mac access-list extended name	リスト名を指定し、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。
ステップ 3 {permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 <ul style="list-style-type: none"> <i>src-MAC-addr</i> には、パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 <i>mask</i> では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 <i>dst-MAC-addr</i> には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 (任意) <i>type mask</i> には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。<i>type</i> の範囲は 0 ~ 65535 です。通常は 16 進数で指定します。<i>mask</i> には、一致をテストする前に Ethertype に適用される 無視 (don't care) ビットを入力します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show access-lists [access-list-number access-list-name]	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no mac access-list extended access-list-name** グローバル コンフィギュレーション コマンドを入力します。

次に、2 つの許可 (permit) ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番目のステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、EtherType が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

クラス マップによるトラフィックの分類

個々のトラフィック フロー (またはクラス) を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。match ステートメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを 1 つ入力することによって定義します。



(注) **class** ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。詳細については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-49) および「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.36-53) を参照してください。

クラス マップを作成し、トラフィックを分類するための一致条件を定義するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 access-list access-list-number {deny permit} source [source-wildcard] または access-list access-list-number {deny permit} protocol source [source-wildcard] destination [destination-wildcard] または mac access-list extended name {permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「 ACL によるトラフィックの分類 」(P.36-44) を参照してください。 (注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

コマンド	目的
ステップ 3 <code>class-map [match-all match-any] class-map-name</code>	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • class-map-name には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定しない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 4 <code>match {access-group acl-index-or-name ip dscp dscp-list ip precedence ip-precedence-list}</code>	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> • access-group acl-index-or-name には、ステップ 2 で作成した ACL の番号または名前を指定します。 • ip dscp dscp-list には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 • ip precedence ip-precedence-list には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 5 <code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6 <code>show class-map</code>	<p>設定を確認します。</p>
ステップ 7 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

既存のポリシー マップを削除するには、**no policy-map policy-map-name** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class-map [match-all | match-any] class-map-name** グローバル コンフィギュレーション コマンドを使用します。一致条件を削除するには、**no match {access-group acl-index-or-name | ip dscp | ip precedence}** クラス マップ コンフィギュレーション コマンドを使用します。

次に、*class1* というクラス マップの設定例を示します。*class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。このクラス マップによって、任意のホストから任意の宛先へのトラフィック (DSCP 値は 10) が許可されます。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、*class2* という名前のクラスマップを作成する例を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラスマップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

作用対象となるトラフィック クラスを指定する非階層型ポリシー マップを、物理ポート上に設定できます。トラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラフィック クラスにトラフィック帯域幅限度を指定するアクション（ポリサー）や、トラフィックが不適合な場合の対処法を指定するアクション（マーキング）などを指定できます。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- ポリシー マップの信頼状態およびポートの信頼状態は互いに排他的であり、最後に設定された方が有効となります。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp dscp1...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにだけ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを使用すると、スイッチはスイッチ設定でこのコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用してパケット IP Precedence 値を変更できます。この設定は、スイッチ コンフィギュレーションで **set ip precedence** として表示されます。
- ポートに定義されたクラスごとに第 2 レベルのポリシー マップを別々に設定できます。第 2 レベルのポリシー マップは、各トラフィック クラスで実行するポリシング作業を指定します。階層型のポリシー マップの設定については、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング」(P.36-53) を参照してください。
- ポリシー マップとポート信頼状態の両方を物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。



(注) 10 ギガビット イーサネット インターフェイスは、ポリシー マップを使用したポリシングをサポートしません。

非階層型ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	class-map [match-all match-any] <i>class-map-name</i>	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定しない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 3	policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ 4	class <i>class-map-name</i>	<p>トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップ クラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 5 <code>trust [cos dscp ip-precedence]</code>	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。</p> <p>(注) このコマンドと set コマンドは、同じポリシー マップ内で相互に排他的になります。trust コマンドを入力する場合は、ステップ 6 へ進んでください。</p> <p>デフォルトでは、ポートは trusted ではありません。このコマンドを入力するときにキーワードを指定しない場合、デフォルトは dscp になります。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • cos : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • dscp : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • ip-precedence : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.36-62) を参照してください。</p>
ステップ 6 <code>set {dscp new-dscp ip precedence new-precedence}</code>	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • dscp new-dscp には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • ip precedence new-precedence には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。

	コマンド	目的
ステップ 7	<code>police rate-bps burst-byte [exceed-action {drop policed-dscp-transmit}]</code>	<p>分類したトラフィックにポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.36-34)を参照してください。</p> <ul style="list-style-type: none"> • <code>rate-bps</code> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <code>burst-byte</code> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットを廃棄する場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.36-64)を参照してください。
ステップ 8	<code>exit</code>	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	<code>interface interface-id</code>	<p>ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>指定できるインターフェイスとして、物理ポートも含まれます。</p>
ステップ 11	<code>service-policy input policy-map-name</code>	<p>ポリシーマップ名を指定し、入力ポートに適用します。</p> <p>サポートされるポリシー マップは、入力ポートごとに 1 つだけです。</p>
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show policy-map [policy-map-name [class class-map-name]]</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map policy-map-name** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class class-map-name** ポリシー マップ コンフィギュレーション コマンドを使用します。**untrusted** ステートに戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set {dscp new-dscp | ip precedence new-precedence}** ポリシー マップ コンフィギュレーション コマンドを使用します。既存のポリサーを削除するには、**no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]** ポリシー マップ コンフィギュレーション コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、**no service-policy input policy-map-name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポリシー マップを作成し、入力ポートに結合する例を示します。この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。この分類にトラフィックが一致した場合、着信パケットの DSCP 値が信頼されます。一致したトラフィックが平均トラフィック レート (48000 bps)、および標準バースト サイズ (8000 バイト) を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP はマークダウンされて、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
```



```
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を示します。最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番目の許可ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックだけが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

SVI 上で階層型のポリシー マップを設定できますが、その他のタイプのインターフェイス上では設定できません。階層型のポリシングは、VLAN レベルおよびインターフェイス レベルのポリシー マップで構成された、1 つのポリシー マップとして作成されます。

SVI では、VLAN レベルのポリシー マップが作用対象とするトラフィック クラスを指定します。アクションには、CoS、DSCP、IP precedence 値の信頼、またはトラフィック クラスの特定の DSCP、IP precedence 値の設定が含まれます。個々のポリサーで作用を受ける物理ポートを指定するには、インターフェイス レベルのポリシー マップを使用します。



(注)

10 ギガビット イーサネット インターフェイスは、ポリシー マップを使用したポリシングをサポートしません。

階層型のポリシー マップを設定するときには、次の注意事項に従ってください。

- 階層型のポリシー マップを設定する前に、インターフェイス レベルのポリシー マップで指定した物理ポートの VLAN ベースの QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに付加できるポリシー マップは、1 つだけです。

- 1 つのポリシー マップに、それぞれ異なる一致条件とアクションを指定した複数のクラス ステートメントを指定できます。
- SVI で受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- スイッチ スタックでは、**match input-interface** クラスマップ コンフィギュレーション コマンドを使用して、ポリシー マップ クラスにスタック メンバー全体のインターフェイスを指定できません。
- ポリシー マップとポート信頼状態の両方を物理インターフェイス上で有効にすることができます。ポリシー マップは、ポート信頼状態の前に適用されます。
- **mls qos map ip-prec-dscp dscp1...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにだけ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを使用すると、スイッチはスイッチ設定でこのコマンドを **set dscp** に変更します。**set ip dscp** コマンドを入力した場合、スイッチ コンフィギュレーションでは **set dscp** の設定として表示されます。
- **set ip precedence** または **set precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP Precedence 値を変更できます。この設定は、スイッチ コンフィギュレーションで **set ip precedence** として表示されます。
- VLAN ベースの QoS がイネーブルの場合、階層型のポリシー マップは直前に設定したポートベースのポリシー マップを優先します。
- 階層型のポリシー マップは SVI に適用され、VLAN に属するすべてのトラフィックに影響します。VLAN レベルのポリシー マップで指定されたアクションは、その SVI のトラフィックに影響します。ポート レベルのポリシー マップのポリシング作業は、影響のある物理インターフェイスの入力トラフィックに影響します。
- トランク ポートの階層型のポリシー マップを設定する場合、VLAN の範囲と重ならないようにしてください。範囲が重なると、ポリシー マップで指定されたアクションは、重なっている VLAN の着信トラフィックおよび発信トラフィックにも作用します。
- 集約ポリサーは階層型のポリシー マップではサポートされません。
- VLAN ベースの QoS がイネーブルになると、スイッチは VLAN マップなどの VLAN ベースの機能をサポートします。
- 階層型のポリシー マップは、プライベート VLAN のプライマリ VLAN 上のみ設定できます。
- VLAN ベース QoS をイネーブルにして、スイッチ スタックに階層型ポリシー マップを設定する場合に、スタックの設定を変更すると、次のアクションが自動的に実行されます。
 - 新しいスタック マスターが選択されると、スタック マスターは自身の適用可能なすべてのインターフェイス上でこれらの機能を再度イネーブルにして、再設定します。
 - 新しいスタック メンバーが追加されると、スタック マスターはスタック メンバーの適用可能なすべてのポート上でこれらの機能を再度イネーブルにして、再設定します。
 - スイッチ スタックをマージすると、新しいスタック マスターは新しいスタック上のスイッチでこれらの機能を再度イネーブルにして、再設定します。
 - スイッチ スタックが 2 つ以上のスイッチ スタックに分割されると、各スイッチ スタックのスタック マスターは、スタック マスターを含むスタック メンバーの適用可能なすべてのインターフェイス上でこの機能を再度イネーブルにして、再設定します。

階層型ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>class-map [match-all match-any] class-map-name</code>	<p>VLAN レベルのクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。クラス マップについては、「クラス マップによるトラフィックの分類」(P.36-47) を参照してください。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <code>class-map-name</code> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定しない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 3	<code>match {access-group acl-index-or-name ip dscp dscp-list ip precedence ip-precedence-list}</code>	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> • access-group acl-index-or-name には、ACL の番号または名前を指定します。 • ip dscp dscp-list には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 • ip precedence ip-precedence-list には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 4	<code>exit</code>	クラス マップ コンフィギュレーション モードに戻ります。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 6 class-map [match-all match-any] <i>class-map-name</i>	<p>インターフェイス レベルのクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>match-all または match-any のどちらのキーワードも指定しない場合、デフォルトは match-all です。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。</p>
ステップ 7 match input-interface <i>interface-id-list</i>	<p>インターフェイス レベルのクラス マップを実行する物理ポートを指定します。次の方法で、最大 6 つ指定できます。</p> <ul style="list-style-type: none"> • 単一のポート (1 つのエントリとしてカウントされます) • スペースで区切られたポートのリスト (各ポートが 1 つのエントリとしてカウントされます) • ハイフンで区切られたポートの範囲 (2 つのエントリとしてカウントされます) <p>このコマンドは、子レベルのポリシー マップでのみ使用可能で、子レベル ポリシー マップ内にある唯一の一致条件でなければなりません。</p>
ステップ 8 exit	<p>クラス マップ コンフィギュレーション モードに戻ります。</p>
ステップ 9 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 10 policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力してインターフェイス レベルのポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されておらず、ポリサーも実行されていません。</p>
ステップ 11 class-map <i>class-map-name</i>	<p>インターフェイス レベルのトラフィック分類を定義し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップのクラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 12 police <i>rate-bps burst-byte</i> [exceed-action { drop policed-dscp-transmit }]	<p>分類したトラフィックにそれぞれポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.36-34)を参照してください。</p> <ul style="list-style-type: none"> • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットを廃棄する場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.36-64)を参照してください。
ステップ 13 exit	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 14 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 15 policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力することによって VLAN レベルのポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ 16 class <i>class-map-name</i>	<p>VLAN レベルのトラフィック分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップのクラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 17 <code>trust [cos dscp ip-precedence]</code>	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。</p> <p>(注) このコマンドと <code>set</code> コマンドは、同じポリシー マップ内で相互に排他的になります。<code>trust</code> コマンドを入力する場合は、ステップ 18 を省略してください。</p> <p>デフォルトでは、ポートは <code>trusted</code> ではありません。このコマンドを入力するときにキーワードを指定しない場合、デフォルトは <code>dscp</code> になります。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • <code>cos</code> : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • <code>dscp</code> : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • <code>ip-precedence</code> : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.36-62) を参照してください。</p>
ステップ 18 <code>set {dscp new-dscp ip precedence new-precedence}</code>	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • <code>dscp new-dscp</code> には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • <code>ip precedence new-precedence</code> には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。
ステップ 19 <code>service-policy policy-map-name</code>	<p>インターフェイス レベルのポリシー マップ名を指定し (ステップ 10 を参照)、VLAN レベルのポリシー マップと連動させます。</p> <p>VLAN レベルのポリシー マップで複数のクラスが指定されている場合、Cisco IOS Release 12.2(25)SED 以降は、各クラスで別々の <code>service-policy policy-map-name</code> コマンドを使用できます。</p>
ステップ 20 <code>exit</code>	<p>ポリシー マップ コンフィギュレーション モードに戻ります。</p>
ステップ 21 <code>exit</code>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 22 <code>interface interface-id</code>	<p>階層型のマップを適用する SVI を指定し、インターフェイス コンフィギュレーション モードを開始します。</p>

コマンド	目的
ステップ 23 service-policy input <i>policy-map-name</i>	VLAN レベルのポリシーマップ名を指定し、SVI にそれを適用します。前のステップとこのコマンドを使用して、他の SVI にポリシーマップを適用します。 階層型 VLAN レベルのポリシーマップに複数のインターフェイスレベルのポリシーマップがある場合、すべてのクラスが service-policy <i>policy-map-name</i> コマンドで指定されている同じ VLAN レベルのポリシーマップに設定されている必要があります。
ステップ 24 end	特権 EXEC モードに戻ります。
ステップ 25 show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] または show mls qos vlan-based	設定を確認します。
ステップ 26 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map *policy-map-name*** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除するには、**no class *class-map-name*** ポリシー マップ コンフィギュレーション コマンドを使用します。

ポリシー マップで **untrusted** の状態に戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、**no set {dscp *new-dscp* | ip precedence *new-precedence*}** ポリシーマップ コンフィギュレーション コマンドを使用します。

インターフェイス レベルのポリシー マップの既存のポリサーを削除するには、**no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]** ポリシーマップ コンフィギュレーション コマンドを使用します。階層型のポリシー マップとポートの対応付けを削除するには、**no service-policy input *policy-map-name*** インターフェイス コンフィギュレーション コマンドを使用します。

次に、階層型のポリシー マップの作成方法を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
```

次に、SVI に新しいマップを割り当てる例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input g3/0/1 - g3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class-map cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class-map cm-1
Switch(config-pmap-c)# set dscp 7
```

```

Switch(config-pmap-c) # service-policy port-plcmap-1
Switch(config-pmap-c) # exit
Switch(config-pmap) # class-map cm-2
Switch(config-pmap-c) # match ip dscp 2
Switch(config-pmap-c) # service-policy port-plcmap-1
Switch(config-pmap) # exit
Switch(config-pmap) # class-map cm-3
Switch(config-pmap-c) # match ip dscp 3
Switch(config-pmap-c) # service-policy port-plcmap-2
Switch(config-pmap) # exit
Switch(config-pmap) # class-map cm-4
Switch(config-pmap-c) # trust dscp
Switch(config-pmap) # exit
Switch(config) # interface vlan 10
Switch(config-if) # ser input vlan-plcmap
Switch(config-if) # exit
Switch(config) # exit
Switch#

```

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシー マップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップにのみ設定できます。



(注) 10 ギガビット イーサネット インターフェイスは集約ポリサーを使用したポリシングをサポートしません。

集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos aggregate-policer <i>aggregate-policer-name rate-bps burst-byte</i> exceed-action {drop policed-dscp-transmit}	<p>同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。</p> <p>デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.36-34) を参照してください。</p> <ul style="list-style-type: none"> • <i>aggregate-policer-name</i> には、集約ポリサーの名前を指定します。 • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 1000000000 です。 • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。パケットを廃棄する場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.36-64) を参照してください。

	コマンド	目的
ステップ 3	class-map [match-all match-any] <i>class-map-name</i>	必要に応じて、トラフィックを分類するクラス マップを作成します。詳細については、「 クラス マップによるトラフィックの分類 」(P.36-47) を参照してください。
ステップ 4	policy-map <i>policy-map-name</i>	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 詳細については、「 ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング 」(P.36-49) を参照してください。
ステップ 5	class <i>class-map-name</i>	トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 詳細については、「 ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング 」(P.36-49) を参照してください。
ステップ 6	police aggregate <i>aggregate-policer-name</i>	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 <i>aggregate-policer-name</i> には、ステップ 2 で指定した名前を入力します。
ステップ 7	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	interface <i>interface-id</i>	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 9	service-policy input <i>policy-map-name</i>	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートごとに 1 つだけです。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show mls qos aggregate-policer [<i>aggregate-policer-name</i>]	設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された集約ポリサーをポリシー マップから削除するには、**no police aggregate *aggregate-policer-name*** ポリシー マップ コンフィギュレーション モードを使用します。集約ポリサーおよびそのパラメータを削除するには、**no mls qos aggregate-policer *aggregate-policer-name*** グローバル コンフィギュレーション コマンドを使用します。

次に、集約ポリサーを作成して、ポリシー マップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。トラフィックが平均レート (48000 bps)、および標準バースト サイズ (8000 バイト) を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP がマークダウンされて、送信されます。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
```

```

Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit

```

DSCP マップの設定

ここでは、次の設定情報について説明します。

- 「CoS/DSCP マップの設定」(P.36-62) (任意)
- 「IP precedence/DSCP マップの設定」(P.36-63) (任意)
- 「ポリシング済み DSCP マップの設定」(P.36-64) (任意、マップのヌル設定が不適切な場合以外)
- 「DSCP/CoS マップの設定」(P.36-65) (任意)
- 「DSCP/DSCP 変換マップの設定」(P.36-66) (任意、マップのヌル設定が不適切な場合以外)

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。

表 36-12 に、デフォルトの CoS/DSCP マップを示します。

表 36-12 デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map cos-dscp dscp1...dscp8</code>	CoS/DSCP マップを変更します。 <i>dscp1...dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps cos-dscp</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos cos-dscp` グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
  cos:   0  1  2  3  4  5  6  7
-----
  dscp:  10 15 20 25 30 35 40 45
```

IP precedence/DSCP マップの設定

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。

表 36-13 に、デフォルトの IP precedence/DSCP マップを示します。

表 36-13 デフォルトの IP precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map ip-prec-dscp dscp1...dscp8</code>	IP precedence/DSCP マップを変更します。 <i>dscp1...dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps ip-prec-dscp</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos ip-prec-dscp` グローバル コンフィギュレーション コマンドを使用します。

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
  ipprec:   0  1  2  3  4  5  6  7
  -----
           dscp:  10 15 20 25 30 35 40 45
```

ポリシング済み DSCP マップの設定

ポリシングおよびマーキング アクションによって得られる新しい値に DSCP 値をマークダウンするには、ポリシング済み DSCP マップを使用します。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map policed-dscp dscp-list to mark-down-dscp</code>	ポリシング済み DSCP マップを変更します。 <ul style="list-style-type: none"> <i>dscp-list</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <i>mark-down-dscp</i> には、対応するポリシング済み（マークダウンされる）DSCP 値を入力します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps policed-dscp</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマッピングに戻すには、**no mls qos policed-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 50 ~ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
Policed-dscp map:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 : 00 01 02 03 04 05 06 07 08 09
  1 : 10 11 12 13 14 15 16 17 18 19
  2 : 20 21 22 23 24 25 26 27 28 29
  3 : 30 31 32 33 34 35 36 37 38 39
  4 : 40 41 42 43 44 45 46 47 48 49
  5 : 00 00 00 00 00 00 00 00 58 59
  6 : 60 61 62 63
```



(注)

このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。

表 36-14 に、デフォルトの DSCP/CoS マップを示します。

表 36-14 デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

DSCP/CoS マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos map dscp-cos dscp-list to cos</code>	DSCP/CoS マップを変更します。 <ul style="list-style-type: none"> <code>dscp-list</code> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <code>cos</code> には、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ~ 63、CoS の範囲は 0 ~ 7 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps dscp-to-cos</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no mls qos dscp-cos` グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :    00 00 00 00 00 00 00 00 00 01
  1 :    01 01 01 01 01 01 00 02 02 02
  2 :    02 02 02 02 00 03 03 03 03 03
  3 :    03 03 00 04 04 04 04 04 04 04
  4 :    00 05 05 05 05 05 05 05 00 06
  5 :    00 06 06 06 06 06 06 07 07 07
  6 :    07 07 07 07
```



(注)

上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。

DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポート適用します (入力変換)。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を使用してパケットを処理します。スイッチは新しい DSCP 値を使用して、ポートからパケットを送信します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map dscp-mutation <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを変更します。 <ul style="list-style-type: none"> <i>dscp-mutation-name</i> には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 <i>in-dscp</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>out-dscp</i> には、DSCP 値を 1 つ入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	interface interface-id	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	mls qos dscp-mutation <i>dscp-mutation-name</i>	指定された DSCP trusted 入力ポートにマップを適用します。 <i>dscp-mutation-name</i> には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mls qos maps dscp-mutation	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no mls qos dscp-mutation dscp-mutation-name** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP/DSCP 変換マップを定義する例を示します。明示的に設定されていないすべてのエントリは変更されません (空のマップで指定された値のままです)。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
mutation1:
  d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
  0 : 00 00 00 00 00 00 00 00 10 10
  1 : 10 10 10 10 14 15 16 17 18 19
  2 : 20 20 20 23 24 25 26 27 28 29
  3 : 30 30 30 30 30 35 36 37 38 39
  4 : 40 41 42 43 44 45 46 47 48 49
  5 : 50 51 52 53 54 55 56 57 58 59
  6 : 60 61 62 63
```



(注)

上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

入力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- 各キューに (DSCP 値または CoS 値によって) 割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック (音声など) の有無

ここでは、次の設定情報について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.36-68) (任意)
- 「入力キュー間のバッファ スペースの割り当て」(P.36-70) (任意)
- 「入力キュー間の帯域幅の割り当て」(P.36-70) (任意)
- 「入力プライオリティ キューの設定」(P.36-71) (任意)

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットが廃棄されるようにキューのしきい値を調整します。

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 mls qos srr-queue input dscp-map queue <i>queue-id</i> threshold <i>threshold-id</i> <i>dscp1...dscp8</i> または mls qos srr-queue input cos-map queue <i>queue-id</i> threshold <i>threshold-id</i> <i>cos1...cos8</i>	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ~ 39 および 48 ~ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ~ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ~ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 <ul style="list-style-type: none"> • <i>queue-id</i> に指定できる範囲は、1 ~ 2 です。 • <i>threshold-id</i> に指定できる範囲は、1 ~ 3 です。しきい値 3 の廃棄の割合は定義済みであり、キューフル ステートに設定されます。 • <i>dscp1...dscp8</i> には、最大 8 つの値をスペースで区切って入力します。指定できる範囲は 0 ~ 63 です。 • <i>cos1...cos8</i> には、最大 8 つの値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
ステップ 3 mls qos srr-queue input threshold <i>queue-id</i> <i>threshold-percentage1</i> <i>threshold-percentage2</i>	入力キューに 2 つの WTD しきい値の割合（しきい値 1 および 2 用）を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。 <ul style="list-style-type: none"> • <i>queue-id</i> に指定できる範囲は、1 ~ 2 です。 • <i>threshold-percentage1</i> <i>threshold-percentage2</i> に指定できる範囲は、1 ~ 100 です。各値はスペースで区切ります。 各しきい値は、キューに割り当てられたキュー記述子の総数の割合です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show mls qos maps	設定を確認します。 DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点が入力キュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。 CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの CoS 入力キューしきい値マップまたはデフォルトの DSCP 入力キューしきい値マップに戻すには、**no mls qos srr-queue input cos-map**、または **no mls qos srr-queue input dscp-map** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD しきい値の割合に戻すには、**no mls qos srr-queue input threshold *queue-id*** グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 0 ～ 6 を、入力キュー 1 およびしきい値 1（ドロップしきい値が 50%）にマッピングする例を示します。DSCP 値 20 ～ 26 は、入力キュー 1 およびしきい値 2（ドロップしきい値が 70%）にマッピングされます。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

この例では、50% の WTD しきい値が DSCP 値（0 ～ 6）に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値（20 ～ 26）よりも先に廃棄されます。

入力キュー間のバッファ スペースの割り当て

2 つのキュー間で入力バッファを分割する比率を定義します（スペース量を割り当てます）。バッファ割り当てと帯域幅割り当てにより、パケットが廃棄される前にバッファに格納できるデータ量が制御されます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input buffers percentage1 percentage2	入力キュー間にバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 <i>percentage1 percentage2</i> に指定できる範囲は、0 ～ 100 です。各値はスペースで区切ります。 キューが着信バースト トラフィックをすべて処理できるように、バッファを割り当てる必要があります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos interface buffer または show mls qos input-queue	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、バッファ スペースの 60% を入力キュー 1 に、40% を入力キュー 2 に割り当てる例を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。帯域幅割り当てとバッファ割り当てにより、パケットが廃棄される前にバッファに格納できるデータ量を制御できます。入力キューで SRR が動作するのは、共有モードの場合のみです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>mls qos srr-queue input bandwidth weight1 weight2</code>	入力キューに共有ラウンド ロビン重みを割り当てます。 <i>weight1</i> および <i>weight2</i> のデフォルト設定は 4 です (帯域幅の 1/2 が 2 つのキューで等しく共有されます)。 <i>weight1</i> および <i>weight2</i> に指定できる範囲は、1 ~ 100 です。各値はスペースで区切ります。 SRR は <code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code> グローバル コンフィギュレーション コマンドの bandwidth キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は <code>mls qos srr-queue input bandwidth weight1 weight2</code> グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。詳細については、「 入力プライオリティ キューの設定 (P.36-71) 」を参照してください。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4 <code>show mls qos interface queueing</code> または <code>show mls qos input-queue</code>	設定を確認します。
ステップ 5 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no mls qos srr-queue input bandwidth` グローバル コンフィギュレーション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューはディセーブルです。キュー 1 に割り当てられた共有帯域幅の比率は 25/(25+75)、キュー 2 の比率は 75/(25+75) です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

入力プライオリティ キューの設定

プライオリティ キューは、迅速な処理が必要なトラフィック (遅延およびジッタを最小に抑える必要のある音声トラフィックなど) にのみ使用します。

プライオリティ キューは、オーバーサブスクライブ リングに激しいネットワーク トラフィックが発生している状況で (バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームが廃棄されている場合)、遅延およびジッタを軽減するように帯域幅の一部が保証されています。

SRR は `mls qos srr-queue input priority-queue queue-id bandwidth weight` グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は `mls qos srr-queue input bandwidth weight1 weight2` グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code>	キューをプライオリティ キューとして割り当て、スタックリングが輻輳している場合にリングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー 2 です。このキューには帯域幅の 10% が割り当てられています。 <ul style="list-style-type: none"> • <code>queue-id</code> に指定できる範囲は、1 ~ 2 です。 • <code>bandwidth weight</code> には、スタックリングの帯域幅に対する割合を割り当てます。指定できる範囲は 0 ~ 40 です。値が大きい場合はリング全体に影響が及び、スタックのパフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos interface queueing</code> または <code>show mls qos input-queue</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no mls qos srr-queue input priority-queue queue-id` グローバル コンフィギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、`mls qos srr-queue input priority-queue queue-id bandwidth 0` を入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は、帯域幅の 10% が割り当てられているプライオリティ キューです。キュー 1 および 2 に割り当てられている帯域幅比率は 4/(4+4) です。SRR は、10% の帯域幅が設定されたキュー 1 (プライオリティ キュー) を最初に処理します。次に、SRR は残りの 90% の帯域幅をキュー 1 と 2 にそれぞれ 45% ずつ割り当てて、各キューで等しく共有します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット (ポートごとの 4 つの出力キュー) に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キュー セットに割り当てる固定バッファ スペースの量
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術 (シェーピング、共有、または両方)

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」 (P.36-73)
- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」 (P.36-73) (任意)
- 「出力キューおよび ID への DSCP または CoS 値のマッピング」 (P.36-75) (任意)
- 「出力キューでの SRR シェーピング重みの設定」 (P.36-76) (任意)
- 「出力キューでの SRR 共有重みの設定」 (P.36-78) (任意)
- 「出力緊急キューの設定」 (P.36-79) (任意)
- 「出力インターフェイスの帯域幅の制限」 (P.36-79) (任意)

設定時の注意事項

緊急キューをイネーブルにする、または SRR 重みに基づいて出力キューを処理する場合は、次の注意事項に従ってください。

- 出力緊急キューがイネーブルの場合、キュー 1 に対応する SRR シェーピング重みおよび共有重みは上書きされます。
- 出力緊急キューがディセーブルで、SRR シェーピング重みおよび共有重みが設定されている場合、シェーピング モードはキュー 1 の共有モードを無効にし、SRR はこのキューをシェーピング モードで処理します。
- 出力緊急キューがディセーブルで、SRR シェーピング重みが設定されていない場合、SRR はこのキューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファの可用性の保証、WTD しきい値の設定、およびキューセットの最大割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。

各しきい値はキューに割り当てられたバッファの割合です。この値を指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサポートします。



(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

メモリ割り当てを設定し、キューセットを廃棄するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos queue-set output <i>qset-id</i> buffers <i>allocation1</i> ... <i>allocation4</i></code>	<p>キューセットにバッファを割り当てます。</p> <p>デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます (25、25、25、25)。各キューにはバッファ スペースの 1/4 が割り当てられます。</p> <ul style="list-style-type: none"> • <i>qset-id</i> には、キューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。各ポートはキューセットに属し、キューセットでは、ポートごとに 4 つの出力キューの特性がすべて定義されます。 • <i>allocation1</i> ... <i>allocation4</i> には、キューセット内のキューごとに 1 つずつ、合計 4 つのパーセントを指定します。<i>allocation1</i>、<i>allocation3</i>、<i>allocation4</i> の場合、指定できる範囲は 0 ~ 99 です。<i>allocation2</i> の場合、指定できる範囲は 1 ~ 100 です (CPU バッファを含む)。 <p>トラフィックの重要性に従ってバッファを割り当てます。たとえば、プライオリティが最も高いトラフィックを格納するキューに、大きな割合のバッファを割り当てます。</p>
ステップ 3	<code>mls qos queue-set output <i>qset-id</i> threshold <i>queue-id</i> <i>drop-threshold1</i> <i>drop-threshold2</i> <i>reserved-threshold</i> <i>maximum-threshold</i></code>	<p>WTD を設定し、バッファの可用性を確保し、キューセット (ポートごとに 4 つの出力キュー) の最大メモリ割り当てを設定します。</p> <p>デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべてのキューの最大は 400% に設定されています。</p> <ul style="list-style-type: none"> • <i>qset-id</i> には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。 • <i>queue-id</i> には、コマンドの実行対象となるキューセット内の特定のキューを入力します。指定できる範囲は 1 ~ 4 です。 • <i>drop-threshold1</i> <i>drop-threshold2</i> には、キューの割り当てメモリの割合として表される 2 つの WTD しきい値を指定します。指定できる範囲は 1 ~ 3200% です。 • <i>reserved-threshold</i> には、割り当てメモリの割合として表されるキューに保証 (確保) されるメモリ サイズを入力します。指定できる範囲は 1 ~ 100% です。 • <i>maximum-threshold</i> を指定すると、いっぱいになったキューが確保量を越えるバッファを取得できるようになります。この値は、共通プールが空でない場合に、パケットが廃棄されるまでキューが使用できるメモリの最大値です。指定できる範囲は 1 ~ 3200% です。
ステップ 4	<code>interface <i>interface-id</i></code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>queue-set <i>qset-id</i></code>	<p>キューセットにポートをマッピングします。</p> <p><i>qset-id</i> には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ~ 2 です。デフォルト値は 1 です。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<code>show mls qos interface [interface-id] buffers</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no mls qos queue-set output qset-id buffers` グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD の割合に戻すには、`no mls qos queue-set output qset-id threshold [queue-id]` グローバル コンフィギュレーション コマンドを使用します。

次に、ポートをキューセット 2 にマッピングする例を示します。出力キュー 1 にはバッファ スペースの 40%、出力キュー 2、3、および 4 には 20% が割り当てられます。キュー 2 の廃棄は割り当てメモリの 40 および 60% に設定され、割り当てメモリの 100% が保証 (確保) され、パケットが廃棄されるまでこのキューが使用できる最大メモリが 200% に設定されます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/0/1
!Switch(config-if)# queue-set 2
```

出力キューおよび ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットが廃棄されるようにキューを調整します。



(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8</code> または <code>mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8</code>	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ~ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ~ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ~ 39 および 48 ~ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ~ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 <ul style="list-style-type: none"> • <code>queue-id</code> に指定できる範囲は、1 ~ 4 です。 • <code>threshold-id</code> に指定できる範囲は、1 ~ 3 です。しきい値 3 の廃棄の割合は定義済みであり、キューフル ステートに設定されます。 • <code>dscp1...dscp8</code> には、最大 8 つの値をスペースで区切って入力します。指定できる範囲は 0 ~ 63 です。 • <code>cos1...cos8</code> には、最大 8 つの値をスペースで区切って入力します。指定できる範囲は 0 ~ 7 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos maps</code>	設定を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、`no mls qos srr-queue output dscp-map` または `no mls qos srr-queue output cos-map` グローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

出力キューでの SRR シェーピング重みの設定



(注) 10 ギガビット インターフェイス上で SRR シェーピング重みは設定できません。

各キューに割り当てられる使用可能な帯域幅の量を指定できます。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックを平滑化したり、出力をより滑らかにしたりするには、シェーピングを使用します。シェーピング重みの詳細については、「SRR のシェーピングおよび共有」(P.36-14) を参照してください。共有重みの詳細については、「出力キューでの SRR 共有重みの設定」(P.36-78) を参照してください。



(注) 入力 10 ギガビット インターフェイスで帯域幅は制限できません。

ポートにマッピングされた 4 つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 srr-queue bandwidth shape weight1 weight2 weight3 weight4	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 weight1 weight2 weight3 weight4 には、シェーピングされるポートの割合を制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比率 (1/weight) によって制御されます。各値はスペースで区切ります。指定できる範囲は 0 ~ 65535 です。 重み 0 を設定した場合は、対応するキューが共有モードで動作します。 srr-queue bandwidth shape コマンドで指定された重みは無視されます。 srr-queue bandwidth share インターフェイス コンフィギュレーション コマンドで各キューに指定された重みが有効になります。シェーピング および共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは共有モードより優先されます。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show mls qos interface interface-id queueing	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。

次に、キュー 1 に帯域幅のシェーピングを設定する例を示します。キュー 2、3、および 4 の重み比率は 0 に設定されているため、これらのキューは共有モードで動作します。キュー 1 の帯域幅の重みは 1/8 (12.5%) です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

出力キューでの SRR 共有重みの設定

共有モードでは、各キューは設定された重みに従って帯域幅を共有します。帯域幅に対してはこのレベルが保証されますが、このレベルに限定されるわけではありません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。



(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

ポートにマッピングされた 4 つの出力キューに共有重みを割り当てて、帯域幅の共有をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>srr-queue bandwidth share weight1 weight2 weight3 weight4</code>	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 <code>weight1 weight2 weight3 weight4</code> には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は 1 ~ 255 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface interface-id queueing</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth share` インターフェイス コンフィギュレーション コマンドを使用します。

次に、出力ポートで稼働している SRR スケジューラの重み比率を設定する例を示します。4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー 1、2、3、および 4 に対して $1/(1+2+3+4)$ 、 $2/(1+2+3+4)$ 、 $3/(1+2+3+4)$ 、および $4/(1+2+3+4)$ になります（それぞれ、10、20、30、および 40%）。つまり、キュー 4 の帯域幅はキュー 1 の 4 倍、キュー 2 の 2 倍、キュー 3 の約 1.3 倍です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のパケットより高くできます。SRR は、このキューが空になるまで処理してから他のキューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mls qos</code>	スイッチ上で QoS をイネーブルにします。
ステップ 3	<code>interface interface-id</code>	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>priority-queue out</code>	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、 <code>srr-queue bandwidth shape</code> または <code>srr-queue bandwidth share</code> コマンドの <code>weight1</code> が無視されます（比率計算に使用されません）。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

出力緊急キューをディセーブルにするには、`no priority-queue out` インターフェイス コンフィギュレーション コマンドを使用します。

次に、SRR 重みが設定されている場合に出力緊急キューをイネーブルにする例を示します。出力緊急キューは、設定済みの SRR 重みよりも優先されます。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

出カインターフェイスの帯域幅の制限



(注) 10 ギガビット インターフェイス上で SSR シェーピング重みは設定できません。

出力ポートの帯域幅は制限できます。たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。



(注) ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

出力ポートの帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>srr-queue bandwidth limit weight1</code>	ポートの上限となるポート速度の割合を指定します。指定できる範囲は 10 ~ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface [interface-id] queueing</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth limit` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。回線レートは接続速度の 80% (800 Mbps) に低下します。ハードウェアは回線レートを増分値 6 で調整するので、これらは厳密な値ではありません。

標準 QoS 情報の表示

標準 QoS 情報を表示するには、表 36-15 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 36-15 標準 QoS 情報を表示するためのコマンド

コマンド	目的
<code>show class-map [class-map-name]</code>	トラフィックを分類するための一致条件を定義した QoS クラスマップを表示します。
<code>show mls qos</code>	グローバル QoS コンフィギュレーション情報を表示します。
<code>show mls qos aggregate-policer [aggregate-policer-name]</code>	集約ポリサーの設定を表示します。
<code>show mls qos input-queue</code>	入力キューの QoS 設定を表示します。
<code>show mls qos interface [interface-id] [buffers policers queueing statistics]</code>	バッファ割り当て、ポリサーが設定されるポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。
<code>show mls qos maps [cos-dscp cos-input-q cos-output-q dscp-cos dscp-input-q dscp-mutation dscp-mutation-name dscp-output-q ip-prec-dscp policed-dscp]</code>	QoS マッピング情報を表示します。

表 36-15 標準 QoS 情報を表示するためのコマンド (続き)

コマンド	目的
<code>show mls qos queue-set [qset-id]</code>	出力キューの QoS 設定を表示します。
<code>show mls qos vlan vlan-id</code>	指定の SVI に適用されたポリシー マップを表示します。
<code>show policy-map [policy-map-name [class class-map-name]]</code>	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 (注) 着信トラフィックの分類情報を表示する場合は、 show policy-map interface 特権 EXEC コマンドを使用しないでください。 control-plane および interface キーワードはサポートされていません。表示される統計情報は無視してください。
<code>show running-config include rewrite</code>	透過的な DSCP 設定を表示します。



CHAPTER 37

EtherChannel およびリンクステート トラッキングの設定

この章では、Catalyst 3750 スイッチに EtherChannel を設定する方法について説明します。EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールト トレラントな高速リンクを提供します。EtherChannel を使用すると、ワイヤリング クローゼットおよびデータ センタ間の帯域幅を拡張できます。EtherChannel はネットワーク上でボトルネックの発生が見込まれるところに、どこでも配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャンネル内の他のリンクにトラフィックをリダイレクトします。この章では、リンクステート トラッキングを設定する方法についても説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

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

- [「EtherChannel の概要」 \(P.37-1\)](#)
- [「EtherChannel の設定」 \(P.37-11\)](#)
- [「EtherChannel、PAgP、および LACP ステータスの表示」 \(P.37-25\)](#)
- [「リンクステート トラッキングの概要」 \(P.37-25\)](#)
- [「リンクステート トラッキングの設定」 \(P.37-28\)](#)

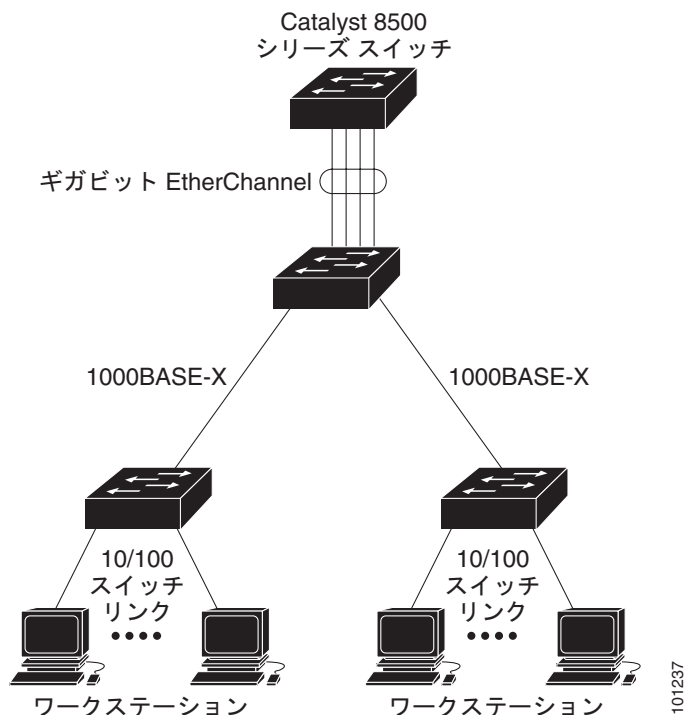
EtherChannel の概要

- [「EtherChannel の概要」 \(P.37-2\)](#)
- [「ポートチャンネル インターフェイス」 \(P.37-4\)](#)
- [「PAgP」 \(P.37-5\)](#)
- [「LACP」 \(P.37-7\)](#)
- [「EtherChannel の On モード」 \(P.37-8\)](#)
- [「ロード バランシングおよび転送方式」 \(P.37-9\)](#)
- [「EtherChannel およびスイッチ スタック」 \(P.37-10\)](#)

EtherChannel の概要

EtherChannel は単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます (図 37-1 を参照)。

図 37-1 一般的な EtherChannel 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 800 Mbps (ファスト EtherChannel) または 8 Gbps (ギガビット EtherChannel) の全二重帯域幅を提供します。各 EtherChannel は、互換性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

各 EtherChannel 内のすべてのポートは、レイヤ 2 またはレイヤ 3 ポートのいずれかとして設定する必要があります。EtherChannel の数は 48 に制限されています。EtherChannel レイヤ 3 ポートは、ルーテッド ポートで構成されます。ルーテッド ポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用してレイヤ 3 モードに設定された物理ポートです。詳細については、第 12 章「インターフェイス特性の設定」を参照してください。

詳細については、「EtherChannel 設定時の注意事項」(P.37-12) を参照してください。

EtherChannel は、Port Aggregation Protocol (PAgP; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、または On のいずれかのモードに設定できます。EtherChannel の両端は同じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端とネゴシエーションし、アクティブにするポートを決定します。互換性のないポートは独立ステートになり、他の単一リンクのようにデータトラフィックに伝送し続けます。ポート設定は変更されませんが、ポートは EtherChannel に参加しません。
- EtherChannel を on モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel のもう一方の端 (他のスイッチ上) も、同じように on モードに設定する必要があります。それ以外を設定した場合、パケットの損失が発生します。

EtherChannel はスタンドアロン スイッチ、スタック内の単一スイッチ、またはスタック内の複数のスイッチ（クロススタック EtherChannel と呼ばれています）上に作成できます。図 37-2 および図 37-3 を参照してください。

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになっている場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。EtherChannel の 1 つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、EtherChannel の他のリンクに戻らないようにブロックされます。

図 37-2 単一スイッチ EtherChannel

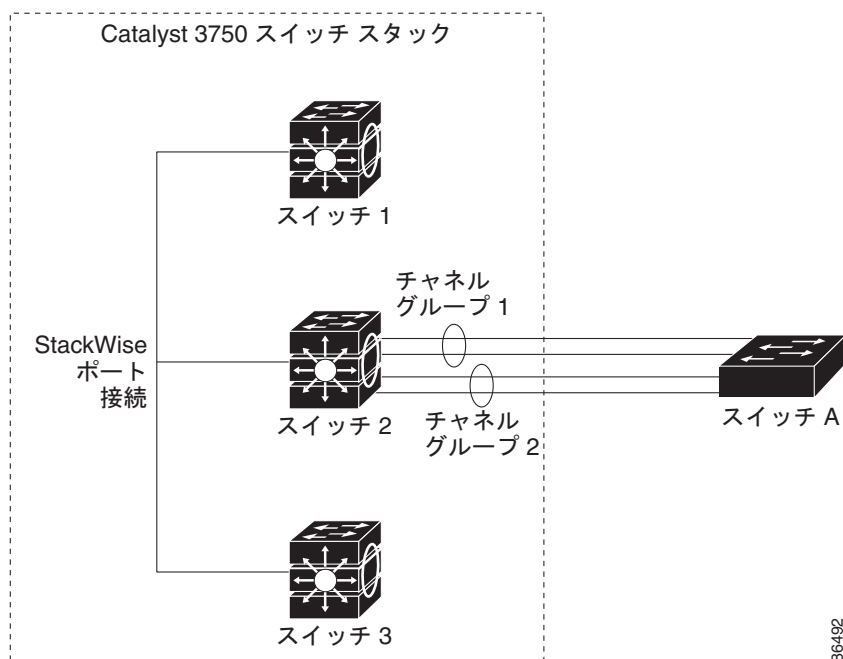
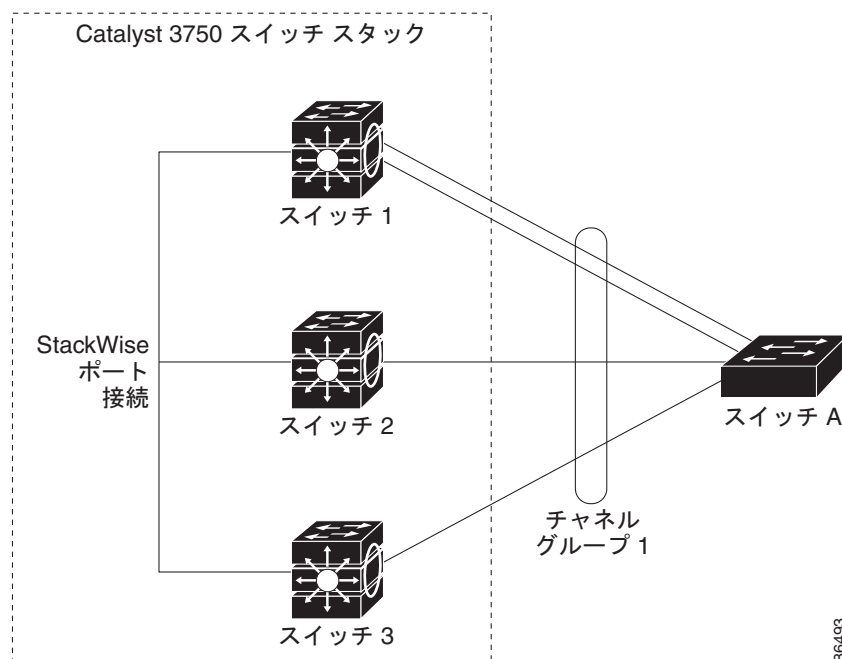


図 37-3 クロススタック EtherChannel



86493

ポートチャネル インターフェイス

EtherChannel を作成すると、ポート チャネル論理インターフェイスも作成されます。

- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを動的に作成します。

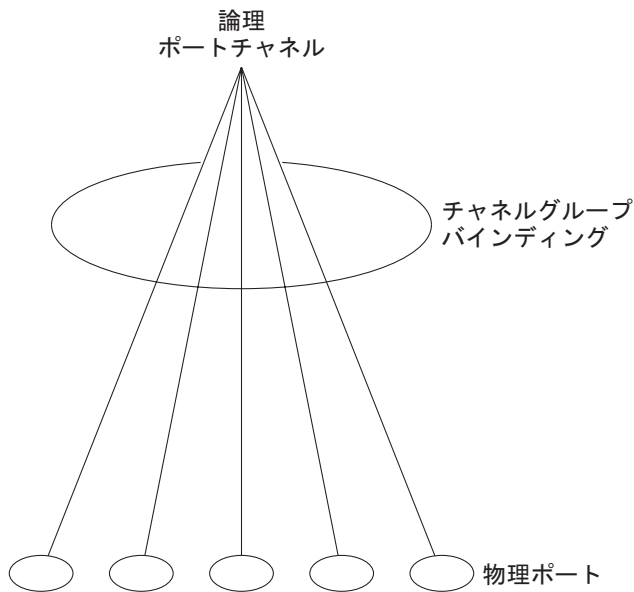
また、**interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用して、ポートチャネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、**channel-group channel-group-number** コマンドを使用する必要があります。**channel-group-number** は **port-channel-number** と同じ値に設定することも、違う値を使用することもできます。新しい値を使用すると、**channel-group** コマンドによって新しいポートチャネルが動的に作成されます。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。そのあと、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。

レイヤ 2 およびレイヤ 3 ポートのいずれの場合も、**channel-group** コマンドを実行すると、物理ポートと論理インターフェイスがバインドされます (図 37-4 を参照)。

各 EtherChannel には 1 ~ 48 番のポートチャネル論理インターフェイスがあります。ポートチャネルインターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定された番号に対応しています。

図 37-4 物理ポート、論理ポートチャンネル、およびチャンネル グループの関係



101238

EtherChannel の設定後 A ポートチャンネル インターフェイスに適用した設定変更は、そのポートチャンネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。EtherChannel のすべてのポートのパラメータを変更するには、コンフィギュレーション コマンド (スパニング ツリー コマンド、またはレイヤ 2 EtherChannel をトランクとして設定するコマンドなど) をポートチャンネル インターフェイスに適用します。

PAgP

Port Aggregation Protocol (PAgP) はシスコ独自のプロトコルで、シスコ製スイッチおよび PAgP をサポートするベンダーによってライセンス供与されたスイッチでのみ稼動します。PAgP を使用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク (チャンネルまたは集約ポート) に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランッキング ステータス、およびトランッキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成したあとで、PAgP は単一スイッチ ポートとして、スパニング ツリーにそのグループを追加します。

PAgP を使用できるのは、単一スイッチ EtherChannel 構成の場合だけです。クロススタック EtherChannel の場合は、PAgP をイネーブルにできません。次に、スタック内の単一のスイッチ上の設定が類似しているポートを、単一の論理リンクに動的にグループ化します。詳細については、「[EtherChannel 設定時の注意事項](#)」(P.37-12) を参照してください。

PAgP モード

表 37-1 に、**channel-group** インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel PAgP モードを示します。

表 37-1 EtherChannel PAgP モード

モード	説明
auto	<p>ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信を最小限に抑えます。</p> <p>EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合（クロススタック EtherChannel）、このモードはサポートされません。</p>
desirable	<p>ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。</p> <p>EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合（クロススタック EtherChannel）、このモードはサポートされません。</p>

スイッチ ポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトラッキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

PAgP モードが異なっても、モード間で互換性があるかぎり、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** モードまたは **auto** モードの別のポートとともに EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートとは EtherChannel を形成できません。

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、非サイレント動作としてスイッチ ポートを設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

仮想スイッチおよびデュアル アクティブ検出との PAgP 相互作用

仮想スイッチは 2 つ以上の Catalyst 6500 コア スイッチから成り、それらを仮想スイッチ リンク (VSL) で接続して制御トラフィックおよびデータ トラフィックを伝送します。スイッチの 1 つがアクティブ モードであり、それ以外のスイッチはスタンバイ モードです。冗長性のため、Catalyst 3750 スイッチなどのリモート スイッチを Remote Satellite Link (RSL) を使用して仮想スイッチに接続します。

2 つのスイッチ間の VSL で障害が発生した場合、一方のスイッチは他方のステータスを知りません。両方のスイッチがアクティブ モードになると、重複する構成（重複する IP アドレスとブリッジ識別子を含む）のネットワークでデュアルアクティブな状態になります。この場合、ネットワークがダウンする可能性があります。

デュアルアクティブな状態にならないようにするために、コア スイッチは RSL を介してリモート スイッチに PAgP Protocol Data Unit (PDU; プロトコル データ ユニット) を送信します。PAgP PDU はアクティブ スイッチを特定し、リモート スイッチはコア スイッチが同期状態となるように PDU をコア スイッチに転送します。アクティブ スイッチが故障したかリセットされた場合、スタンバイ スイッチがアクティブ スイッチとして処理を引き継ぎます。VSL がダウンした場合、一方のコア スイッチは他方のスイッチのステータスを知り、状態は変わりません。

PAgP と他の機能との相互作用

Dynamic Trunking Protocol (DTP) および Cisco Discovery Protocol (CDP) は、EtherChannel の物理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP Protocol Data Unit (PDU; プロトコル データ ユニット) を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

レイヤ 3 EtherChannel の場合は、(**interface port-channel** グローバル コンフィギュレーション コマンドを使用して) ポートが作成された直後に、スタック マスターから MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼動状態のポート上だけです。

LACP

LACP は IEEE 802.3ad で定義されており、シスコ製スイッチが IEEE 802.3ad プロトコルに適合したスイッチ間のイーサネット チャンネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク（チャンネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成したあとで、LACP は単一スイッチ ポートとして、スパニング ツリーにそのグループを追加します。

LACP モード

表 37-2 に、**channel-group** インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel LACP モードを示します。

表 37-2 EtherChannel LACP モード

モード	説明
アクティブ	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに返信しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

LACP モードが異なっても、モード間で互換性があるかぎり、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** モードまたは **passive** モードの別のポートとともに EtherChannel を形成できます。
- どのポートも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートとは EtherChannel を形成できません。

LACP と他の機能との相互作用

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

レイヤ 3 EtherChannel の場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用してインターフェイスが作成された直後に、スタック マスターから MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が **active** モードまたは **passive** モードでイネーブルになっている稼動状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合に限り EtherChannel を使用できます。

同じチャンネル グループの **on** モードで設定されたポートは、速度やデブプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されていたとしても、互換性のないポートは **suspended** ステートになります。



注意

on モードでの作業は慎重に行ってください。このモードは手動による設定が必要です。EtherChannel の両端のポートには同じ内容を設定する必要があります。グループの設定を誤ると、パケット損失またはスパンニング ツリー ループが発生する可能性があります。

ロード バランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャンネル内の 1 つのリンクを選択する数値に縮小することによって、チャンネル内のリンク間でトラフィックのロード バランシングを行います。EtherChannel のロード バランシングには、MAC アドレスまたは IP アドレス、送信元アドレスや宛先アドレスのどちらか一方、またはその両方のアドレスを使用できます。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方式を設定するには、**port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャンネル ポート間で分配されます。したがって、ロード バランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャンネル ポートを使用しますが、送信元ホストが同じパケットは同じチャンネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されている宛先ホストの MAC アドレスに基づいてチャンネル ポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャンネル ポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャンネル ポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のスイッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャンネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、IP アドレスが異なるパケットはそれぞれ異なるチャンネル ポートを使用しますが、IP アドレスが同じパケットは同じチャンネル ポートを使用します。

宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロード バランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャンネル ポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャンネル ポートで送信されます。

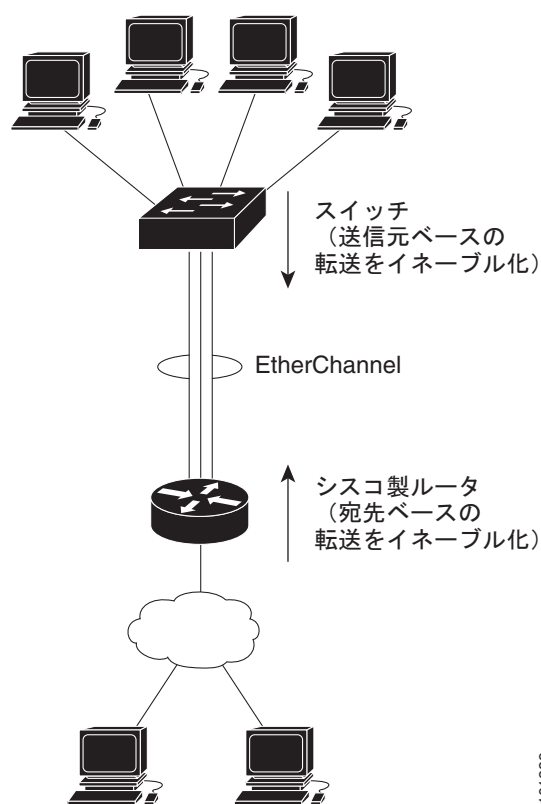
送信元/宛先 IP アドレスベース転送の場合、パケットは EtherChannel に送信されて、着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたものです。特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切であるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャンネル ポートを使用できます。

ロード バランシング方式ごとに利点異なります。ロード バランシング方式は、ネットワーク内のスイッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。

図 37-5 では、4 つのワークステーションからデータを集約しているスイッチからの EtherChannel がルータと通信しています。ルータは単一 MAC アドレス デバイスなので、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチがルータの使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。

設定で一番種類が多くなるオプションを使用してください。たとえば、チャンネル上のトラフィックが単一 MAC アドレスのみを宛先とする場合、宛先 MAC アドレスを使用すると、チャンネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなる場合があります。

図 37-5 負荷の分散および転送方式



101239

EtherChannel およびスイッチ スタック

EtherChannel に参加しているポートを持つスタック メンバーに障害が発生するか、またはこのスタック メンバーがスタックから脱退すると、スタック マスターはこのスタック メンバーのスイッチ ポートを EtherChannel から削除します。EtherChannel 内にポートが残っている場合、これらのポートは引き続き接続されています。

既存のスタックにスイッチが追加されると、新しいスイッチはスタック マスターから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック設定を使用して自身の設定を更新します。スタック メンバーは動作情報 (動作中のポート リスト、およびチャンネル メンバーであるポートのリスト) も受信します。

EtherChannel が設定された 2 つのスタックを結合すると、セルフループ ポートになります。スパニング ツリーはこの状況を検出して、適宜に対応します。権利を獲得したスイッチ スタックでは PAgP または LACP 設定が変更されませんが、権利を獲得しなかったスイッチ スタックでは、スタックの再起動後に PAgP または LACP 設定が失われます。

PAgP を使用すると、スタック マスターが障害を起こすかスタックから脱退した場合、新しいスタック マスターが選択されます。EtherChannel の帯域幅が変更されないかぎり、スパニング ツリーの再コンバージェンスは発生しません。新しいスタック マスターにより、スタック メンバーの設定とスタック マスターの設定が同期されます。古いスタック マスター上にあるポートが EtherChannel に含まれる場合を除き、PAgP 設定はスタック マスターの変更による影響を受けません。

LACP を使用すると、システム ID ではスタック マスターからのスタック MAC アドレスが使用され、スタック マスターが変わると、LACP システム ID が変わることがあります。LACP システム ID が変わると、EtherChannel 全体がフラップし、STP 再コンバージェンスが発生します。マスターのフェールオーバー中にスタック MAC アドレスを変えるかどうかを制御するには、**stack-mac persistent timer** コマンドを使用します。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

EtherChannel の設定

ここでは、次の設定情報について説明します。

- 「EtherChannel のデフォルト設定」(P.37-12)
- 「EtherChannel 設定時の注意事項」(P.37-12)
- 「レイヤ 2 EtherChannel の設定」(P.37-14) (必須)
- 「レイヤ 3 EtherChannel の設定」(P.37-16) (必須)
- 「EtherChannel ロード バランシングの設定」(P.37-20) (任意)
- 「PAgP 学習方式およびプライオリティの設定」(P.37-21) (任意)
- 「LACP ホットスタンバイ ポートの設定」(P.37-23) (任意)



(注) 必ず、ポートを正しく設定してください。詳細については、「EtherChannel 設定時の注意事項」(P.37-12) を参照してください。



(注) EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

EtherChannel のデフォルト設定

表 37-3 に、EtherChannel のデフォルト設定を示します。

表 37-3 EtherChannel のデフォルト設定

機能	デフォルト設定
チャンネル グループ	割り当てなし
ポートチャンネル論理インターフェイス	未定義
PAgP モード	デフォルトなし
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768.
LACP システム ID	LACP システム プライオリティおよびスタック MAC アドレス
ロード バランシング	着信パケットの送信元 MAC アドレスに基づいてスイッチ上で負荷を分散

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を防ぐため、次の注意事項に従ってください。

- スイッチ スタック上では、48 を超える数の EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- LACP EtherChannel は、同じタイプのイーサネット ポートを最大 16 まで使用して設定します。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- クロススタック EtherChannel で最大 2 つの 10 ギガビット イーサネット モジュール ポートを設定します。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。shutdown インターフェイス コンフィギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの 1 つに転送されます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
 - 許可 VLAN リスト
 - 各 VLAN のスパニング ツリー パス コスト
 - 各 VLAN のスパニング ツリー ポート プライオリティ

- スパニング ツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバーになるように設定しないでください。
- 1 つの EtherChannel に PAgP モードと LACP モードの両方を設定しないでください。PAgP および LACP が稼動している複数の EtherChannel グループは、同じスイッチまたはスタック内の別のスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用はできません。
- EtherChannel の一部として Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 宛先ポートを設定しないでください。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- プライベート VLAN ポートを EtherChannel の一部として設定しないでください。
- EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにするポートを IEEE 802.1X ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。
- EtherChannel がスイッチ インターフェイス上に設定されている場合、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1X をスイッチ上でグローバルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除してください。
- レイヤ 2 EtherChannel の場合
 - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
 - トランク ポートから EtherChannel を設定する場合は、すべてのトランクでトランキング モード (ISL または IEEE 802.1Q) が同じであることを確認してください。EtherChannel ポートのトランクのモードが一致していないと、予想外の結果になる可能性があります。
 - EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
 - スパニング ツリー パス コストが異なるポートは、設定上の矛盾がないかぎり、EtherChannel を形成できます。異なるスパニング ツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。
- レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャンネル内の物理ポートでなく、ポートチャンネル論理インターフェイスに割り当ててください。
- クロススタック EtherChannel 設定の場合は、EtherChannel 用のすべてのポートが LACP 用に設定されているか、**channel-group channel-group-number mode on** インターフェイス コンフィギュレーション コマンドでチャンネル グループに含まれるように手動設定されているかを確認します。PAgP プロトコルは、クロススタック EtherChannel ではサポートされません。
- クロススタック EtherChannel が設定されていて、スイッチ スタックが分割されている場合、ループおよび転送が正しく動作しないことがあります。

レイヤ 2 EtherChannel の設定

レイヤ 2 EtherChannel を設定するには、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、チャンネル グループにポートを割り当てます。このコマンドにより、ポートチャンネル論理インターフェイスが自動的に作成されます。

auto モードか **desirable** モードのポートで PAgP をイネーブルにした場合は、**on** モードか LACP モードに再設定してから、このポートをクロススタック EtherChannel に追加する必要があります。PAgP では、クロススタック EtherChannel がサポートされません。

レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	<code>switchport mode {access trunk}</code> <code>switchport access vlan vlan-id</code>	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN だけに割り当ててください。指定できる範囲は 1 ~ 4094 です。

コマンド	目的
ステップ 4 channel-group <i>channel-group-number</i> mode { auto [non-silent] desirable [non-silent] on } { active passive }	<p>チャンネルグループにポートを割り当て、PAgP モードまたは LACP モードを指定します。</p> <p><i>channel-group-number</i> の範囲は 1 ~ 48 です。</p> <p>mode には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> auto : PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合、このキーワードはサポートされません。 desirable : PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合、このキーワードはサポートされません。 on : PAgP や LACP を使用せずにポートを強制的にチャンネル化します。on モードの場合、EtherChannel が存在するのは、on モードのポートグループが同じく on モードの別のポートグループに接続される場合だけです。 non-silent : (任意) PAgP 対応のデバイスに接続されたスイッチのポートが auto または desirable モードの場合に、非サイレント動作を行うようにこのポートを設定します。non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイルサーバまたはパケットアナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネルグループにポートを結合し、このポートが伝送に使用されず。 active : LACP デバイスが検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 passive : ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 <p>スイッチおよびデバイスのモードの互換性に関する情報については、「PAgP モード」(P.37-6) および「LACP モード」(P.37-8) を参照してください。</p>
ステップ 5 end	特権 EXEC モードに戻ります。

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

EtherChannel グループからポートを削除するには、**no channel-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが **desirable** であるチャンネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティック アクセス ポートとして、LACP モードが **active** であるチャンネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次に、クロススタック EtherChannel を設定する例を示します。この例では LACP パッシブ モードを使用し、スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートを、VLAN 10 のスタティック アクセス ポートとしてチャンネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode active
Switch(config-if)# exit
```

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel を設定するには、ポートチャンネル論理インターフェイスを作成し、そのポートチャンネルにイーサネット ポートを組み込みます。次に設定方法を説明します。

ポートチャンネル論理インターフェイスの作成

レイヤ 3 EtherChannel を設定する場合、まず **interface port-channel** グローバル コンフィギュレーション コマンドを使用し、ポートチャンネル論理インターフェイスを手動で作成しなければなりません。次に、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して論理インターフェイスをチャンネル グループに配置します。



(注) 物理ポートから EtherChannel に IP アドレスを移動するには、物理ポートから IP アドレスを削除してから、その IP アドレスをポートチャンネル インターフェイス上で設定する必要があります。

レイヤ 3 EtherChannel 用のポートチャンネル インターフェイスを作成するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface port-channel <i>port-channel-number</i>	ポートチャンネル論理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 <i>port-channel-number</i> の範囲は 1 ~ 48 です。
ステップ 3 no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 4 ip address <i>ip-address mask</i>	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show etherchannel <i>channel-group-number</i> detail	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 8	レイヤ 3 EtherChannel にイーサネット ポートを割り当てます。詳細については、「 物理インターフェイスの設定 (P.37-17) 」を参照してください。

ポートチャンネルを削除するには、**no interface port-channel *port-channel-number*** グローバル コンフィギュレーション コマンドを使用します。

次に、論理ポート チャンネル 5 を作成し、IP アドレスとして 172.10.20.10 を割り当てる例を示します。

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

物理インターフェイスの設定

レイヤ 3 EtherChannel にイーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i>	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスとして、物理ポートも含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 3	no ip address	この物理ポートに割り当てられている IP アドレスをすべて削除します。
ステップ 4	no switchport	ポートをレイヤ 3 モードにします。

コマンド	目的
ステップ 5 <code>channel-group channel-group-number mode {auto [non-silent] desirable [non-silent] on} {active passive}</code>	<p>チャンネル グループにポートを割り当て、PAgP モードまたは LACP モードを指定します。</p> <p><code>channel-group-number</code> の範囲は 1 ~ 48 です。この番号は、「ポートチャンネル論理インターフェイスの作成」(P.37-16) で設定した <code>port-channel-number</code> (論理ポート) と同一である必要があります。</p> <p>mode には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • auto : PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合、このキーワードはサポートされません。 • desirable : PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合、このキーワードはサポートされません。 • on : PAgP や LACP を使用せずにポートを強制的にチャンネル化します。on モードの場合、EtherChannel が存在するのは、on モードのポート グループが同じく on モードの別のポート グループに接続される場合だけです。 • non-silent : (任意) PAgP 対応のパートナーに接続されたスイッチのポートが auto または desirable モードの場合に、非サイレント動作を行うようにこのポートを設定します。non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネル グループにポートを結合し、このポートが伝送に使用されません。 • active : LACP デバイスが検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • passive : ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。 <p>スイッチおよびデバイスのモードの互換性に関する情報については、「PAgP モード」(P.37-6) および「LACP モード」(P.37-8) を参照してください。</p>
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

次に、EtherChannel を設定する例を示します。2 つのポートは、LACP モードが **active** であるチャンネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次に、クロススタック EtherChannel を設定する例を示します。スタック メンバー 2 の 2 つのポートとスタック メンバー 3 の 1 つのポートは、LACP アクティブ モードでチャンネル 7 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 7 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# no ip address
Switch(config-if)# no switchport
Switch(config-if)# channel-group 7 mode active
Switch(config-if)# exit
```

EtherChannel ロード バランシングの設定

ここでは、送信元ベースまたは宛先ベースの転送方式を使用することによって、EtherChannel のロード バランシングを設定する手順について説明します。詳細については、「[ロード バランシングおよび転送方式](#)」(P.37-9) を参照してください。

EtherChannel のロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>port-channel load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}</code>	EtherChannel のロード バランシング方式を設定します。 デフォルトは src-mac です。 次のいずれかの負荷分散方式を選択します。 <ul style="list-style-type: none"> • dst-ip : 宛先ホスト IP アドレスに基づいて負荷を分散します。 • dst-mac : 着信パケットの宛先ホスト MAC アドレスに基づいて負荷を分散します。 • src-dst-ip : 送信元および宛先ホスト IP アドレスに基づいて負荷を分散します。 • src-dst-mac : 送信元および宛先ホスト MAC アドレスに基づいて負荷を分散します。 • src-ip : 送信元ホスト IP アドレスに基づいて負荷を分散します。 • src-mac : 着信パケットの送信元 MAC アドレスに基づいて負荷を分散します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show etherchannel load-balance</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel のロード バランシングをデフォルトの設定に戻す場合は、**no port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

PAgP 学習方式およびプライオリティの設定

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式はリンクの両端で同じ方式に設定する必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャンネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカル デバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要があります。

グループ内の 1 つのポートですべての伝送を行うように設定して、他のポートをホットスタンバイに使用することもできます。選択された 1 つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるように、ポートを設定するには、**pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。



(注)

CLI (コマンドライン インターフェイス) で **physical-port** キーワードを指定した場合でも、スイッチがサポートするのは、集約ポート上でのアドレス ラーニングだけです。**pagp learn-method** コマンドおよび **pagp port-priority** コマンドはスイッチ ハードウェアに影響を与えませんが、物理ポートによるアドレス学習だけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

スイッチのリンクの相手側が物理ラーナー (Catalyst 1900 シリーズ スイッチなど) の場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して、Catalyst 3750 スイッチを物理ポート ラーナーとして設定することを推奨します。送信元 MAC アドレスに基づいて負荷の分散方式を設定するには、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用します。このように設定すると、送信元アドレスの学習元である EtherChannel 内の同じポートを使用して、パケットが Catalyst 1900 スイッチに送信されます。**pagp learn-method** コマンドは、このような場合に限りて使用してください。

スイッチを PAgP 物理ポート ラーナーとして設定し、バンドル内の同じポートがパケット送信用として選択されるようにプライオリティを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	pagp learn-method physical-port	PAgP 学習方式を選択します。 デフォルトでは、 aggregation-port learning が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、パケットが送信元に送信されます。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届くかは重要ではありません。 物理ラーナーである別のスイッチに接続するには、 physical-port を選択します。 port-channel load-balance グローバル コンフィギュレーション コマンドは、必ず src-mac に設定してください (「EtherChannel ロード バランシングの設定」(P.37-20) を参照)。 学習方式はリンクの両端で同じ方式に設定する必要があります。
ステップ 4	pagp port-priority priority	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 <i>priority</i> の範囲は、0 ~ 255 です。デフォルト値は 128 です。プライオリティが高いほど、そのポートが PAgP 送信用に選択される可能性が高まります。
ステップ 5	end	特権 EXEC モードに戻ります。

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

プライオリティをデフォルト設定に戻すには、**no pagp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。学習方式をデフォルト設定に戻すには、**no pagp learn-method** インターフェイス コンフィギュレーション コマンドを使用します。

LACP ホットスタンバイ ポートの設定

イネーブルの場合、LACP はチャンネル内の LACP 互換ポート数を最大に設定しようとします (最大 16 ポート)。同時にアクティブになれる LACP リンクは 8 つだけです。リンクが追加されるとソフトウェアによってホットスタンバイ モードになります。アクティブ リンクの 1 つが非アクティブになると、ホットスタンバイ モードのリンクが代わりにアクティブになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホットスタンバイ ポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、以下の要素 (プライオリティ順) で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID (スイッチの MAC アドレス)
- LACP ポート プライオリティ
- ポート番号

プライオリティを比較する場合、数値的により低い方が高いプライオリティを持っています。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイ モードにするポートを決定します。

アクティブ ポートかホットスタンバイ ポートかを判別するには、次の (2 つの) 手順を使用します。はじめに、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートとホットスタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。詳細については、「[LACP システム プライオリティの設定](#)」(P.37-23) および「[LACP ポート プライオリティの設定](#)」(P.37-24) を参照してください。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して LACP をイネーブルにしているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済みの各チャンネルに対しては、システム プライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホットスタンバイ モードのポートを確認できます (ポートステート フラグが H になっています)。

LACP システム プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>lACP system-priority priority</code>	LACP システム プライオリティを設定します。 <i>priority</i> の範囲は、1 ~ 65535 です。デフォルト値は 32768 です。 値が小さいほど、システム プライオリティは高くなります。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code> または <code>show lACP sys-id</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

LACP システム プライオリティをデフォルトの値に戻すには、`no lACP system-priority` グローバル コンフィギュレーション コマンドを使用します。

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイ リンクを変更できます。ホットスタンバイ ポートは、番号が小さい方が先にチャンネルでアクティブになります。ホットスタンバイ モードのポートを確認するには、`show etherchannel summary` 特権 EXEC コマンドを使用します (ホットスタンバイ モードのポートには *H* ポートステート フラグが付加されます)。



(注)

LACP がすべての互換ポートを集約できない場合 (たとえば、ハードウェアの制約が大きいリモート システム)、EtherChannel 中でアクティブにならないポートはすべてホットスタンバイ ステートになり、チャンネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>lACP port-priority priority</code>	LACP ポート プライオリティを設定します。 <i>priority</i> の範囲は、1 ~ 65535 です。デフォルト値は 32768 です。プライオリティが低いほど、そのポートが LACP 送信用に選択される可能性が高まります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 5 show running-config または show lacp [<i>channel-group-number</i>] internal	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LACP ポート プライオリティをデフォルト値に戻すには、**no lacp port-priority** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel、PAgP、および LACP ステータスの表示

表 37-4 EtherChannel、PAgP、および LACP ステータスを表示するためのコマンド

コマンド	説明
show etherchannel [<i>channel-group-number</i> { detail port port-channel protocol summary }] { detail load-balance port port-channel protocol summary }	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロード バランシング方式またはフレーム配布方式、ポート、ポートチャンネル、プロトコルの情報も表示されます。
show pagp [<i>channel-group-number</i>] { counters internal neighbor }	トラフィック情報、内部 PAgP 設定、近接情報などの PAgP 情報が表示されます。
show pagp [<i>channel-group-number</i>] dual-active	デュアルアクティブ検出ステータスを表示します。
show lacp [<i>channel-group-number</i>] { counters internal neighbor }	トラフィック情報、内部 LACP 設定、近接情報などの LACP 情報が表示されます。

PAgP チャンネルグループ情報およびトラフィック カウンタをクリアするには、**clear pagp** [*channel-group-number* **counters** | **counters**] 特権 EXEC コマンドを使用します。

LACP チャンネルグループ情報およびトラフィック カウンタをクリアするには、**clear lacp** [*channel-group-number* **counters** | **counters**] 特権 EXEC コマンドを使用します。

出力内の各フィールドについては、このリリースのコマンド リファレンスを参照してください。

リンクステート トラッキングの概要

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスのリンクステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ NIC アダプタ チューニング機能とともに使用すると、ネットワークで冗長性が実現されます。サーバ ネットワーク アダプタが、チューニングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ インターフェイスでリンクが消失した場合、接続はセカンダリ インターフェイスに透過的に変更されます。



(注) ポートの集合 (EtherChannel)、アクセス モードまたはトランク モードの単一の物理ポート、またはルーテッド ポートをインターフェイスに指定できます。

図 37-6 (P.37-28) は、リンクステート トラッキングを使用して設定されたネットワークを示しています。リンクステート トラッキングをイネーブルにするには、リンクステート グループを作成して、リンクステート グループに割り当てられるインターフェイスを指定します。リンクステート グループでは、これらのインターフェイスは互いにバンドルされています。ダウンストリーム インターフェイスは、アップストリーム インターフェイスにバインドされています。サーバに接続されているインターフェイスは、ダウンストリーム インターフェイスと呼ばれ、ディストリビューション スイッチやネットワーク デバイスに接続されているインターフェイスはアップストリーム インターフェイスと呼ばれます。

図 37-6 の設定により、ネットワーク トラフィック フローが次のようにバランスが保たれます。

- スイッチと他のネットワーク デバイスへのリンクの場合
 - サーバ 1 とサーバ 2 は、プライマリ リンクにスイッチ A を使用し、セカンダリ リンクにスイッチ B を使用しています。
 - サーバ 3 とサーバ 4 は、プライマリ リンクにスイッチ B を使用し、セカンダリ リンクにスイッチ A を使用しています。
- スイッチ A のリンクステート グループ 1
 - スイッチ A は、リンクステート グループ 1 を介してサーバ 1 とサーバ 2 にプライマリ リンクを提供します。ポート 1 はサーバ 1 に接続され、ポート 2 はサーバ 2 に接続されます。ポート 1 およびポート 2 は、リンクステート グループ 1 のダウンストリーム インターフェイスです。
 - ポート 5 およびポート 6 は、リンクステート グループ 1 を介してディストリビューション スイッチ 1 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 1 のアップストリーム インターフェイスです。
- スイッチ A のリンクステート グループ 2
 - スイッチ A は、リンクステート グループ 2 を介してサーバ 3 とサーバ 4 にセカンダリ リンクを提供します。ポート 3 はサーバ 3 に接続され、ポート 4 はサーバ 4 に接続されます。ポート 3 およびポート 4 は、リンクステート グループ 2 のダウンストリーム インターフェイスです。
 - ポート 7 とポート 8 は、リンクステート グループ 2 を介してディストリビューション スイッチ 2 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 2 のアップストリーム インターフェイスです。
- スイッチ B のリンクステート グループ 2
 - スイッチ B は、リンクステート グループ 2 を介してサーバ 3 とサーバ 4 にプライマリ リンクを提供します。ポート 3 はサーバ 3 に接続され、ポート 4 はサーバ 4 に接続されます。ポート 3 およびポート 4 は、リンクステート グループ 2 のダウンストリーム インターフェイスです。
 - ポート 5 とポート 6 は、リンクステート グループ 2 を介してディストリビューション スイッチ 2 に接続されます。ポート 5 およびポート 6 は、リンクステート グループ 2 のアップストリーム インターフェイスです。
- スイッチ B のリンクステート グループ 1
 - スイッチ B は、リンクステート グループ 1 を介してサーバ 1 とサーバ 2 にセカンダリ リンクを提供します。ポート 1 はサーバ 1 に接続され、ポート 2 はサーバ 2 に接続されます。ポート 1 およびポート 2 は、リンクステート グループ 1 のダウンストリーム インターフェイスです。
 - ポート 7 およびポート 8 は、リンクステート グループ 1 を介してディストリビューション スイッチ 1 に接続されます。ポート 7 およびポート 8 は、リンクステート グループ 1 のアップストリーム インターフェイスです。

ディストリビューション スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リンクステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。これらは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアップストリーム インターフェイス間の相互作用です。

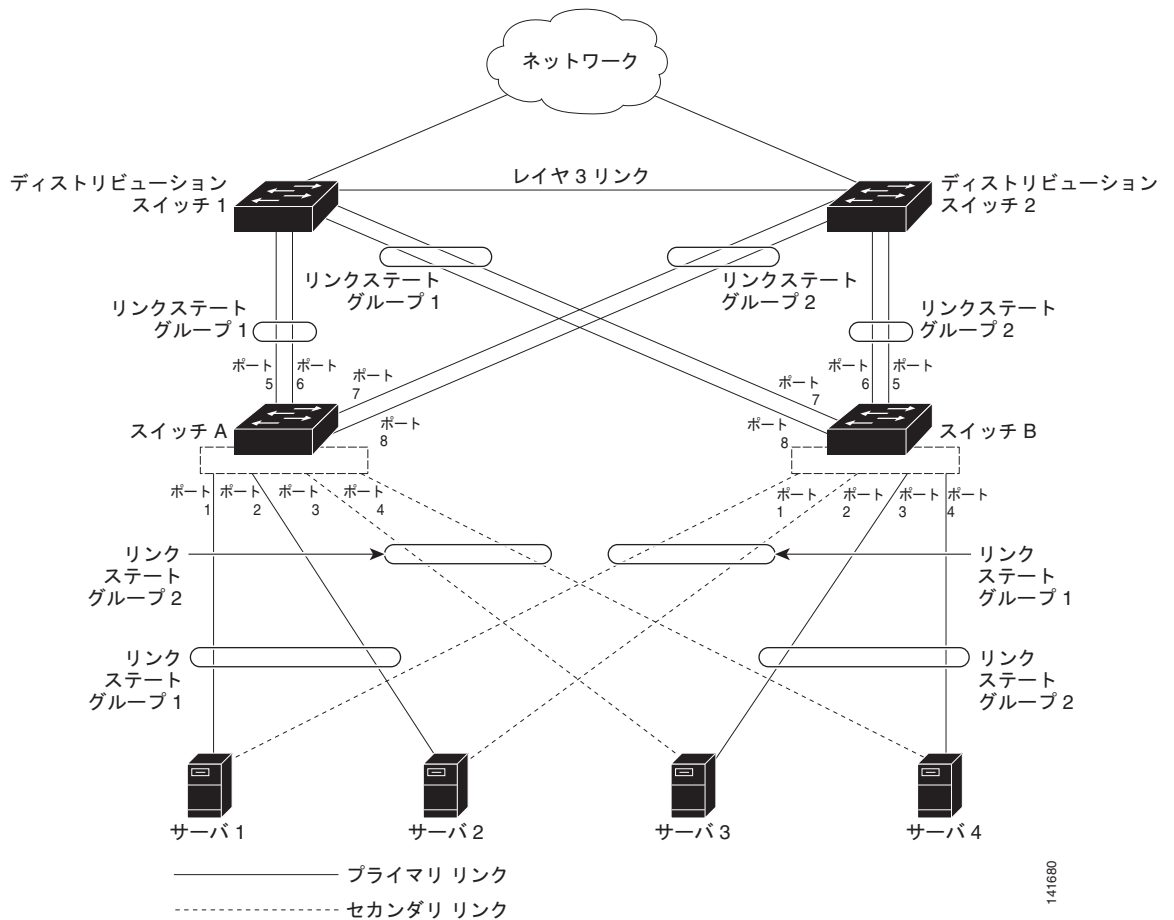
- アップストリーム インターフェイスがリンクアップ ステートの場合、ダウンストリーム インターフェイスをリンクアップ ステートに変更したり、リンクアップ ステートのままにしたりすることができます。
- すべてのアップストリーム インターフェイスが利用不能になった場合、リンクステート トラッキングが自動的にダウンストリーム インターフェイスを **errdisable** ステートにします。サーバ間の接続は、自動的にプライマリ サーバ インターフェイスからセカンダリ サーバ インターフェイスに変更されます。

スイッチ A のリンクステート グループ 1 からリンクステート グループ 2 への接続の変更例については、[図 37-6 \(P.37-28\)](#) を参照してください。ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンクダウン ステートに変更されます。また、サーバ 1 およびサーバ 2 の接続はリンクステート グループ 1 からリンクステート グループ 2 に変更されます。ダウンストリーム ポート 3 および 4 は、リンクグループ 2 にあるため変更されません。

- リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ステートは変更されないままになります。サーバはこのアップストリーム接続が切断されたことを認識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。複数のダウンストリーム インターフェイスを復旧させるには、リンクステート グループをディセーブルにします。

図 37-6 一般的なリンクステートトラッキングの設定



リンクステートトラッキングの設定

- 「デフォルトのリンクステートトラッキングの設定」 (P.37-28)
- 「リンクステートトラッキングの設定時の注意事項」 (P.37-29)
- 「リンクステートトラッキングの設定」 (P.37-29)
- 「リンクステートトラッキングステータスの表示」 (P.37-30)

デフォルトのリンクステートトラッキングの設定

リンクステートグループは定義されておらず、リンクステートトラッキングはどのグループでもイネーブルではありません。

リンクステート トラッキングの設定時の注意事項

設定上の問題を防ぐため、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスは、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義できません。その逆も同様です。
- 1 つのインターフェイスが、複数のリンクステート グループのメンバーになることはできません。
- スイッチ 1 つにつき設定できるリンクステート グループは 10 だけです。

リンクステート トラッキングの設定

リンクステート グループを設定し、そのグループにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>link state track number</code>	リンクステート グループを作成して、リンクステート トラッキングをイネーブルにします。グループ番号は 1 ~ 10 に設定できます。デフォルトは 1 です。
ステップ 3	<code>interface interface-id</code>	物理インターフェイスまたはインターフェイスの範囲を設定して、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、アクセス モードまたはトランク モード (IEEE 802.1q) のスイッチ ポート、ルーテッド ポート、EtherChannel インターフェイス (スタティックまたは LACP) にバンドルされた、トランク モードの複数ポートが含まれます。
ステップ 4	<code>link state group [number] {upstream downstream}</code>	リンクステート グループを指定し、グループ内のインターフェイスを upstream または downstream インターフェイスに設定します。グループ番号は 1 ~ 10 に設定できます。デフォルトは 1 です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、リンクステート グループを作成してインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range gigabitethernet1/0/21 -22
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet1/0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

リンクステート グループをディセーブルにするには、**no link state track number** グローバル コンフィギュレーション コマンドを使用します。

リンクステート トラッキング ステータスの表示

show link state group コマンドを使用してリンクステート グループの情報を表示します。すべてのリンクステート グループの情報を表示するには、このコマンドをキーワードなしで入力します。特定のグループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、**detail** キーワードを入力します。

次に、**show link stage group 1** コマンドの出力例を示します。

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

次に、**show link stage group detail** コマンドの出力例を示します。

```
Switch> show link state group detail

(Up):Interface up      (Dwn):Interface Down  (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn) Gi1/0/17(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER 38

IP ユニキャスト ルーティングの設定

この章では、Catalyst 3750 スイッチに Internet Protocol Version 4 (IPv4) ユニキャスト ルーティングを設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチ スタックを意味します。スイッチ スタックは、ネットワーク内のそれ以外のルータに対して、単一のルータとして動作し、認識されます。スタティック ルーティングおよび Routing Information Protocol (RIP) などの基本的なルーティング機能は、IP ベース イメージと IP サービス イメージの両方で使用できます。先進のルーティング機能およびその他のルーティングプロトコルを使用するには、スタンドアロンスイッチやスタック マスターに IP サービス イメージをインストールする必要があります。



(注)

スイッチ スタックが拡張 IP サービス イメージを実行している場合、IP バージョン 6 (IPv6) ユニキャスト ルーティングもイネーブルにして IPv4 トラフィックに加えて IPv6 トラフィックを転送するようにインターフェイスを設定できます。スイッチに IPv6 を設定する手順については、第 39 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

IP ユニキャスト設定情報に関する詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。このセクションで使用するコマンドの構文および使用方法の詳細については、それぞれのコマンドリファレンスを参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』 Release 12.2
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』 Release 12.2

この章で説明する内容は、次のとおりです。

- 「IP ルーティングの概要」 (P.38-2)
- 「ルーティングを設定する手順」 (P.38-5)
- 「IP アドレス指定の設定」 (P.38-6)
- 「IP ユニキャスト ルーティングのイネーブル化」 (P.38-20)
- 「RIP の設定」 (P.38-21)
- 「OSPF の設定」 (P.38-27)
- 「EIGRP の設定」 (P.38-38)
- 「BGP の設定」 (P.38-47)
- 「ISO CLNS ルーティングの設定」 (P.38-69)

- 「マルチ VRF CE の設定」(P.38-80)
- 「プロトコル独立機能の設定」(P.38-95)
- 「IP ネットワークのモニタおよびメンテナンス」(P.38-111)



(注)

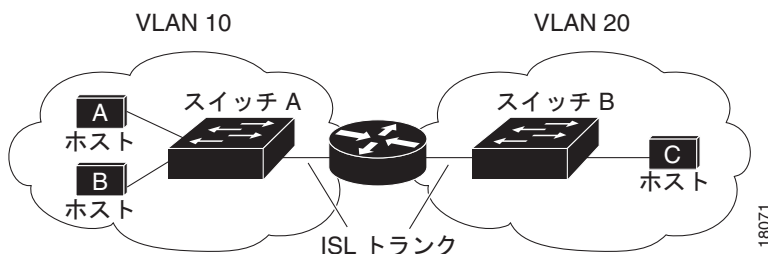
スイッチにルーティングパラメータを設定する場合、使用できるユニキャストルート数が最大となるようにシステムリソースを割り当てるには、**sdm prefer routing** グローバルコンフィギュレーションコマンドを使用し、ルーティングテンプレートに Switch Database Management (SDM; スイッチデータベース管理) 機能を設定します。SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」、またはこのリリースのコマンドリファレンスの **sdm prefer** コマンドを参照してください。

IP ルーティングの概要

一部のネットワーク環境で、VLAN (仮想 LAN) は各ネットワークまたはサブネットワークに関連付けられています。IP ネットワークで、各サブネットワークは 1 つの VLAN に対応しています。VLAN を設定すると、ブロードキャストドメインのサイズを制御し、ローカルトラフィックをローカル内にとどめることができます。ただし、異なる VLAN 内のネットワークデバイスが相互に通信するには、VLAN 間でトラフィックをルーティング (VLAN 間ルーティング) するレイヤ 3 デバイス (ルータ) が必要です。VLAN 間ルーティングでは、適切な宛先 VLAN にトラフィックをルーティングするため、1 つまたは複数のルータを設定します。

図 38-1 に基本的なルーティングトポロジを示します。スイッチ A は VLAN 10 内、スイッチ B は VLAN 20 内にあります。ルータには各 VLAN のインターフェイスが備わっています。

図 38-1 ルーティングトポロジの例



VLAN 10 内のホスト A が VLAN 10 内のホスト B と通信する場合、ホスト A はホスト B 宛にアドレス指定されたパケットを送信します。スイッチ A はパケットをルータに送信せず、ホスト B に直接転送します。

ホスト A から VLAN 20 内のホスト C にパケットを送信する場合、スイッチ A はパケットをルータに転送し、ルータは VLAN 10 インターフェイスでトラフィックを受信します。ルータはルーティングテーブルを調べて正しい発信インターフェイスを判別し、VLAN 20 インターフェイスを経由してパケットをスイッチ B に送信します。スイッチ B はパケットを受信し、ホスト C に転送します。

ここでは、ルーティングに関する次の内容について説明します。

- 「ルーティングタイプ」(P.38-3)
- 「IP ルーティングおよびスイッチスタック」(P.38-3)

ルーティング タイプ

ルータおよびレイヤ 3 スイッチは、次の 3 つの方法でパケットをルーティングできます。

- デフォルト ルーティング
- 事前にプログラミングされているトラフィックのスタティック ルートの使用
- ルーティング プロトコルによるルートの動的な計算

デフォルト ルーティングとは、宛先がルータにとって不明であるトラフィックをデフォルトの出口または宛先に送信することです。

スタティック ユニキャスト ルーティングの場合、パケットは事前に設定されたポートから単一のパスを通り、ネットワークの内部または外部に転送されます。スタティック ルーティングは安全で、帯域幅をほとんど使用しません。ただし、リンク障害などのネットワークの変更には自動的に対応しないため、パケットが宛先に到達しないことがあります。ネットワークが拡大するにつれ、スタティック ルーティングの設定は煩雑になります。

ルータでは、トラフィックを転送する最適ルートを動的に計算するため、ダイナミック ルーティング プロトコルが使用されます。ダイナミック ルーティング プロトコルには次の 2 つのタイプがあります。

- ディスタンス ベクタ プロトコルを使用するルータでは、ネットワーク リソースの距離の値を使用してルーティング テーブルを保持し、これらのテーブルをネイバーに定期的に渡します。ディスタンス ベクタ プロトコルは 1 つまたは複数のメトリックを使用し、最適なルートを計算します。これらのプロトコルは、簡単に設定、使用できます。
- リンク ステート プロトコルを使用するルータでは、ルータ間の Link-State Advertisement (LSA; リンクステート アドバタイズメント) の交換に基づき、ネットワーク トポロジに関する複雑なデータベースを保持します。LSA はネットワークのイベントによって起動され、コンバージェンス時間、またはこれらの変更への対応時間を短縮します。リンクステート プロトコルはトポロジの変更にはすばやく対応しますが、ディスタンス ベクタ プロトコルよりも多くの帯域幅およびリソースが必要になります。

スイッチでサポートされているディスタンス ベクタ プロトコルは、RIP および Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) です。RIP は最適パスを決定するために単一の距離メトリック (コスト) を使用し、BGP はパス ベクタ メカニズムを追加します。また、Open Shortest Path First (OSPF) リンクステート プロトコル、および従来の Interior Gateway Routing Protocol (IGRP) にリンクステート ルーティング機能の一部を追加して効率化を図った Enhanced IGRP (EIGRP) もサポートされています。



(注)

スイッチ スタックでサポートされるプロトコルは、スタック マスター上で稼動しているソフトウェアによって決まります。スタック マスター上で IP ベース イメージが稼動している場合は、デフォルトのルーティング、スタティック ルーティング、および RIP だけがサポートされます。その他のすべてのルーティング プロトコルには、IP サービス イメージが必要です。

IP ルーティングおよびスイッチ スタック

スタック内のどのスイッチがルーティング ピアに接続されているかに関係なく、ネットワークは Catalyst 3750 スイッチ スタックを単一ルータとして認識します。スイッチ スタックの動作の詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

スタック マスターは、次に示す機能を実行します。

- ルーティング プロトコルを初期化し、設定します。
- ルーティング プロトコル メッセージおよびアップデートを他のルータに送信します。

- ピア ルータから受信したルーティング プロトコル メッセージおよびアップデートを処理します。
- **distributed Cisco Express Forwarding (dCEF)** データベースを生成および維持し、すべてのスタック メンバーに配信します。このデータベースに基づいて、スタック内のすべてのスイッチにルートがプログラムされます。
- スタック マスターの **MAC (メディア アクセス制御)** アドレスはスタック全体のルータ **MAC** アドレスとして使用され、すべての外部デバイスはこのアドレスを使用して **IP** パケットをスタックに送信します。
- ソフトウェア転送またはソフトウェア処理を必要とするすべての **IP** パケットは、スタック マスターの **CPU** を通ります。

スタック メンバーは、次に示す機能を実行します。

- ルーティング スタンバイ スイッチとして機能します。スタック マスターに障害が発生し、新規スタック マスターとして選択された場合に、処理を引き継ぐことができます。
- ルートをハードウェアにプログラムします。スタック メンバーによってプログラムされたルートは、**dCEF** データベースの一部としてスタック マスターがダウンロードしたルートと同じです。

スタック マスターに障害が発生すると、スタックはスタック マスターがダウンしていることを検出し、スタック メンバーの 1 つを新規スタック マスターとして選択します。この期間中に、ハードウェアは一時的な中断を除き、アクティブなプロトコルがない状態で、パケットの転送を継続します。

ただし、スイッチ スタックで障害発生後にハードウェア **ID** を保持していても、スタック マスターがリスタートする前の短時間の中断中に、ルータ ネイバーのルーティング プロトコルがフラップすることもあります。**OSPF** や **EIGRP** などのルーティング プロトコルは、ネイバー トランジションを認識する必要があります。ルータでは、2 つのレベルの **Nonstop Forwarding (NSF)** を使用してスイッチオーバーを検出し、ネットワーク トラフィックの転送を継続し、ピア デバイスからのルート情報を回復しています。

- **NSF** 認識ルータは、近接ルータの障害を許容しています。近接ルータが再起動したあとに、**NSF** 認識ルータが要求に応じてステートとルートの隣接関係に関する情報を提供します。
- **NSF** 対応ルータは **NSF** をサポートします。スタック マスターの変更を検出すると、**NSF** 認識ネイバーまたは **NSF** 対応ネイバーからルーティング情報を再構築し、再起動まで待機しません。

スイッチ スタックは **OSPF** および **EIGRP** の **NSF** 対応ルーティングをサポートしています。詳細については、「**OSPF NSF 機能**」(P.38-30) および「**EIGRP NSF 機能**」(P.38-42) を参照してください。

新規スタック マスターは、選択されたときに次の機能を実行します。

- ルーティング アップデートの生成、受信、および処理を開始します。
- ルーティング テーブルを構築し、**CEF** データベースを生成して、スタック メンバーに配信します。
- ルータ **MAC** アドレスとして自身の **MAC** アドレスを使用します。新規 **MAC** アドレスのネットワーク ピアを通知するために、新規ルータ **MAC** アドレスを使用して **Gratuitous Address Resolution Protocol (ARP)** 応答を定期的に (5 分間、数秒おきに) 送信します。



(注) 固定 **MAC** アドレス機能をスタックに設定してスタック マスターを変更した場合、スタック **MAC** アドレスは設定された期間変更されません。この期間に前のスタック マスターがメンバー スイッチとしてスタックに復帰する場合、スタック **MAC** アドレスは前のスタック マスターの **MAC** アドレスのままになります。「**固定 MAC アドレスのイネーブル化**」(P.5-19) を参照してください。

- ARP 要求をプロキシ ARP IP アドレスに送信し、ARP 応答を受信して、各プロキシ ARP エントリの到達可能性を判別しようとします。到達可能なプロキシ ARP IP アドレスごとに、新規ルータ MAC アドレスを使用して Gratuitous ARP 応答を生成します。このプロセスは、新規スタック マスターが選択されたあと、5 分間繰り返されます。



(注)

スタック マスターで IP サービス イメージが稼働中の場合、スタックは OSPF、EIGRP、BGP などのすべてのサポートするプロトコルを実行することができます。スタック マスターに障害が発生し、新規に選択されたスタック マスター上で IP ベース イメージが稼働している場合、これらのプロトコルはスタック内で稼働しなくなります。



注意

スイッチ スタックを複数のスタックに分割すると、ネットワークが適切に動作しなくなる場合があります。

ルーティングを設定する手順

スイッチ上で、IP ルーティングはデフォルトでディセーブルとなっています。ルーティングを行う前に、IP ルーティングをイネーブルにする必要があります。IP ルーティング設定情報に関する詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

次の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。

- ルーテッド ポート : **no switchport** インターフェイス コンフィギュレーション コマンドを使用し、レイヤ 3 ポートとして設定された物理ポートです。
- Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) : **interface vlan vlan_id** グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
- レイヤ 3 モードの EtherChannel ポート チャネル : **interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャネルグループにバインドして作成されたポートチャネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」(P.37-16) を参照してください。



(注)

スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。

ルーティングが発生するすべてのレイヤ 3 インターフェイスに、IP アドレスを割り当てる必要があります。「ネットワーク インターフェイスへの IP アドレスの割り当て」(P.38-7) を参照してください。



(注)

レイヤ 3 スイッチでは、ルーテッド ポートおよび SVI ごとに IP アドレスを 1 つ割り当てることができます。ソフトウェアに、設定できるルーテッド ポートおよび SVI の個数制限はありません。ただし、ハードウェアによって制限されるため、設定できるルーテッド ポートおよび SVI の個数と、実装されている機能の組み合わせによっては、CPU 利用率が影響を受けることがあります。システム メモリをルーティング用に最適化するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用します。

ルーティングを設定するための主な手順は次のとおりです。

- VLAN インターフェイスをサポートするために、スイッチ スタックで VLAN を作成および設定し、レイヤ 2 インターフェイスに VLAN メンバシップを割り当てます。詳細は、第 14 章「VLAN の設定」を参照してください。
- レイヤ 3 インターフェイスを設定します。
- スイッチ上で IP ルーティングをイネーブルにします。
- レイヤ 3 インターフェイスに IP アドレスを割り当てます。
- 選択したルーティング プロトコルをスイッチ上でイネーブルにします。
- ルーティング プロトコル パラメータを設定します (任意)。

IP アドレス指定の設定

IP ルーティングを設定するには、レイヤ 3 ネットワーク インターフェイスに IP アドレスを割り当ててインターフェイスをイネーブルにし、IP を使用するインターフェイスを経由してホストとの通信を許可する必要があります。ここでは、さまざまな IP アドレス機能の設定方法について説明します。IP アドレスをインターフェイスに割り当てる手順は必須ですが、その他の手順は任意です。

- 「アドレス指定のデフォルト設定」(P.38-6)
- 「ネットワーク インターフェイスへの IP アドレスの割り当て」(P.38-7)
- 「アドレス解決方法の設定」(P.38-10)
- 「IP ルーティングがディセーブルの場合のルーティング支援機能」(P.38-13)
- 「ブロードキャスト パケットの処理方法の設定」(P.38-15)
- 「IP アドレスのモニタおよびメンテナンス」(P.38-20)

アドレス指定のデフォルト設定

表 38-1 に、アドレス指定のデフォルト設定を示します。

表 38-1 アドレス指定のデフォルト設定

機能	デフォルト設定
IP アドレス	未定義。
ARP	Address Resolution Protocol (ARP; アドレス解決プロトコル) キャッシュに永続的なエントリはありません。 カプセル化: 標準イーサネット形式の ARP。 タイムアウト: 14400 秒 (4 時間)。
IP ブロードキャスト アドレス	255.255.255.255 (すべて 1)。
IP クラスレス ルーティング	イネーブル。
IP デフォルト ゲートウェイ	ディセーブル。
IP 指定ブロードキャスト	ディセーブル (すべての IP 指定ブロードキャストが廃棄されます)。

表 38-1 アドレス指定のデフォルト設定 (続き)

機能	デフォルト設定
IP ドメイン	ドメイン リスト：ドメイン名は未定義。 ドメイン検索：イネーブル。 ドメイン名：イネーブル。
IP 転送プロトコル	ヘルパー アドレスが定義されているか、または UDP フラッドイングが設定されている場合、デフォルト ポートでは UDP 転送がイネーブルとなります。 ローカル ブロードキャスト：ディセーブル。 Spanning-Tree Protocol (STP; スパニング ツリー プロトコル)：ディセーブル。 ターボフラッドイング：ディセーブル。
IP ヘルパー アドレス	ディセーブル。
IP ホスト	ディセーブル。
ICMP Router Discovery Protocol (IRDP)	ディセーブル。 イネーブルの場合のデフォルト： <ul style="list-style-type: none"> ブロードキャスト IRDP アドバタイズメント。 アドバタイズメント間の最大インターバル：600 秒。 アドバタイズメント間の最小インターバル：最大インターバルの 0.75 倍。 初期設定：0。
IP プロキシ ARP	イネーブル。
IP ルーティング	ディセーブル。
IP サブネットゼロ	ディセーブル。

ネットワーク インターフェイスへの IP アドレスの割り当て

IP アドレスは IP パケットの送信先を特定します。一部の IP アドレスは特殊な目的のために予約されていて、ホスト、サブネット、またはネットワーク アドレスには使用できません。RFC 1166 「Internet Numbers」には IP アドレスに関する公式の説明が記載されています。

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。マスクは、IP アドレスのネットワーク番号を表すビットを特定します。マスクを使用してネットワークをサブネット化する場合、そのマスクをサブネット マスクと呼びます。割り当てられているネットワーク番号については、インターネット サービス プロバイダーにお問い合わせください。

IP アドレスおよびネットワーク マスクをレイヤ 3 インターフェイスに割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。

	コマンド	目的
ステップ 3	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。
ステップ 4	ip address ip-address subnet-mask	IP アドレスおよび IP サブネット マスクを設定します。
ステップ 5	no shutdown	インターフェイスをイネーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [interface-id] show ip interface [interface-id] show running-config interface [interface-id]	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

サブネット ゼロの使用

サブネット アドレスがゼロであるサブネットを作成しないでください。同じアドレスを持つネットワークおよびサブネットがある場合に問題が発生することがあります。たとえば、ネットワーク 131.108.0.0 のサブネットが 255.255.255.0 の場合、サブネット ゼロは 131.108.0.0 と記述され、ネットワーク アドレスと同じとなります。

すべてが 1 のサブネット (131.108.255.0) は使用可能です。また、IP アドレス用にサブネット スペース全体が必要な場合は、サブネット ゼロの使用をイネーブルにできます (ただし推奨できません)。

サブネット ゼロをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip subnet-zero	インターフェイス アドレスおよびルーティングの更新時にサブネット ゼロの使用をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して、サブネット ゼロの使用をディセーブルにするには、**no ip subnet-zero** グローバル コンフィギュレーション コマンドを使用します。

クラスレス ルーティング

ルーティングを行うように設定されたスイッチで、クラスレス ルーティング動作はデフォルトでイネーブルとなっています。クラスレス ルーティングがイネーブルの場合、デフォルト ルートがないネットワークのサブネット宛パケットをルータが受信すると、ルータは最適なスーパーネット ルートにパケットを転送します。スーパーネットは、単一の大規模アドレス スペースをシミュレーションするために使用されるクラス C アドレス スペースの連続ブロックで構成されています。スーパーネットは、クラス B アドレス スペースの急速な枯渇を回避するために設計されました。

図 38-2 では、クラスレス ルーティングがイネーブルになっています。ホストがパケットを 128.20.4.1 に送信すると、ルータはパケットを廃棄せずに、最適なスーパーネット ルートに転送します。クラスレス ルーティングがディセーブルの場合、デフォルト ルートがないネットワークのサブネット宛パケットを受信したルータは、パケットを廃棄します。

図 38-2 IP クラスレス ルーティングがイネーブルの場合

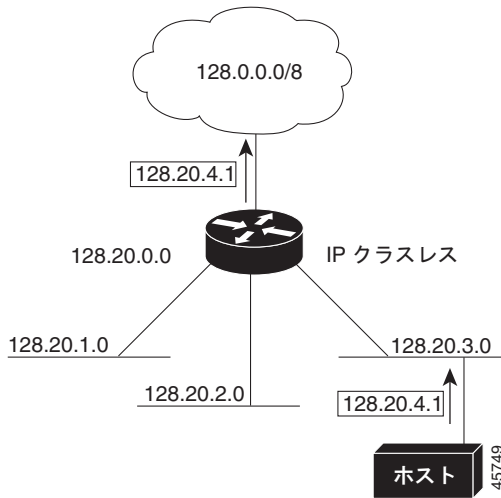
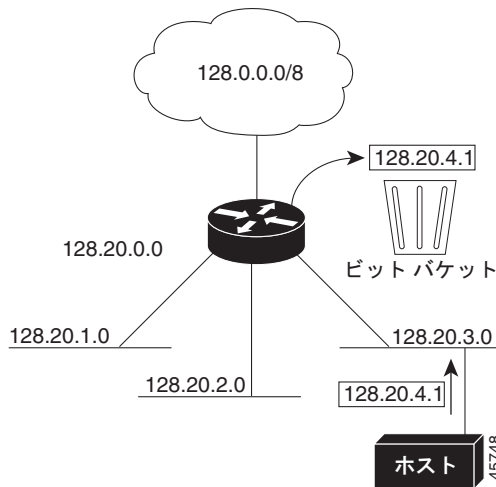


図 38-3 では、ネットワーク 128.20.0.0 のルータはサブネットワーク 128.20.1.0、128.20.2.0、128.20.3.0 に接続されています。ホストがパケットを 128.20.4.1 に送信した場合、ネットワークのデフォルト ルートが存在しないため、ルータはパケットを廃棄します。

図 38-3 IP クラスレス ルーティングがディセーブルの場合



認識されないサブネットワーク宛のパケットが最適なスーパーネットワーク ルートに転送されないようにするには、クラスレス ルーティング動作をディセーブルにします。

クラスレス ルーティングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>no ip classless</code>	クラスレス ルーティング動作をディセーブルにします。
ステップ 3 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4 <code>show running-config</code>	設定を確認します。
ステップ 5 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトに戻して、デフォルト ルートがないネットワークのサブネット宛パケットが最適なスーパーネット ルートに転送されるようにするには、**ip classless** グローバル コンフィギュレーション コマンドを使用します。

アドレス解決方法の設定

インターフェイス固有の IP 処理方法を制御するには、アドレス解決を行います。IP を使用するデバイスには、ローカル セグメントまたは LAN 上のデバイスを一意に定義するローカル アドレスまたは MAC (メディア アクセス制御) アドレスと、デバイスが属するネットワークを特定するネットワーク アドレスがあります。



(注)

Catalyst 3750 スイッチ スタックでは、スタックの単一の MAC アドレスおよび IP アドレスを使用して、ネットワーク通信を行います。

ローカルアドレス (MAC アドレス) は、パケット ヘッダーのデータ リンク層 (レイヤ 2) セクションに格納されて、データ リンク (レイヤ 2) デバイスによって読み取られるため、データ リンク アドレスと呼ばれます。ソフトウェアがイーサネット上のデバイスと通信するには、デバイスの MAC アドレスを学習する必要があります。IP アドレスから MAC アドレスを学習するプロセスを、**アドレス解決**と呼びます。MAC アドレスから IP アドレスを学習するプロセスを、**逆アドレス解決**と呼びます。

スイッチでは、次の形式のアドレス解決を行うことができます。

- **ARP** : IP アドレスを MAC アドレスと関連付けるために使用されます。ARP は IP アドレスを入力と解釈し、対応する MAC アドレスを学習します。次に、IP アドレス/MAC アドレスの関連を ARP キャッシュに格納し、すぐに取り出せるようにします。そのあと、IP データグラムがリンク レイヤ フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化、および ARP 要求や応答については、Subnetwork Access Protocol (SNAP) で規定されています。
- **プロキシ ARP** : ルーティング テーブルを持たないホストで、他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにします。スイッチ (ルータ) が送信元と異なるインターフェイス上のホストに宛てた ARP 要求を受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。

スイッチでは、ARP と同様の機能 (RARP パケットがローカル MAC アドレスでなく IP アドレスを要求する点を除く) を持つ **Reverse Address Resolution Protocol (RARP; 逆アドレス解決プロトコル)** を使用することもできます。RARP を使用するには、ルータ インターフェイスと同じネットワーク セグメント上に RARP サーバを設置する必要があります。サーバを識別するには、**ip rarp-server address** インターフェイス コンフィギュレーション コマンドを使用します。

RARP に関する詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*] Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides]) からアクセス可能です。

アドレス解決を設定するために必要な作業は次のとおりです。

- 「**スタティック ARP キャッシュの定義**」 (P.38-11)
- 「**ARP カプセル化の設定**」 (P.38-12)
- 「**プロキシ ARP のイネーブル化**」 (P.38-12)

スタティック ARP キャッシュの定義

ARP および他のアドレス解決プロトコルを使用すると、IP アドレスと MAC アドレス間を動的にマッピングできます。ほとんどのホストでは動的なアドレス解決がサポートされているため、通常の場合、スタティック ARP キャッシュ エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。グローバルに定義すると、IP アドレスを MAC アドレスに変換するために使用される永続的なエントリを、ARP キャッシュに確保できます。また、指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定することもできます。ARP エントリを永続的なエントリにしない場合は、ARP エントリのタイムアウト期間を指定できます。

IP アドレスと MAC アドレスの間でスタティック マッピングを行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>arp ip-address hardware-address type</code>	ARP キャッシュ内で IP アドレスを MAC (ハードウェア) アドレスにグローバルに関連付け、次に示すカプセル化タイプのいずれかを指定します。 <ul style="list-style-type: none"> • arpa : ARP カプセル化 (イーサネット インターフェイス用) • snap : SNAP カプセル化 (トークン リングおよび FDDI インターフェイス用) • sap : HP の ARP タイプ
ステップ 3	<code>arp ip-address hardware-address type [alias]</code>	(任意) 指定された IP アドレスがスイッチに属する場合と同じ方法で、スイッチが ARP 要求に応答するように指定します。
ステップ 4	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 5	<code>arp timeout seconds</code>	(任意) ARP キャッシュ エントリがキャッシュに保持される期間を設定します。デフォルトは 14400 秒 (4 時間) です。指定できる範囲は 0 ~ 2147483 秒です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show interfaces [interface-id]</code>	すべてのインターフェイスまたは特定のインターフェイスで使用される ARP のタイプおよびタイムアウト値を確認します。
ステップ 8	<code>show arp</code> または <code>show ip arp</code>	ARP キャッシュの内容を表示します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ARP キャッシュからエントリを削除するには、`no arp ip-address hardware-address type` グローバル コンフィギュレーション コマンドを使用します。ARP キャッシュから非スタティック エントリをすべて削除するには、`clear arp-cache` 特権 EXEC コマンドを使用します。

ARP カプセル化の設定

IP インターフェイスでは、イーサネット ARP 形式の ARP カプセル化 (**arpa** キーワードで表される) がデフォルトでイネーブルに設定されています。ネットワークの必要性に応じて、カプセル化方法を SNAP に変更できます。

ARP カプセル化タイプを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	arp {arpa snap}	ARP カプセル化方法を指定します。 <ul style="list-style-type: none"> • arpa : ARP • snap : SNAP
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces [interface-id]	すべてのインターフェイスまたは指定されたインターフェイスの ARP カプセル化設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

カプセル化タイプをディセーブルにするには、**no arp arpa** または **no arp snap** インターフェイス コンフィギュレーション コマンドを使用します。

プロキシ ARP のイネーブル化

デフォルトでは、プロキシ ARP が使用されます。ホストが他のネットワークまたはサブネット上のホストの MAC アドレスを学習できるようにするためです。

ディセーブルになっているプロキシ ARP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip proxy-arp	インターフェイスでプロキシ ARP をイネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip interface [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスでプロキシ ARP をディセーブルにするには、**no ip proxy-arp** インターフェイス コンフィギュレーション コマンドを使用します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、スイッチは IP ルーティングがイネーブルでない場合、別のネットワークへのルートを取得できます。

- 「プロキシ ARP」 (P.38-13)
- 「デフォルト ゲートウェイ」 (P.38-13)
- 「ICMP Router Discovery Protocol (IRDP)」 (P.38-14)

プロキシ ARP

プロキシ ARP は、他のルートを取得する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネット ホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカル イーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。送信元と異なるネットワーク上にあるホストに宛てた ARP 要求を受信したスイッチは、そのホストへの最適なルートがあるかどうかを調べます。最適ルートがある場合、スイッチはスイッチ自身のイーサネット MAC アドレスが格納された ARP 応答パケットを送信します。要求の送信元ホストはパケットをスイッチに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 処理を実行します。

プロキシ ARP は、デフォルトでイネーブルに設定されています。ディセーブル化されたプロキシ ARP をイネーブルにするには、「[プロキシ ARP のイネーブル化](#)」 (P.38-12) を参照してください。プロキシ ARP は、他のルータでサポートされている限り有効です。

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP Control Message Protocol (ICMP) リダイレクト メッセージを返信するという方法で、ホストが使用するローカル ルータを定義します。スイッチはリダイレクト メッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

IP ルーティングがディセーブルの場合にデフォルト ゲートウェイ (ルータ) を定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip default-gateway ip-address</code>	デフォルト ゲートウェイ (ルータ) を設定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip redirects</code>	設定を確認するため、デフォルト ゲートウェイ ルータのアドレスを表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、`no ip default-gateway` グローバル コンフィギュレーション コマンドを使用します。

ICMP Router Discovery Protocol (IRDP)

ルータ ディスカバリを使用すると、スイッチは IRDP を使用し、他のネットワークへのルートを動的に取得します。ホストは IRDP を使用し、ルータを特定します。クライアントとして動作しているスイッチは、ルータ ディスカバリ パケットを生成します。ホストとして動作しているスイッチは、ルータ ディスカバリ パケットを受信します。スイッチは Routing Information Protocol (RIP) ルーティングの更新を受信し、この情報からルータの場所を推測することもできます。実際のところ、ルーティング デバイスによって送信されたルーティング テーブルは、スイッチに格納されません。どのシステムがデータを送信しているのかが記録されるだけです。IRDP を使用する利点は、プライオリティと、パケットが受信されなくなってからデバイスがダウンしていると思なされるまでの期間をルータごとに両方指定できることです。

検出された各デバイスは、デフォルト ルータの候補となります。現在のデフォルト ルータがダウンしたと宣言された場合、または再送信が多すぎて TCP 接続がタイムアウトになりつつある場合、プライオリティが上位のルータが検出されると、最も高いプライオリティを持つ新しいルータが選択されます。

インターフェイスで IRDP ルーティングを行う場合は、インターフェイスで IRDP 処理をイネーブルにしてください。IRDP 処理をイネーブルにすると、デフォルトのパラメータが適用されます。これらのパラメータを変更することもできます。

インターフェイス上で IRDP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	<code>ip irdp</code>	インターフェイス上で IRDP 処理をイネーブルにします。
ステップ 4	<code>ip irdp multicast</code>	(任意) IP ブロードキャストの代わりに、マルチキャストアドレス (224.0.0.1) に IRDP アドバタイズメントを送信します。 (注) このコマンドを使用すると、IRDP パケットをマルチキャストとして送信するサン マイクロシステムズ社の Solaris との互換性を維持できます。実装機能の中には、これらのマルチキャストを受信できないものも多くあります。このコマンドを使用する前に、エンドホストがこの機能に対応していることを確認してください。
ステップ 5	<code>ip irdp holdtime seconds</code>	(任意) アドバタイズメントが有効である IRDP 期間を設定します。デフォルトは <code>maxadvertinterval</code> 値の 3 倍です。 <code>maxadvertinterval</code> 値よりも大きな値 (9000 秒以下) を指定する必要があります。 <code>maxadvertinterval</code> 値を変更すると、この値も変更されます。
ステップ 6	<code>ip irdp maxadvertinterval seconds</code>	(任意) アドバタイズメント間の IRDP の最大インターバルを設定します。デフォルト値は 600 秒です。
ステップ 7	<code>ip irdp minadvertinterval seconds</code>	(任意) アドバタイズメント間の IRDP の最小インターバルを設定します。デフォルトは <code>maxadvertinterval</code> 値の 0.75 倍です。 <code>maxadvertinterval</code> を変更すると、この値も新しいデフォルト値 (<code>maxadvertinterval</code> の 0.75 倍) に変更されます。
ステップ 8	<code>ip irdp preference number</code>	(任意) デバイスの IRDP 初期設定レベルを設定します。指定できる範囲は -2^{31} ~ 2^{31} です。デフォルトは 0 です。大きな値を設定すると、ルータの初期設定レベルも高くなります。

	コマンド	目的
ステップ 9	<code>ip irdp address address [number]</code>	(任意) プロキシアドバタイズメントを行うために必要な IRDP アドレスと初期設定を指定します。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show ip irdp</code>	IRDP 値を表示し、設定を確認します。
ステップ 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

`maxadvertinterval` 値を変更すると、`holdtime` 値および `minadvertinterval` 値も変更されます。最初に `maxadvertinterval` 値を変更し、次に `holdtime` 値または `minadvertinterval` 値のいずれかを手動で変更することが重要です。

IRDP ルーティングをディセーブルにするには、`no ip irdp` インターフェイス コンフィギュレーション コマンドを使用します。

ブロードキャスト パケットの処理方法の設定

IP インターフェイス アドレスを設定したあとで、ルーティングをイネーブルにしたり、1 つまたは複数のルーティング プロトコルを設定したり、ネットワーク ブロードキャストへのスイッチの応答方法を設定したりできます。ブロードキャストは、物理ネットワーク上のすべてのホスト宛のデータ パケットです。2 種類のブロードキャストがサポートされています。

- 指定ブロードキャスト パケット：特定のネットワークまたは一連のネットワークに送信されます。指定ブロードキャスト アドレスには、ネットワークまたはサブネット フィールドが含まれます。
- フラッドイング ブロードキャスト パケット：すべてのネットワークに送信されます。



(注) **storm-control** インターフェイス コンフィギュレーション コマンドを使用して、トラフィック抑制レベルを設定し、レイヤ 2 インターフェイスでブロードキャスト、ユニキャスト、マルチキャストトラフィックを制限することもできます。詳細は、第 26 章「ポート単位のトラフィック制御の設定」を参照してください。

ルータはローカル ケーブル長を制限して、ブロードキャスト ストームを防ぎます。ブリッジ (インテリジェントなブリッジを含む) はレイヤ 2 デバイスであるため、ブロードキャストはすべてのネットワーク セグメントに転送され、ブロードキャスト ストームが伝播します。ブロードキャスト ストーム問題を解決する最善の方法は、ネットワーク上で単一のブロードキャスト アドレス方式を使用することです。最新の IP 実装機能ではほとんどの場合、アドレスをブロードキャスト アドレスとして使用するように設定できます。スイッチをはじめ、多数の実装機能では、ブロードキャスト メッセージを転送するためのアドレス方式が複数サポートされています。

これらの方式をイネーブルにするには、次に示す作業を実行します。

- 「指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化」(P.38-16)
- 「UDP ブロードキャスト パケットおよびプロトコルの転送」(P.38-17)
- 「IP ブロードキャスト アドレスの確立」(P.38-18)
- 「IP ブロードキャストのフラッドイング」(P.38-18)

指定ブロードキャストから物理ブロードキャストへの変換のイネーブル化

デフォルトでは、IP 指定ブロードキャストが廃棄されるため、転送されることはありません。IP 指定ブロードキャストが廃棄されると、ルータが DoS 攻撃にさらされる危険が少なくなります。

ブロードキャストが物理 (MAC レイヤ) ブロードキャストになるインターフェイスでは、IP 指定ブロードキャストの転送をイネーブルにできます。ip forward-protocol グローバル コンフィギュレーション コマンドを使用し、設定されたプロトコルだけを転送できます。

転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが、指定ブロードキャストから物理ブロードキャストに変換できるようになります。アクセス リストの詳細については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。

インターフェイス上で IP 指定ブロードキャストの転送をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	<code>ip directed-broadcast [access-list-number]</code>	<p>インターフェイス上で、指定ブロードキャストから物理ブロードキャストへの変換をイネーブルにします。転送するブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、アクセス リストで許可されている IP パケットだけが変換可能になります。</p> <p>(注) <code>ip directed-broadcast</code> インターフェイス コンフィギュレーション コマンドは VPN Routing/Forwarding (VRF) インターフェイスで設定でき、こうすると VRF 認識になります。指定ブロードキャストトラフィックが VRF 内だけでルーティングされます。</p>
ステップ 4	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	<code>ip forward-protocol {udp [port] nd sdns}</code>	<p>ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。</p> <ul style="list-style-type: none"> <code>udp</code> : UDP データグラムを転送します。 <code>port</code> : (任意) 転送される UDP サービスを制御する宛先ポートです。 <code>nd</code> : ND データグラムを転送します。 <code>sdns</code> : SDNS データグラムを転送します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip interface [interface-id]</code> または <code>show running-config</code>	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定ブロードキャストから物理ブロードキャストへの変換をディセーブルにするには、**no ip directed-broadcast** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

UDP ブロードキャスト パケットおよびプロトコルの転送

UDP は IP のホスト間レイヤ プロトコルで、TCP と同様です。UDP はオーバーヘッドが少ない、コネクションレスのセッションを 2 つのエンドシステム間に提供しますが、受信されたデータグラムの確認応答は行いません。場合に応じてネットワーク ホストは UDP ブロードキャストを使用し、アドレス、コンフィギュレーション、名前に関する情報を検索します。このようなホストが、サーバを含まないネットワーク セグメント上にある場合、通常 UDP ブロードキャストは転送されません。この状況を改善するには、特定のクラスのブロードキャストをヘルパー アドレスに転送するように、ルータのインターフェイスを設定します。インターフェイスごとに、複数のヘルパー アドレスを使用できます。

UDP 宛先ポートを指定し、転送される UDP サービスを制御できます。複数の UDP プロトコルを指定することもできます。旧式のディスクレス Sun ワークステーションおよびネットワーク セキュリティ プロトコル SDNS で使用される Network Disk (ND) プロトコルも指定できます。

ヘルパー アドレスがインターフェイスに定義されている場合、デフォルトでは UDP と ND の両方の転送がイネーブルになっています。『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』Release 12.2 の **ip forward-protocol** インターフェイス コンフィギュレーション コマンドの説明には、UDP ポートを指定しない場合にデフォルトで転送されるポートがリストされています。

UDP ブロードキャストの転送を設定するときに UDP ポートを指定しないと、ルータは BOOTP 転送 エージェントとして動作するように設定されます。BOOTP パケットは Dynamic Host Configuration Protocol (DHCP) 情報を伝達します。

インターフェイスで UDP ブロードキャスト パケットの転送をイネーブルにし、宛先アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip helper-address address	転送をイネーブルにし、BOOTP などの UDP ブロードキャスト パケットを転送するための宛先アドレスを指定します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	ip forward-protocol {udp [port] nd sdns}	ブロードキャスト パケットを転送するときに、ルータによって転送されるプロトコルを指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip interface [interface-id] または show running-config	指定されたインターフェイスまたはすべてのインターフェイスの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定アドレスへのブロードキャスト パケットの転送をディセーブルにするには、**no ip helper-address** インターフェイス コンフィギュレーション コマンドを使用します。プロトコルまたはポートを削除するには、**no ip forward-protocol** グローバル コンフィギュレーション コマンドを使用します。

IP ブロードキャストアドレスの確立

最も一般的な（デフォルトの）IP ブロードキャストアドレスは、すべて 1 で構成されているアドレスです（255.255.255.255）。ただし、任意の形式の IP ブロードキャストアドレスを生成するようにスイッチを設定することもできます。

インターフェイス上で IP ブロードキャストアドレスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	<code>ip broadcast-address ip-address</code>	デフォルト値と異なるブロードキャストアドレス（128.1.255.255 など）を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip interface [interface-id]</code>	指定されたインターフェイスまたはすべてのインターフェイスのブロードキャストアドレスを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの IP ブロードキャストアドレスに戻すには、`no ip broadcast-address` インターフェイス コンフィギュレーション コマンドを使用します。

IP ブロードキャストのフラッディング

IP ブロードキャストをインターネットワーク全体に、制御可能な方法でフラッディングできるようにするには、ブリッジング STP で作成されたデータベースを使用します。この機能を使用すると、ループを回避することもできます。この機能を使用できるようにするには、フラッディングが行われるインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイス上でも、ブロードキャストを受信できます。ただし、ブリッジングが設定されていないインターフェイスでは、受信したブロードキャストが転送されません。また、異なるインターフェイスで受信されたブロードキャストを送信する場合、このインターフェイスは使用されません。

IP ヘルパー アドレスのメカニズムを使用して単一のネットワーク アドレスに転送されるパケットを、フラッディングできます。各ネットワーク セグメントには、パケットのコピーが 1 つだけ送信されません。

フラッディングを行う場合、パケットは次の条件を満たす必要があります（これらの条件は、IP ヘルパー アドレスを使用してパケットを転送するときの条件と同じです）。

- パケットは MAC レベルのブロードキャストでなければなりません。
- パケットは IP レベルのブロードキャストでなければなりません。
- パケットは Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル)、Domain Name System (DNS; ドメイン ネーム システム)、Time、NetBIOS、ND、または BOOTP パケット、または `ip forward-protocol udp` グローバル コンフィギュレーション コマンドで指定された UDP でなければなりません。
- パケットの Time To Live (TTL) 値は 2 以上でなければなりません。

フラッディングされた UDP データグラムには、出力インターフェイスで **ip broadcast-address** インターフェイス コンフィギュレーション コマンドによって指定された宛先アドレスを設定します。宛先アドレスを、任意のアドレスに設定できます。このため、データグラムがネットワーク内を伝播するにつれ、宛先アドレスが変更されることもあります。送信元アドレスは変更されません。TTL 値が減ります。

フラッディングされた UDP データグラムがインターフェイスから送信されると（場合によっては宛先アドレスが変更される）、データグラムは通常の IP 出力ルーチンに渡されます。このため、出力インターフェイスにアクセス リストがある場合、データグラムはその影響を受けます。

ブリッジング スパニング ツリー データベースを使用し、UDP データグラムをフラッディングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip forward-protocol spanning-tree	ブリッジング スパニング ツリー データベースを使用し、UDP データグラムをフラッディングします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP ブロードキャストのフラッディングをディセーブルにするには、**no ip forward-protocol spanning-tree** グローバル コンフィギュレーション コマンドを使用します。

スイッチでは、パケットの大部分がハードウェアで転送され、スイッチの CPU を経由しません。CPU に送信されるパケットの場合は、ターボフラッディングを使用し、スパニング ツリーベースの UDP フラッディングを約 4 ~ 5 倍高速化します。この機能は、ARP カプセル化用に設定されたイーサネット インターフェイスでサポートされています。

スパニング ツリーベースのフラッディングを向上させるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip forward-protocol turbo-flood	スパニング ツリー データベースを使用し、UDP データグラムのフラッディングを高速化します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip forward-protocol turbo-flood** グローバル コンフィギュレーション コマンドを使用します。

IP アドレスのモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容が無効になった場合、または無効である可能性がある場合は、**clear** 特権 EXEC コマンドを使用し、すべての内容を消去できます。表 38-2 に、内容を消去するために使用するコマンドを示します。

表 38-2 キャッシュ、テーブル、データベースを消去するコマンド

コマンド	目的
clear arp-cache	IP ARP キャッシュおよび高速スイッチング キャッシュを消去します。
clear host {name *}	ホスト名およびアドレス キャッシュから 1 つまたはすべてのエントリを削除します。
clear ip route {network [mask] *}	IP ルーティング テーブルから 1 つまたは複数のルートを削除します。

IP ルーティング テーブル、キャッシュ、データベースの内容、ノードへの到達可能性、ネットワーク内のパケットのルーティングパスなど、特定の統計情報を表示できます。表 38-3 に、IP 統計情報を表示するために使用する特権 EXEC コマンドを示します。

表 38-3 キャッシュ、テーブル、データベースを表示するコマンド

コマンド	目的
show arp	ARP テーブルのエントリを表示します。
show hosts	デフォルトのドメイン名、検索サービスの方式、サーバホスト名、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
show ip aliases	TCP ポートにマッピングされた IP アドレスを表示します (エイリアス)。
show ip arp	IP ARP キャッシュを表示します。
show ip interface [interface-id]	インターフェイスの IP ステータスを表示します。
show ip irdp	IRDp 値を表示します。
show ip masks address	ネットワーク アドレスに対して使用されるマスクおよび各マスクを使用するサブネット番号を表示します。
show ip redirects	デフォルト ゲートウェイのアドレスを表示します。
show ip route [address [mask]] [protocol]	ルーティング テーブルの現在のステータスを表示します。
show ip route summary	ルーティング テーブルの現在のステータスをサマリー形式で表示します。

IP ユニキャスト ルーティングのイネーブル化

デフォルトで、スイッチはレイヤ 2 スwitchング モード、IP ルーティングはディセーブルとなっています。スイッチのレイヤ 3 機能を使用するには、IP ルーティングをイネーブルにする必要があります。

IP ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティングをイネーブルにします。

コマンド	目的
ステップ 3 <code>router ip_routing_protocol</code>	IP ルーティング プロトコルを指定します。このステップでは、他のコマンドを実行することもできます。たとえば、 network (RIP) ルータ コンフィギュレーション コマンドを使用し、ルーティングするネットワークを指定できます。具体的なプロトコルの詳細については、この章の後半および『 <i>Cisco IOS IP Configuration Guide</i> 』 Release 12.2 を参照してください。 (注) IP ベース イメージは、ルーティング プロトコルとして RIP だけをサポートします。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。

次に、ルーティング プロトコルとして RIP を使用し、IP ルーティングをイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

ここで、選択したルーティング プロトコルのパラメータを設定できます。具体的な手順は次のとおりです。

- 「RIP の設定」 (P.38-21)
- 「OSPF の設定」 (P.38-27)
- 「EIGRP の設定」 (P.38-38)
- 「BGP の設定」 (P.38-47)
- 「プロトコル独立機能の設定」 (P.38-95) (任意)

RIP の設定

RIP は、小規模な同種ネットワーク間で使用するために作成された Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) です。RIP は、ブロードキャスト UDP データ パケットを使用してルーティング情報を交換するディスタンス ベクタ ルーティング プロトコルです。このプロトコルは RFC 1058 に文書化されています。RIP の詳細については、『*IP Routing Fundamentals*』 (Cisco Press 刊) を参照してください。



(注) RIP は IP ベース イメージでサポートされている唯一のルーティング プロトコルです。その他のルーティング プロトコルを使用する場合は、スタック マスター上で IP サービス イメージを稼働させる必要があります。

スイッチは RIP を使用し、30 秒ごとにルーティング情報アップデート（アドバタイズメント）を送信します。180 秒以上を経過しても別のルータからアップデートがルータに届かない場合、該当するルータから送られたルートは使用不能としてマークされます。240 秒が経過してもアップデートが届かない場合、アップデートを行わないルータに関するすべてのルーティングテーブル エントリは削除されません。

RIP では、各ルートの値を評価するためにホップ カウントが使用されます。ホップ カウントは、ルート内で経由されるルータ数です。直接接続されているネットワークのホップ カウントは 0 です。ホップ カウントが 16 のネットワークに到達することはできません。このように範囲（0 ～ 15）が狭いため、RIP は大規模ネットワークには適していません。

ルータにデフォルトのネットワーク パスが設定されている場合、RIP はルータを疑似ネットワーク 0.0.0.0 にリンクするルートをアドバタイズします。0.0.0.0 ネットワークは存在しません。RIP はデフォルトのルーティング機能を実行するためのネットワークとして、このネットワークを処理します。デフォルト ネットワークが RIP によって取得された場合、またはルータが最終ゲートウェイで、RIP がデフォルト メトリックによって設定されている場合、スイッチはデフォルト ネットワークをアドバタイズします。RIP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイスのネットワークを指定しないと、RIP アップデート中にアドバタイズされません。

ここでは、次の設定情報について説明します。

- 「RIP のデフォルト設定」(P.38-22)
- 「基本的な RIP パラメータの設定」(P.38-23)
- 「RIP 認証の設定」(P.38-25)
- 「サマリー アドレスおよびスプリット ホライズンの設定」(P.38-25)

RIP のデフォルト設定

表 38-4 に、RIP のデフォルト設定を示します。

表 38-4 RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。
デフォルト情報送信元	ディセーブル。
デフォルト メトリック	自動メトリック変換（組み込み）。
IP RIP 認証キーチェーン	認証なし。 認証モード：クリア テキスト。
IP RIP 受信バージョン	version ルータ コンフィギュレーション コマンドに準拠。
IP RIP 送信バージョン	version ルータ コンフィギュレーション コマンドに準拠。
IP RIP の起動	version ルータ コンフィギュレーション コマンドに準拠。
IP スプリット ホライズン	メディアにより異なる。
ネイバー	未定義。
ネットワーク	指定なし。
オフセット リスト	ディセーブル。
出力遅延	0 ミリ秒。

表 38-4 RIP のデフォルト設定 (続き)

機能	デフォルト設定
タイマー基準	<ul style="list-style-type: none"> • update : 30 秒。 • invalid : 180 秒。 • holddown : 180 秒。 • flush : 240 秒。
アップデート送信元の検証	イネーブル。
バージョン	RIP バージョン 1 およびバージョン 2 パケットを受信し、バージョン 1 パケットを送信します。

基本的な RIP パラメータの設定

RIP を設定するには、ネットワークに対して RIP ルーティングをイネーブルにします。他のパラメータを設定することもできます。Catalyst 3750 スイッチでは、ネットワーク番号を設定するまで RIP コンフィギュレーション コマンドは無視されます。

RIP をイネーブルにして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip routing</code>	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合に限り、必須です)。
ステップ 3	<code>router rip</code>	RIP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	<code>network network number</code>	ネットワークを RIP ルーティング プロセスに関連付けます。複数の network コマンドを指定できます。RIP ルーティング アップデートの送受信は、これらのネットワークのインターフェイスを経由する場合に限り可能です。 (注) RIP コマンドを有効にするためにネットワーク番号を設定する必要があります。
ステップ 5	<code>neighbor ip-address</code>	(任意) ルーティング情報を交換する近接ルータを定義します。このステップを使用すると、RIP (通常はブロードキャストプロトコル) からのルーティング アップデートが非ブロードキャスト ネットワークに到達するようになります。
ステップ 6	<code>offset list [access-list number name] {in out} offset [type number]</code>	(任意) オフセットリストをルーティング メトリックに適用し、RIP によって取得したルートへの着信および発信メトリックを増加します。アクセスリストまたはインターフェイスを使用し、オフセットリストを制限できます。

	コマンド	目的
ステップ 7	<code>timers basic update invalid holddown flush</code>	(任意) ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効範囲は 0 ~ 4294967295 秒です。 <ul style="list-style-type: none"> • <code>update</code> : ルーティング アップデートの送信間隔。デフォルト値は 30 秒です。 • <code>invalid</code> : ルートが無効と宣言されたあとの時間。デフォルト値は 180 秒です。 • <code>holddown</code> : ルートがルーティング テーブルから削除されるまでの時間。デフォルト値は 180 秒です。 • <code>flush</code> : ルーティング アップデートが延期される時間。デフォルト値は 240 秒です。
ステップ 8	<code>version {1 2}</code>	(任意) RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにスイッチを設定します。デフォルトの場合、スイッチではバージョン 1 および 2 を受信しますが、バージョン 1 だけを送信します。 インターフェイス コマンド <code>ip rip {send receive} version 1 2 1 2</code> を使用し、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 9	<code>no auto summary</code>	(任意) 自動サマライズをディセーブルにします。デフォルトでは、クラスフル ネットワーク境界を通過するときにサブプレフィクスがサマライズされます。サマライズをディセーブルにし (RIP バージョン 2 に限る)、クラスフル ネットワーク境界にサブネットおよびホストルーティング情報をアドバタイズします。
ステップ 10	<code>no validate-update-source</code>	(任意) 着信 RIP ルーティング アップデートの送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチが着信 RIP ルーティング アップデートの送信元 IP アドレスを検証します。送信元アドレスが無効な場合は、アップデートが廃棄されます。通常の環境で使用する場合は、この機能をディセーブルにしないでください。ただし、ネットワークに接続されていないルータがあり、そのルータのアップデートを受信する場合は、このコマンドを使用できます。
ステップ 11	<code>output-delay delay</code>	(任意) 送信する RIP アップデートにパケット間遅延を追加します。デフォルトでは、複数のパケットからなる RIP アップデートのパケットに、パケット間遅延が追加されません。パケットを低速なデバイスに送信する場合は、8 ~ 50 ミリ秒のパケット間遅延を追加できます。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip protocols</code>	設定を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをオフにするには、`no router rip` グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと現在のステータスを表示するには、`show ip protocols` 特権 EXEC コマンドを使用します。RIP データベースのサマリー アドレス エントリを表示するには、`show ip rip database` 特権 EXEC コマンドを使用します。

RIP 認証の設定

RIP バージョン 1 では、認証がサポートされていません。RIP バージョン 2 のパケットを送受信する場合は、インターフェイスで RIP 認証をイネーブルにできます。インターフェイスで使用できる一連の鍵は、キーチェーンによって決まります。キーチェーンが設定されていないと、デフォルトの場合でも認証は実行されません。「[認証鍵の管理](#)」(P.38-110)に記載されている作業も実行してください。

RIP 認証がイネーブルであるインターフェイスでは、プレーンテキストと MD5 という 2 つの認証モードがサポートされています。デフォルトはプレーンテキストです。

インターフェイスに RIP 認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	<code>ip rip authentication key-chain name-of-chain</code>	RIP 認証をイネーブルにします。
ステップ 4	<code>ip rip authentication mode [text md5]</code>	プレーンテキスト認証 (デフォルト) または MD5 ダイジェスト認証を使用するように、インターフェイスを設定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config interface [interface-id]</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

クリア テキスト認証に戻すには、**no ip rip authentication mode** インターフェイス コンフィギュレーション コマンドを使用します。認証を禁止するには、**no ip rip authentication key-chain** インターフェイス コンフィギュレーション コマンドを使用します。

サマリー アドレスおよびスプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンス ベクタ ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報がその情報の発信元であるインターフェイスで、ルータによってアドバタイズされないようにします。この機能を使用すると、通常の場合は複数のルータ間通信が最適化されます (特にリンクが壊れている場合)。



(注) ルートを適切にアドバタイズするため、スプリット ホライズンをディセーブルにすることがアプリケーションに必要な場合を除き、通常はこの機能をディセーブルにしないでください。

ダイヤルアップ クライアント用のネットワーク アクセス サーバで、サマライズされたローカルな IP アドレス プールをアドバタイズするように、RIP が動作しているインターフェイスを設定する場合は、**ip summary-address rip** インターフェイス コンフィギュレーション コマンドを使用します。



(注) スプリット ホライズンがイネーブルの場合、自動サマリーとインターフェイス IP サマリー アドレスはともにアドバタイズされません。

サマライズされたローカル IP アドレスをアドバタイズし、インターフェイスのスプリット ホライズンをディセーブルにするようにインターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip address ip-address subnet-mask	IP アドレスおよび IP サブネットを設定します。
ステップ 4	ip summary-address rip ip address ip-network mask	サマライズする IP アドレスおよび IP ネットワーク マスクを設定します。
ステップ 5	no ip split horizon	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip interface interface-id	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP サマライズをディセーブルにするには、**no ip summary-address rip** ルータ コンフィギュレーション コマンドを使用します。

次の例では、主要ネットは 10.0.0.0 です。自動サマリー アドレス 10.0.0.0 はサマリー アドレス 10.2.0.0 によって上書きされるため、10.2.0.0 はインターフェイス ギガビット イーサネット ポート 2 からアドバタイズされますが、10.0.0.0 はアドバタイズされません。次の例では、インターフェイスがまだレイヤ 2 モード (デフォルト) の場合、**no switchport** インターフェイス コンフィギュレーション コマンドを入力してから、**ip address** インターフェイス コンフィギュレーション コマンドを入力する必要があります。



(注)

スプリット ホライズンがイネーブルである場合、(**ip summary-address rip** ルータ コンフィギュレーション コマンドによって設定される) 自動サマリーとインターフェイス サマリー アドレスはともにアドバタイズされません。

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

スプリット ホライズンの設定

ブロードキャストタイプの IP ネットワークに接続され、ディスタンス ベクタ ルーティング プロトコルを使用するルータでは、通常ルーティング ループの発生を抑えるために、スプリット ホライズン メカニズムが使用されます。スプリット ホライズンは、ルートに関する情報がその情報の発信元である インターフェイスで、ルータによってアダプタイズされないようにします。この機能を使用すると、複数のルータ間通信が最適化されます（特にリンクが壊れている場合）。



(注) ルートを適切にアダプタイズするために、スプリット ホライズンをディセーブルにすることがアプリケーションに必要である場合を除き、通常この機能をディセーブルにしないでください。

インターフェイスでスプリット ホライズンをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	ip address ip-address subnet-mask	IP アドレスおよび IP サブネットを設定します。
ステップ 4	no ip split-horizon	インターフェイスでスプリット ホライズンをディセーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip interface interface-id	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スプリット ホライズン メカニズムをイネーブルにするには、**ip split-horizon** インターフェイス コンフィギュレーション コマンドを使用します。

OSPF の設定

ここでは、OSPF の設定方法について簡単に説明します。OSPF コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』 Release 12.2 を参照してください。これには、Cisco.com ホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセスできます。



(注) OSPF では、各メディアがブロードキャスト ネットワーク、非ブロードキャスト ネットワーク、ポイントツーポイント ネットワークに分類されます。スイッチでは、ブロードキャスト ネットワーク（イーサネット、トークンリング、FDDI）およびポイントツーポイント ネットワーク（ポイントツーポイント リンクとして設定されたイーサネット インターフェイス）がサポートされます。

OSPF は IP ネットワーク専用の IGP で、IP サブネット化、および外部から取得したルーティング情報のタグ付けをサポートしています。OSPF を使用するとパケット認証も可能になり、パケットを送受信するときに IP マルチキャストが使用されます。シスコの実装機能では、RFC1253 の OSPF MIB（管理情報ベース）がサポートされています。

シスコの実装機能は、次の主要機能を含む OSPF バージョン 2 仕様に準拠します。

- スタブ エリアの定義がサポートされています。
- 任意の IP ルーティング プロトコルによって取得されたルートは、別の IP ルーティング プロトコルに再配信されます。つまり、ドメイン内レベルで、OSPF は EIGRP および RIP によって取得したルートを取り込むことができます。OSPF ルートを RIP に伝達することもできます。
- エリア内の近接ルータ間でのプレーン テキスト認証および MD5 認証がサポートされています。
- 設定可能なルーティング インターフェイス パラメータには、インターフェイス出力コスト、再送信インターバル、インターフェイス送信遅延、ルータ プライオリティ、ルータの dead と hello インターバル、認証鍵などがあります。
- 仮想リンクがサポートされています。
- RFC 1587 に基づく Not-So-Stubby-Area (NSSA) がサポートされています。

通常、OSPF を使用するには、多くの内部ルータ、複数のエリアに接続された *Area Border Router* (ABR; エリア境界ルータ)、および *Autonomous System Boundary Router* (ASBR; 自律システム境界ルータ) 間で調整する必要があります。最小設定では、すべてのデフォルトパラメータ値、エリアに割り当てられたインターフェイスが使用され、認証は行われません。環境をカスタマイズする場合は、すべてのルータの設定を調整する必要があります。

ここでは、次の設定情報について説明します。

- 「OSPF のデフォルト設定」(P.38-28)
- 「基本的な OSPF パラメータの設定」(P.38-31)
- 「OSPF インターフェイスの設定」(P.38-32)
- 「OSPF エリア パラメータの設定」(P.38-33)
- 「その他の OSPF パラメータの設定」(P.38-34)
- 「LSA グループ同期設定の変更」(P.38-36)
- 「ループバック インターフェイスの設定」(P.38-37)
- 「OSPF のモニタ」(P.38-37)



(注) OSPF をイネーブルにするには、スタック マスター上で IP サービス イメージが稼働している必要があります。

OSPF のデフォルト設定

表 38-5 に、OSPF のデフォルト設定を示します。

表 38-5 OSPF のデフォルト設定

機能	デフォルト設定
インターフェイス パラメータ	コスト：デフォルト コストは未定義。 再送信インターバル：5 秒。 送信遅延：1 秒。 プライオリティ：1。 hello インターバル：10 秒。 dead インターバル：hello インターバルの 4 倍。 認証なし。 パスワードの指定なし。 MD5 認証はディセーブル。
エリア	認証タイプ：0（認証なし）。 デフォルト コスト：1。 範囲：ディセーブル。 スタブ：スタブ エリアは未定義。 NSSA：NSSA エリアは未定義。
自動コスト	100 Mbps。
デフォルト情報送信元	ディセーブル。イネーブルの場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルトはタイプ 2 です。
デフォルト メトリック	各ルーティング プロトコルに適切な、組み込みの自動メトリック変換。
距離 OSPF	dist1（エリア内のすべてのルート）：110。 dist2（エリア間のすべてのルート）：110。 dist3（他のルーティング ドメインからのルート）：110。
OSPF データベース フィルタ	ディセーブル。すべての発信 LSA がインターフェイスにフラッディングされます。
IP OSPF 名検索	ディセーブル。
隣接関係変更ログ	イネーブル
ネイバー	指定なし
近接データベース フィルタ	ディセーブル。すべての発信 LSA はネイバーにフラッディングされます。
ネットワーク エリア	ディセーブル
NSF ¹ 認識	IP サービス イメージが稼動しているスイッチの場合、イネーブル。 レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、近接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 機能	ディセーブル。Catalyst 3750 スイッチは、IPv4 対応の OSPF NSF（NSF 対応ルーティング）をサポートしています。
ルータ ID	OSPF ルーティング プロセスは未定義
サマリー アドレス	ディセーブル

表 38-5 OSPF のデフォルト設定 (続き)

機能	デフォルト設定
タイマー LSA グループの同期設定	240 秒
タイマー Shortest Path First (SPF)	spf-delay : 5 秒 spf-holdtime : 10 秒
仮想リンク	エリア ID またはルータ ID は未定義 hello インターバル : 10 秒 再送信インターバル : 5 秒 送信遅延 : 1 秒 dead インターバル : 40 秒 認証鍵 : 鍵は未定義 メッセージダイジェスト鍵 (MD5) : 鍵は未定義

1. NSF = Nonstop Forwarding

OSPF Nonstop Forwarding

スイッチ スタックは 2 つのレベルの NSF をサポートしています。

- 「OSPF NSF 認識」(P.38-30)
- 「OSPF NSF 機能」(P.38-30)

OSPF NSF 認識

IP サービス イメージは IPv4 の OSPF NSF 認識をサポートしています。近接ルータが NSF 対応で、レイヤ 3 スイッチでは、プライマリ Route Processor (RP) に障害が発生してルータのバックアップ RP によって引き継がれる前に、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、ルータからパケットを転送し続けます。

この機能をディセーブルにすることはできません。この機能の詳細については、次の URL の『*OSPF Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a0080153edd.shtml

OSPF NSF 機能

IP サービス イメージは、良好なコンバージェンスおよびスタック マスター変更後のトラフィックの損失を低減させるために、IPv4 の OSPF NSF 対応ルーティングをサポートしています。スタック マスターの変更が OSPF NSF 対応スタックで発生すると、新規スタック マスターでは、OSPF ネイバーとのリンクステート データベースを再同期させるために、次の 2 つのを行う必要があります。

- ネイバー関係をリセットせずにネットワーク上にある、利用可能な OSPF ネイバーを解放する。
- ネットワークのリンクステート データベースの内容を再取得する。

スタック マスターの変更後、新規マスターは OSPF NSF 信号をネイバー NSF 認識デバイスに送信します。デバイスでは、この信号を認識してスタックとのネイバー関係をリセットする必要がないことを把握します。NSF 対応スタック マスターは、ネットワーク上の他のルートから信号を受信すると、近接リストの再構築を開始します。

ネイバー関係が再構築されると、NSF 対応スタック マスターがデータベースと NSF 認識ネイバーを再同期させ、ルーティング情報を OSPF ネイバーと交換します。新規スタック マスターがこのルーティング情報を使用して無効なルートを削除し、Routing Information Database (RIB) をアップデートし、新規情報で Forwarding Information Base (FIB; 転送情報ベース) をアップデートします。これで、OSPF プロトコルが完全にコンバージします。



(注) OSPF NSF では、すべての近接ネットワーク デバイスが NSF 認識となっている必要があります。NSF 対応ルータがネットワーク セグメント内で非 NSF 対応ネイバーを検出すると、そのセグメントの NSF 機能がディセーブルになります。すべてのデバイスが NSF 認識または NSF 対応である他のネットワーク セグメントでは、NSF 機能が提供され続けます。

OSPF NSF ルーティングをイネーブルにするには、**nsf ospf** ルーティング コンフィギュレーション コマンドを使用します。このルーティングがイネーブルであることを確認するには、**show ip ospf** 特権 EXEC コマンドを使用します。

NSF の詳細については、次の URL の『Cisco Nonstop Forwarding Feature Overview』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00800ab7fc.html



(注) NSF は、Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) に設定されたインターフェイスをサポートしていません。

基本的な OSPF パラメータの設定

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに関連付ける IP アドレスの範囲を指定して、この範囲に関連付けるエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID はローカルに割り当てられ、内部で使用する識別パラメータで、任意の正の整数を指定できます。各 OSPF ルーティング プロセスには一意の値があります。
ステップ 3	nsf	(任意) OSPF の NSF 動作をイネーブルにします。
ステップ 4	network address wildcard-mask area area-id	OSPF が動作するインターフェイス、およびそのインターフェイスのエリア ID を定義します。単一のコマンドにワイルドカード マスクを指定し、特定の OSPF エリアに関連付けるインターフェイスを 1 つまたは複数定義できます。エリア ID には 10 進数または IP アドレスを指定できます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip protocols	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスを終了するには、**no router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。

次に、OSPF ルーティング プロセスを設定し、プロセス番号 109 を割り当てる例を示します。

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

OSPF インターフェイスの設定

ip ospf インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイス固有の OSPF パラメータを変更できます。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ (**hello** インターバル、**dead** インターバル、認証鍵など) については、接続されたネットワーク内のすべてのルータで統一性を維持する必要があります。これらのパラメータを変更した場合は、ネットワーク内のすべてのルータの値も同様に変更してください。



(注) **ip ospf** インターフェイス コンフィギュレーション コマンドはすべて任意です。

OSPF インターフェイス パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	ip ospf cost	(任意) インターフェイスでパケットを送信するコストを明確に指定します。
ステップ 4	ip ospf retransmit-interval seconds	(任意) リンクステート アドバタイズメント送信間隔を秒数で指定します。範囲は 1 ~ 65535 秒です。デフォルト値は 5 秒です。
ステップ 5	ip ospf transmit-delay seconds	(任意) リンク ステート アップデート パケットを送信するまでの予測待機時間を秒数で設定します。範囲は 1 ~ 65535 秒です。デフォルト値は 1 秒です。
ステップ 6	ip ospf priority number	(任意) ネットワークに対して、OSPF で指定されたルータを検索するときに役立つプライオリティを設定します。指定できる範囲は 0 ~ 255 です。デフォルト値は 1 です。
ステップ 7	ip ospf hello-interval seconds	(任意) OSPF インターフェイスで hello パケットの送信間隔を秒数で設定します。値はネットワークのすべてのノードで同じとします。範囲は 1 ~ 65535 秒です。デフォルト値は 10 秒です。
ステップ 8	ip ospf dead-interval seconds	(任意) 最後のデバイスで hello パケットが確認されてから、OSPF ルータがダウンしていることがネイバーによって宣言されるまでの時間を秒数で設定します。値はネットワークのすべてのノードで同じとします。範囲は 1 ~ 65535 秒です。デフォルト値は hello インターバルの 4 倍です。
ステップ 9	ip ospf authentication-key key	(任意) 近接 OSPF ルータで使用されるパスワードを割り当てます。パスワードには、キーボードから入力した任意の文字列 (最大 8 バイト長) を指定できます。同じネットワーク上のすべての近接ルータには、OSPF 情報を交換するため、同じパスワードを設定する必要があります。

コマンド	目的
ステップ 10 <code>ip ospf message-digest-key keyid md5 key</code>	(任意) MDS 認証をイネーブルにします。 <ul style="list-style-type: none"> • <i>keyid</i> : 1 ~ 255 の ID • <i>key</i> : 最大 16 バイトの英数字パスワード
ステップ 11 <code>ip ospf database-filter all out</code>	(任意) インターフェイスへの OSPF LSA パケットのフラッディングを阻止します。デフォルトでは、LSA が着信するインターフェイスを除き、同じエリア内のすべてのインターフェイスに OSPF は新しい LSA をフラッディングします。
ステップ 12 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 13 <code>show ip ospf interface [interface-name]</code>	OSPF に関連するインターフェイス情報を表示します。
ステップ 14 <code>show ip ospf neighbor detail</code>	近接スイッチの NSF 認証ステータスを表示します。出力は、次のいずれかに一致します。 <ul style="list-style-type: none"> • <i>Options is 0x52</i> <i>LLS Options is 0x1 (LR)</i> これらの行の両方が表示される場合、近接スイッチが NSF アウェアです。 <ul style="list-style-type: none"> • <i>Options is 0x42</i> : 近接スイッチが NSF アウェアでないことを示します。
ステップ 15 <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

OSPF エリア パラメータの設定

複数の OSPF エリア パラメータを設定することもできます。設定できるパラメータには、エリア、スタブ エリア、および Not-So-Stubby-Area (NSSA) への無許可アクセスをパスワードによって阻止する認証用パラメータがあります。スタブ エリアに外部ルートに関する情報は送信されませんが、代わりに、Autonomous System (AS; 自律システム) 外の宛先に対するデフォルトの外部ルートが、Area Border Router (ABR) によって生成されます。NSSA ではコアからそのエリアへ向かう LSA の一部がフラッディングされませんが、再配信することによって、エリア内の AS 外部ルートを取り込むことができます。

ルートのサマライズは、アドバタイズされたアドレスを、他のエリアでアドバタイズされる単一のサマリールートに統合することです。ネットワーク番号が連続する場合は、**area range** ルータ コンフィギュレーション コマンドを使用し、範囲内のすべてのネットワークを対象とするサマリールートをアドバタイズするように ABR を設定できます。



(注) OSPF **area** ルータ コンフィギュレーション コマンドはすべて任意です。

エリア パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>area area-id authentication</code>	(任意) 特定のエリアへの無許可アクセスに対して、パスワードベースの保護を可能にします。ID には 10 進数または IP アドレスのいずれかを指定できます。
ステップ 4	<code>area area-id authentication message-digest</code>	(任意) エリアに関して MD5 認証をイネーブルにします。
ステップ 5	<code>area area-id stub [no-summary]</code>	(任意) エリアをスタブ エリアとして定義します。 no-summary キーワードを指定すると、ABR はサマリー リンク アドバタイズメントをスタブ エリアに送信できなくなります。
ステップ 6	<code>area area-id nssa [no-redistribution] [default-information-originate] [no-summary]</code>	(任意) エリアを NSSA として定義します。同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。次のキーワードのいずれかを選択します。 <ul style="list-style-type: none"> no-redistribution : ルータが NSSA ABR の場合、redistribute コマンドを使用して、ルートを NSSA でなく通常のエリアに取り込む場合に選択します。 default-information-originate : タイプ 7 LSA を NSSA に取り込むようにする場合に、ABR で選択します。 no-redistribution : サマリー LSA を NSSA に送信しない場合に選択します。
ステップ 7	<code>area area-id range address mask</code>	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show ip ospf [process-id]</code>	設定を確認するため、一般的な OSPF ルーティング プロセスまたは特定のプロセス ID に関する情報を表示します。
	<code>show ip ospf [process-id [area-id]] database</code>	特定のルータの OSPF データベースに関連する情報のリストを表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたパラメータ値を削除する場合、またはデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

その他の OSPF パラメータの設定

ルータ コンフィギュレーション モードで、その他の OSPF パラメータを設定することもできます。

- ルート サマライズ: 他のプロトコルからのルートを再配信すると ([「ルート マップによるルーティング情報の再配信」\(P.38-99\)](#) を参照)、各ルートは外部 LSA 内で個別にアドバタイズされます。OSPF リンク ステート データベースのサイズを小さくするには、**summary-address** ルータ コンフィギュレーション コマンドを使用し、指定されたネットワーク アドレスおよびマスクに含まれる、再配信されたすべてのルートを単一のルータにアドバタイズします。

- 仮想リンク：OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンが不連続である場合に仮想リンクを確立するには、2 つの ABR を仮想リンクのエンドポイントとして設定します。設定情報には、他の仮想エンドポイント（他の ABR）の ID、および 2 つのルータに共通する非バックボーンリンク（通過エリア）などがあります。仮想リンクをスタブ エリアから設定することはできません。
- デフォルト ルート：OSPF ルーティング ドメイン内へのルート再配信を設定すると、ルータは自動的に自律システム境界ルータ（ASBR）になります。ASBR を設定し、強制的に OSPF ルーティング ドメインにデフォルト ルートを生成できます。
- すべての OSPF **show** 特権 EXEC コマンドで使用される Domain Name Server（DNS）名を使用すると、ルータ ID やネイバー ID を指定して表示する場合に比べ、ルータを簡単に特定できます。
- デフォルト メトリック：OSPF は、インターフェイスの帯域幅に従ってインターフェイスの OSPF メトリックを計算します。メトリックは、帯域幅で分割された *ref-bw* として計算されます。ここでの *ref* のデフォルト値は 10 で、帯域幅 (*bw*) は **bandwidth** インターフェイス コンフィギュレーション コマンドによって指定されます。大きな帯域幅を持つ複数のリンクの場合は、大きな数値を指定し、これらのリンクのコストを区別できます。
- 管理距離は、ルーティング情報送信元の信頼性を表す数値です。0 ~ 255 の整数を指定でき、値が大きいほど信頼性は低下します。管理距離が 255 の場合はルーティング情報送信元をまったく信頼できないため、無視する必要があります。OSPF では、エリア内のルート（エリア内）、別のエリアへのルート（エリア間）、および再配信によって取得した別のルーティング ドメインからのルート（外部）の 3 つの管理距離が使用されます。どの管理距離の値でも変更できます。
- パッシブ インターフェイス：イーサネット上の 2 つのデバイス間のインターフェイスは 1 つのネットワーク セグメントしか表しません。このため、OSPF が送信側インターフェイスに **hello** パケットを送信しないようにするには、送信側デバイスをパッシブ インターフェイスに設定する必要があります。両方のデバイスは受信側インターフェイス宛の **hello** パケットを使用することで、相互の識別を可能にします。
- ルート計算タイマー：OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間、および 2 つの SPF 計算の間のホールド タイムを設定できます。
- ネイバー変更ログ：OSPF ネイバー ステートが変更されたときに Syslog メッセージを送信するようにルータを設定し、ルータの変更を詳細に表示できます。

上記の OSPF パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router ospf process-id	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	summary-address address mask	(任意) 1 つのサマリー ルートだけがアドバタイズされるように、再配信されたルート of アドレスおよび IP サブネット マスクを指定します。
ステップ 4	area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [trans] [[authentication-key key] message-digest-key keyid md5 key]]	(任意) 仮想リンクを確立し、パラメータを設定します。パラメータ定義については「OSPF インターフェイスの設定」(P.38-32)、仮想リンクのデフォルト設定については表 38-5 (P.38-29) を参照してください。
ステップ 5	default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]	(任意) 強制的に OSPF ルーティング ドメインにデフォルト ルートを生成するように ASBR を設定します。パラメータはすべて任意です。
ステップ 6	ip ospf name-lookup	(任意) DNS 名検索を設定します。デフォルトはディセーブルです。

	コマンド	目的
ステップ 7	<code>ip auto-cost reference-bandwidth ref-bw</code>	(任意) 単一のルートをアドバタイズするアドレス範囲を指定します。このコマンドは、ABR に対してだけ使用します。
ステップ 8	<code>distance ospf {[inter-area dist1] [inter-area dist2] [external dist3]}</code>	(任意) OSPF の距離の値を変更します。各タイプのルートのデフォルト距離は 110 です。指定できる範囲は 1 ~ 255 です。
ステップ 9	<code>passive-interface type number</code>	(任意) 指定されたインターフェイス経由の hello パケットの送信を抑制します。
ステップ 10	<code>timers throttle spf spf-delay spf-holdtime spf-wait</code>	(任意) ルート計算タイマーを設定します。 <ul style="list-style-type: none"> <code>spf-delay</code> : SPF 計算の変更を受信する間の遅延。指定できる範囲は 1 ~ 600000 ミリ秒です。 <code>spf-holdtime</code> : 最初と 2 番目の SPF 計算の間の遅延。指定できる範囲は 1 ~ 600000 ミリ秒です。 <code>spf-wait</code> : SPF 計算の最大待機時間 (ミリ秒)。指定できる範囲は 1 ~ 600000 ミリ秒です。
ステップ 11	<code>ospf log-adj-changes</code>	(任意) ネイバー ステートが変更されたとき、Syslog メッセージを送信します。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show ip ospf [process-id [area-id]] database</code>	特定のルータの OSPF データベースに関連する情報のリストを表示します。キーワード オプションの一部については、「 OSPF のモニタ 」(P.38-37) を参照してください。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

LSA グループ同期設定の変更

OSPF LSA グループ同期設定機能を使用すると、OSPF LSA をグループ化し、リフレッシュ、チェックサム、エージング機能の同期を取って、ルータをより効率的に使用することが可能となります。デフォルトでこの機能はイネーブルとなっています。デフォルトの同期インターバルは 4 分間です。通常は、このパラメータを変更する必要はありません。最適なグループ同期インターバルは、ルータがリフレッシュ、チェックサム、エージングを行う LSA 数に反比例します。たとえば、データベース内に約 10,000 個の LSA が格納されている場合は、同期設定インターバルを短くすると便利です。小さなデータベース (40 ~ 100 LSA) を使用する場合は、同期インターバルを長くし、10 ~ 20 分に設定してください。

OSPF LSA 同期を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>timers lsa-group-pacing seconds</code>	LSA のグループ同期を変更します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

ループバック インターフェイスの設定

OSPF は、インターフェイスに設定されている最大の IP アドレスをルータ ID として使用します。このインターフェイスがダウンした場合、または削除された場合、OSPF プロセスは新しいルータ ID を再計算し、すべてのルーティング情報をそのルータのインターフェイスから再送信します。ループバック インターフェイスが IP アドレスによって設定されている場合、他のインターフェイスにより大きな IP アドレスがある場合でも、OSPF はこの IP アドレスをルータ ID として使用します。ループバック インターフェイスに障害は発生しないため、安定性は増大します。OSPF は他のインターフェイスよりもループバック インターフェイスを自動的に優先し、すべてのループバック インターフェイスの中で最大の IP アドレスを選択します。

ループバック インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface loopback 0	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip address address mask	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

OSPF のモニタ

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

表 38-6 に、統計情報を表示するために使用する特権 EXEC コマンドの一部を示します。**show ip ospf database** 特権 EXEC コマンドのオプションおよび表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。

表 38-6 IP OSPF 統計情報の表示コマンド

コマンド	目的
<code>show ip ospf [process-id]</code>	OSPF ルーティング プロセスに関する一般的な情報を表示します。
<code>show ip ospf [process-id] database [router] [link-state-id]</code> <code>show ip ospf [process-id] database [router] [self-originate]</code> <code>show ip ospf [process-id] database [router] [adv-router [ip-address]]</code> <code>show ip ospf [process-id] database [network] [link-state-id]</code> <code>show ip ospf [process-id] database [summary] [link-state-id]</code> <code>show ip ospf [process-id] database [asbr-summary] [link-state-id]</code> <code>show ip ospf [process-id] database [external] [link-state-id]</code> <code>show ip ospf [process-id area-id] database [database-summary]</code>	OSPF データベースに関連する情報を表示します。
<code>show ip ospf border-routes</code>	内部の OSPF ルーティング ABR および ASBR テーブル エントリを表示します。
<code>show ip ospf interface [interface-name]</code>	OSPF に関連するインターフェイス情報を表示します。
<code>show ip ospf neighbor [interface-name] [neighbor-id] detail</code>	OSPF インターフェイス近接情報を表示します。
<code>show ip ospf virtual-links</code>	OSPF に関連する仮想リンク情報を表示します。

EIGRP の設定

EIGRP は IGRP のシスコ独自の拡張バージョンです。EIGRP は IGRP と同じディスタンス ベクタ アルゴリズムおよび距離情報を使用しますが、EIGRP では収束性および動作効率が大幅に改善されています。

コンバージェンス技術には、Diffusing Update Algorithm (DUAL) と呼ばれるアルゴリズムが採用されています。DUAL を使用すると、ルート計算の各段階でループが発生しなくなり、トポロジの変更に関連するすべてのデバイスを同時に同期できます。トポロジ変更の影響を受けないルータは、再計算から除外されます。

IP EIGRP を導入すると、ネットワークの幅が広がります。RIP の場合、ネットワークの最大幅は 15 ホップです。EIGRP メトリックは数千ホップをサポートするほど大きいため、ネットワークを拡張するときに問題となるのは、トランスポート レイヤのホップ カウンタだけです。IP パケットが 15 台のルータを経由し、宛先方向のネクスト ホップが EIGRP によって取得されている場合だけ、EIGRP は転送制御フィールドの値を増やします。RIP ルートを宛先へのネクスト ホップとして使用する場合、転送制御フィールドでは、通常どおり値が増加します。

EIGRP には次の機能があります。

- 高速コンバージェンス
- 差分更新：宛先のステータスに変更された場合、ルーティング テーブルの内容全体を送信する代わりに差分更新を行い、EIGRP パケットに必要な帯域幅を最小化します。
- 低い CPU 使用率：受信ごとに完全更新パケットを処理する必要がないため、CPU 使用率が低下します。
- プロトコルに依存しない近接ディスカバリ メカニズム：このメカニズムを使用し近接ルータに関する情報を取得します。

- Variable-Length Subnet Mask (VLSM; 可変長サブネット マスク)
- 任意のルート サマライズ
- 大規模ネットワークへの対応

EIGRP には次に示す 4 つの基本コンポーネントがあります。

- **近接ディスカバリおよび回復**: 直接接続されたネットワーク上の他のルータに関する情報を動的に取得するために、ルータで使用されるプロセスです。ネイバーが到達不能になる場合、または操作不能になった場合、ルータもこの情報を検出する必要があります。近接ディスカバリおよび回復は、サイズの小さな **hello** パケットを定期的送信することにより、わずかなオーバーヘッドで実現されます。**hello** パケットが受信されているかぎり、Cisco ISO ソフトウェアは、ネイバーが有効に機能していると学習します。このように判別された場合、近接ルータはルーティング情報を交換できます。
- **信頼できるトランスポート プロトコル**: EIGRP パケットをすべてのネイバーに確実に、順序どおりに配信します。マルチキャストおよびユニキャスト パケットが混在する送信もサポートされます。EIGRP パケットには確実に送信する必要があるものと、そうでないものがあります。効率を高めるために、必要な場合だけ信頼性が確保されます。たとえば、マルチキャスト機能があるマルチアクセス ネットワーク (イーサネットなど) では、すべてのネイバーにそれぞれ **hello** パケットを確実に送信する必要はありません。したがって、EIGRP はパケットへの確認応答が不要であることを知らせる、レシーバー宛の情報をパケットに格納し、単一のマルチキャスト **hello** を送信します。他のタイプのパケット (アップデートなど) の場合は、確認応答 (ACK パケット) を要求します。信頼性の高い伝送であれば、ペンディング中の未確認応答パケットがある場合、マルチキャスト パケットを迅速に送信できます。このため、リンク速度が変化する場合でも、コンバージェンス時間を短く保つことができます。
- **DUAL 有限状態マシン**: すべてのルート計算に関する決定プロセスを統合し、すべてのネイバーによってアドバタイズされたすべてのルートをトラッキングします。DUAL は距離情報 (メトリックともいう) を使用して、効率的な、ループのないパスを選択し、さらに DUAL は適切な後継ルータに基づいて、ルーティング テーブルに挿入するルートを選択します。後継ルータは、宛先への最小コスト パス (ルーティング ループに関連しないことが保証されている) を持つ、パケット転送に使用される近接ルータです。適切な後継ルータが存在しなくても、宛先にアドバタイズするネイバーが存在する場合は再計算が行われ、この結果、新しい後継ルータが決定されます。ルートの再計算に要する時間によって、コンバージェンス時間が変わります。再計算はプロセッサに負荷がかかるため、必要でない場合は、再計算しないようにしてください。トポロジが変更されると、DUAL は適切な後継ルータの有無を調べます。適切な後継ルータが存在する場合は、それらを探して使用し、不要な再計算を回避します。
- **プロトコル依存モジュール**: ネットワーク レイヤ プロトコル特有の作業を行います。たとえば、IP EIGRP モジュールは、IP でカプセル化された EIGRP パケットを送受信します。このモジュールは、EIGRP パケットを解析し、受信した新しい情報を DUAL に通知する作業を行います。EIGRP は DUAL にルーティング決定を行うように要求しますが、結果は IP ルーティング テーブルに格納されます。EIGRP は、他の IP ルーティング プロトコルによって取得したルートの再配信も行います。

ここでは、次の設定情報について説明します。

- 「EIGRP のデフォルト設定」 (P.38-40)
- 「基本的な EIGRP パラメータの設定」 (P.38-42)
- 「EIGRP インターフェイスの設定」 (P.38-43)
- 「EIGRP ルート認証の設定」 (P.38-44)
- 「EIGRP スタブ ルーティングの設定」 (P.38-45)
- 「EIGRP のモニタおよびメンテナンス」 (P.38-46)



(注) EIGRP をイネーブルにするには、スタック マスター上で IP サービス イメージが稼動している必要があります。

EIGRP のデフォルト設定

表 38-7 に、EIGRP のデフォルト設定を示します。

表 38-7 EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。クラスフル ネットワーク境界を通過するとき、この境界にサブプレフィクスがサマライズされます。
デフォルト情報	再配信中は外部ルートが許可され、EIGRP プロセス間でデフォルト情報が渡されます。
デフォルト メトリック	デフォルト メトリックなしで再配信できるのは、接続されたルートおよびインターフェイスのスタティック ルートだけです。デフォルト メトリックは次のとおりです。 <ul style="list-style-type: none"> 帯域幅：0 kbps 以上 遅延 (10 マイクロ秒)：0 または 39.1 ナノ秒の倍数である任意の正の数値 信頼性：0 ~ 255 の任意の数値 (255 の場合は信頼性が 100%) 負荷：0 ~ 255 の数値で表される有効帯域幅 (255 の場合は 100% の負荷) Maximum Transmission Unit (MTU; 最大伝送ユニット)：バイトで表されたルートの MTU サイズ (0 または任意の正の整数)
距離	内部距離：90 外部距離：170
EIGRP の近接関係変更ログ	ディセーブル。隣接関係の変更はロギングされません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅比率	50%
IP hello 間隔	低速の Nonbroadcast Multiaccess (NBMA; 非ブロードキャスト マルチアクセス) ネットワークの場合：60 秒、それ以外のネットワークの場合：5 秒
IP ホールドタイム	低速の NBMA ネットワークの場合：180 秒、それ以外のネットワークの場合：15 秒
IP スプリットホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリック ウェイト	tos : 0. k1 および k3 : 1. k2, k4, および k5 : 0。
ネットワーク	指定なし

表 38-7 EIGRP のデフォルト設定 (続き)

機能	デフォルト設定
NSF ¹ 認識	IP サービス イメージが稼動しているスイッチの場合、イネーブル。 レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、近接する NSF 対応ルータからのパケットを転送し続けることができます。
NSF 機能	ディセーブル (注) Catalyst 3750 スイッチは IPv4 の EIGRP NSF 対応ルーティングをサポートしています。
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップにはメトリック設定なし
トラフィック共有	メトリックの比率に応じて配分
差異	1 (等価コスト ロード バランシング)

1. NSF = Nonstop Forwarding

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにし、ネットワークを関連付ける必要があります。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。インターフェイス ネットワークを指定しないと、どの EIGRP アップデートでもアドバタイズされません。



(注)

ネットワーク上に IGRP 用に設定されているルータがあり、この設定を EIGRP に変更する場合は、IGRP と EIGRP の両方が設定された移行ルータを指定する必要があります。この場合は、この次のセクションに記載されているステップ 1 ~ 3 を実行してください (「[スプリット ホライズンの設定](#)」(P.38-27) も参照)。ルートを自動的に再配信するには、同じ AS 番号を使用する必要があります。

EIGRP Nonstop Forwarding

スイッチ スタックは 2 つのレベルの EIGRP をサポートしています。

- 「[EIGRP NSF 認識](#)」(P.38-41)
- 「[EIGRP NSF 機能](#)」(P.38-42)

EIGRP NSF 認識

EIGRP NSF 認識機能が IP サービス イメージの IPv4 でサポートされています。近接ルータが NSF 対応である場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、近接ルータからパケットを転送し続けます。

この機能をディセーブルにすることはできません。この機能の詳細については、次の URL の『*EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080160010.html

EIGRP NSF 機能

良好なコンバージェンスと、スタック マスター変更後のトラフィック損失を低減させるために、IP サービス イメージで IPv4 の EIGRP NSF 対応ルーティングをサポートしています。EIGRP NSF 対応スタック マスターがリスタートする際、または新規スタック マスターが起動して NSF が再起動する際、スイッチにはネイバーがなく、トポロジ テーブルは空です。スイッチでは、スイッチ スタックに向かうトラフィックを中断せずに、インターフェイスを始動させ、ネイバーを再取得して、トポロジとルーティング テーブルを再構築する必要があります。EIGRP ピア ルータでは、新規スタック マスターから学習したルートを維持し、NSF リスタート プロセスを通じてトラフィックを転送し続けます。

ネイバーによる隣接リセットを避けるために、新規スタック マスターは新規リスタート (RS) ビットを使用して EIGRP パケット ヘッダーにリスタートを表示します。ネイバーがこれを受信すると、ピアリスト内のスタックを同期させてスタックとの隣接関係を維持します。次にネイバーは、NSF 認識を示し新規スタック マスターを援助するように設定された RS ビットとともにトポロジ テーブルをスタック マスターに送信します。

少なくともスタック ピア ネイバーの 1 つが NSF 認識である場合、スタック マスターはアップデートを受信してそのデータベースを再構築します。各 NSF 認識ネイバーは、最後のアップデート パケットで End of Table (EOT) マーカを送信して、テーブル内容の終了を示します。スタック マスターで EOT マーカを受信すると、コンバージェンスを認識し、アップデートの送信を開始します。スタック マスターがすべての EOT マーカをネイバーから受信するか、あるいは NSF コンバージェンス タイマーが切れると、EIGRP によって RIB がコンバージェンスが通知され、トポロジ テーブルがすべての NSF 認識ピアにフラッディングされます。




(注) NSF は、Hot Standby Router Protocol (HSRP) に設定されたインターフェイスをサポートしていません。

EIGRP NSF ルーティングをイネーブルにするには、`nsf` EIGRP ルーティング コンフィギュレーション コマンドを使用します。NSF がデバイスでイネーブルであることを確認するには、`show ip protocol` 特権 EXEC コマンドを使用します。`nsf` コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

基本的な EIGRP パラメータの設定

EIGRP を設定するには、特権 EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外のステップは任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router eigrp autonomous-system number</code>	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号によって他の EIGRP ルータへのルートを特定し、ルーティング情報をタグ付けします。
ステップ 3	<code>nsf</code>	(任意) EIGRP NSF をイネーブルにします。スタック マスターとすべてのピアにこのコマンドを入力します。
ステップ 4	<code>network network-number</code>	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は指定されたネットワーク内のインターフェイスにアップデートを送信します。
ステップ 5	<code>eigrp log-neighbor-changes</code>	(任意) EIGRP 近接関係変更のロギングをイネーブルにし、ルーティング システムの安定性をモニタします。

コマンド	目的
ステップ 6 metric weights <i>tos k1 k2 k3 k4 k5</i>	(任意) EIGRP メトリックを調整します。デフォルト値はほとんどのネットワークで適切に動作するよう入念に設定されていますが、調整することも可能です。  注意 メトリックを設定する作業は複雑です。熟練したネットワーク設計者の指導がない場合は、行わないでください。
ステップ 7 offset list [<i>access-list number name</i>] { in out } <i>offset [type number]</i>	(任意) オフセット リストをルーティング メトリックに適用し、EIGRP によって取得したルートへの着信および発信メトリックを増やします。アクセス リストまたはインターフェイスを使用し、オフセット リストを制限できます。
ステップ 8 no auto-summary	(任意) ネットワークレベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。
ステップ 9 ip summary-address eigrp <i>autonomous-system-number address mask</i>	(任意) サマリー集約を設定します。
ステップ 10 end	特権 EXEC モードに戻ります。
ステップ 11 show ip protocols	設定を確認します。
ステップ 12 show ip protocols	設定を確認します。 NSF 認識の場合、出力に次のように表示されます。 *** IP Routing is NSF aware *** EIGRP NSF enabled
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。


EIGRP インターフェイスの設定

インターフェイスごとに、他の EIGRP パラメータを任意で設定できます。

EIGRP インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface <i>interface-id</i>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3 ip bandwidth-percent eigrp <i>percent</i>	(任意) インターフェイスで EIGRP が使用できる帯域幅の割合を設定します。デフォルト値は 50% です。
ステップ 4 ip summary-address eigrp <i>autonomous-system-number address mask</i>	(任意) 指定されたインターフェイスのサマリー集約アドレスを設定します (auto-summary がイネーブルの場合は、通常設定する必要はありません)。

EIGRP の設定

	コマンド	目的
ステップ 5	<code>ip hello-interval eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスの hello タイム インターバルを変更します。範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルトは 60 秒、その他のすべてのネットワークでは 5 秒です。
ステップ 6	<code>ip hold-time eigrp autonomous-system-number seconds</code>	(任意) EIGRP ルーティング プロセスのホールド タイム インターバルを変更します。範囲は 1 ~ 65535 秒です。低速 NBMA ネットワークの場合のデフォルトは 180 秒、その他のすべてのネットワークでは 15 秒です。  注意 ホールド タイムを調整する前に、シスコのテクニカル サポートにお問い合わせください。
ステップ 7	<code>no ip split-horizon eigrp autonomous-system-number</code>	(任意) スプリット ホライズンをディセーブルにし、ルート情報が情報元インターフェイスからルータによってアドバタイズされるようにします。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show ip eigrp interface</code>	EIGRP がアクティブであるインターフェイス、およびそれらのインターフェイスに関連する EIGRP の情報を表示します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

EIGRP ルート認証の設定

EIGRP ルート認証を行うと、EIGRP ルーティング プロトコルからのルーティング アップデートに関する MD5 認証が可能になり、承認されていない送信元から無許可または問題のあるルーティング メッセージを受け取ることがなくなります。

認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	<code>ip authentication mode eigrp autonomous-system md5</code>	IP EIGRP パケットの MD5 認証をイネーブルにします。
ステップ 4	<code>ip authentication key-chain eigrp autonomous-system key-chain</code>	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	<code>key chain name-of-chain</code>	キー チェーンを識別し、キーチェーン コンフィギュレーション モードを開始します。ステップ 4 で設定した名前を指定します。
ステップ 7	<code>key number</code>	キーチェーン コンフィギュレーション モードで、鍵番号を識別します。
ステップ 8	<code>key-string text</code>	キーチェーン コンフィギュレーション モードで、キー スtring を識別します。
ステップ 9	<code>accept-lifetime start-time {infinite end-time duration seconds}</code>	(任意) 鍵を受信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトはデフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および duration は infinite です。
ステップ 10	<code>send-lifetime start-time {infinite end-time duration seconds}</code>	(任意) 鍵を送信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトはデフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および duration は infinite です。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show key chain</code>	認証鍵情報を表示します。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

機能をディセーブルにする場合、または設定をデフォルト値に戻す場合は、上記コマンドの **no** 形式を使用します。

EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能は、すべてのイメージで使用することができ、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。



(注)

IP ベース イメージに含まれているのは EIGRP スタブ ルーティング機能だけです。この機能は、ルーティング テーブルからネットワークの他のスイッチに接続ルートまたは集約ルートをアドバタイズするだけです。スイッチはアクセス レイヤで EIGRP スタブ ルーティングを使用するため、その他の種類のルーティング アドバタイズを使用する必要がなくなります。拡張機能および完全な EIGRP ルーティングのために、スイッチは IP サービス イメージを実行する必要があります。IP ベース イメージが稼働しているスイッチで、マルチ VRF CE と EIGRP スタブ ルーティングを同時に設定しようとする場合、この設定は許可されません。

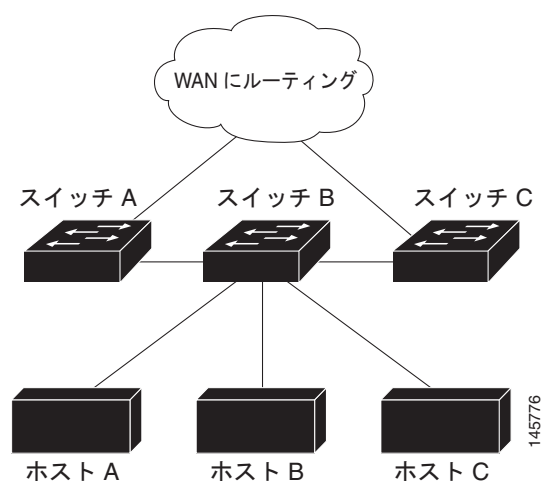
EIGRP スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートだけが EIGRP スタブ ルーティングを設定しているスイッチを通過します。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRP スタブ ルーティングを使用しているときは、EIGRP を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ステータスを通知するパケットを受信するネイバーは、スタブ ルータのクエリーを実行せず、スタブ ピアを有するルータはそのピアのクエリーを実行しません。スタブ ルータは、分散ルータに依存してすべてのピアに適切なアップデートを送信します。

図 38-4 では、スイッチ B が EIGRP スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A および C にアドバタイズします。スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（その逆も同様）。

図 38-4 EIGRP スタブ ルータ設定



(注)

eigrp stub ルータ コンフィギュレーション コマンドを入力したあと、**eigrp stub connected summary** コマンドだけが有効です。Command-Line Interface (CLI; コマンドライン インターフェイス) のヘルプが **receive-only** および **static** キーワードを表示し、これらのキーワードを入力したとしても、IP ベース イメージが稼動しているスイッチは、常に **connected** および **summary** キーワードが設定されているように動作します。

EIGRP スタブ ルーティングの詳細については、『Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols』Release 12.2 の「Configuring EIGRP Stub Routing」を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

EIGRP のモニタおよびメンテナンス

近接テーブルからネイバーを削除できます。さらに、各種 EIGRP ルーティング統計情報を表示することもできます。表 38-8 に、ネイバー削除および統計情報表示用の特権 EXEC コマンドを示しています。表示されるフィールドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

表 38-8 IP EIGRP の clear および show コマンド

コマンド	目的
<code>clear ip eigrp neighbors [if-address interface]</code>	近接テーブルからネイバーを削除します。
<code>show ip eigrp interface [interface] [as number]</code>	EIGRP 用に設定されたインターフェイスの情報を表示します。
<code>show ip eigrp neighbors [type-number]</code>	EIGRP によって検出されたネイバーを表示します。
<code>show ip eigrp topology [autonomous-system-number] [[ip-address] mask]</code>	指定されたプロセスの EIGRP トポロジテーブルを表示します。
<code>show ip eigrp traffic [autonomous-system-number]</code>	すべてまたは特定の EIGRP プロセスの送受信パケット数を表示します。

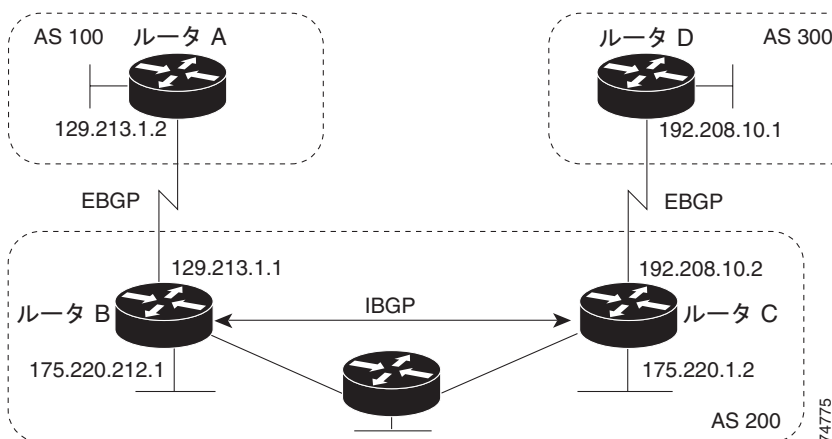
BGP の設定

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) は、Exterior Gateway Protocol (EGP; 外部ゲートウェイ プロトコル) です。Autonomous System (AS; 自律システム) 間で、ループの発生しないルーティング情報交換を保証するドメイン間ルーティング システムを設定するために使用されます。AS は、同じ管理下で動作して RIP や OSPF などの IGP を境界内で実行し、EGP を使用して相互接続されるルータで構成されます。BGP バージョン 4 は、インターネット内でドメイン間ルーティングを行うための標準 EGP です。このプロトコルは、RFC 1163、1267、および 1771 で定義されています。RIP の詳細については、Cisco Press 発行の『*Internet Routing Architectures*』および、『*Cisco IP and IP Routing Configuration Guide*』の「Configuring BGP」の章を参照してください。この資料には、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] からアクセスできます。

BGP コマンドおよびキーワードの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*』 Release 12.2 の「IP Routing Protocols」を参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 D 「Cisco IOS Release 12.2(52)SE でサポートされていないコマンド」を参照してください。

BGP アップデートを交換する場合、同じ AS に属するルータは *Internal BGP* (IBGP) を実行し、異なる AS に属するルータは *External BGP* (EBGP) を実行します。大部分のコンフィギュレーション コマンドは、EBGP と IBGP で同じですが、ルーティング アップデートが AS 間で交換されるか (EBGP)、または AS 内で交換されるか (IBGP) という点で異なります。図 38-5 に、EBGP と IBGP の両方が稼動するネットワークを示します。

図 38-5 EBGP、IBGP、および複数の AS



外部 AS と情報を交換する前に、BGP は AS 内のルータ間で内部 BGP ピアリングを定義し、IGRP や OSPF など AS 内で稼動する IGP に BGP ルーティング情報を再配信して、AS 内のネットワークに到達することを確認します。

BGP ルーティング プロセスを実行するルータは、通常 BGP スピーカーと呼ばれます。BGP はトランスポート プロトコルとして TCP を使用します（特にポート 179）。ルーティング情報を交換するため相互に TCP 接続された 2 つの BGP スピーカーを、ピアまたはネイバーと呼びます。図 38-5 では、ルータ A と B、ルータ B と C、およびルータ C と D がそれぞれ BGP ピアです。ルーティング情報は、宛先ネットワークへの完全パスを示す一連の AS 番号です。BGP はこの情報を使用し、ループのない AS マップを作成します。

このネットワークの特徴は次のとおりです。

- ルータ A および B では EBGP が、ルータ B および C では IBGP が稼動しています。EBGP ピアは直接接続されていますが、IBGP ピアは直接接続されていないことに注意してください。IGP が稼動し、2 つのネイバーが相互に到達する限り、IBGP ピアを直接接続する必要はありません。
- AS 内のすべての BGP スピーカーは、相互にピア関係を確立する必要があります。つまり、AS 内の BGP スピーカーは、論理的な完全メッシュ型に接続する必要があります。BGP4 は、論理的な完全メッシュに関する要求を軽減する 2 つの技術（*連合*および*ルート リフレクタ*）を提供します。
- AS 200 は AS 100 および AS 300 の中継 AS です。つまり、AS 200 は AS 100 と AS 300 間でパケットを転送するために使用されます。

BGP ピアは完全な BGP ルーティング テーブルを最初に交換し、差分更新だけを送信します。BGP ピアはキープアライブ メッセージ（接続が有効であることを確認）、および通知メッセージ（エラーまたは特殊条件に応答）を交換することもできます。

BGP の場合、各ルートはネットワーク番号、情報が通過した AS のリスト（AS パス）、および他のパス アトリビュートリストで構成されます。BGP システムの主な機能は、AS パスのリストに関する情報など、ネットワークの到達可能性情報を他の BGP システムと交換することです。この情報は、AS が接続されているかどうかを判別したり、ルーティング ループをブルーニングしたり、AS レベル ポリシー判断を行うために使用できます。

Cisco IOS が稼動しているルータまたはスイッチが IBGP ルートを選択または使用するの、ネクストホップルータで使用可能なルートがあり、IGP から同期信号を受信している（IGP 同期がディセーブルの場合は除く）場合です。複数のルートが使用可能な場合、BGP はアトリビュート値に基づいてパスを選択します。BGP アトリビュートの詳細については、「[BGP 判断アトリビュートの設定](#)」

(P.38-56) を参照してください。

BGP バージョン 4 では Classless Interdomain Routing (CIDR) がサポートされているため、集約ルートを作成してスーパーネットを構築し、ルーティング テーブルのサイズを削減できます。CIDR は、BGP 内部のネットワーク クラスの概念をエミュレートし、IP プレフィックスのアドバタイズメントをサポートします。

ここでは、次の設定情報について説明します。

- 「BGP のデフォルト設定」 (P.38-49)
- 「BGP ルーティングのイネーブル化」 (P.38-52)
- 「ルーティング ポリシー変更の管理」 (P.38-55)
- 「BGP 判断アトリビュートの設定」 (P.38-56)
- 「ルート マップによる BGP フィルタリングの設定」 (P.38-58)
- 「ネイバーによる BGP フィルタリングの設定」 (P.38-59)
- 「BGP フィルタリング用のプレフィックス リストの設定」 (P.38-60)
- 「BGP コミュニティ フィルタリングの設定」 (P.38-61)
- 「BGP ネイバーおよびピア グループの設定」 (P.38-63)
- 「集約アドレスの設定」 (P.38-65)
- 「ルーティング ドメイン連合の設定」 (P.38-66)
- 「BGP ルート リフレクタの設定」 (P.38-66)
- 「ルート ダンピング化の設定」 (P.38-67)
- 「BGP のモニタおよびメンテナンス」 (P.38-68)

BGP 設定の詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Routing Protocols」の「Configuring BGP」を参照してください。特定コマンドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocol』 Release 12.2 を参照してください。これらのマニュアルは、Cisco.com ホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References]) にあります。

表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 D 「Cisco IOS Release 12.2(52)SE でサポートされていないコマンド」を参照してください。

BGP のデフォルト設定

表 38-9 に、BGP の基本的なデフォルト設定を示します。すべての特性の詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2 の特定のコマンドを参照してください。

表 38-9 BGP のデフォルト設定

機能	デフォルト設定
集約アドレス	ディセーブル：未定義
AS パス アクセス リスト	未定義
自動サマリー	イネーブル
最適パス	<ul style="list-style-type: none"> • ルータはルートを選択する場合に AS パスを考慮します。外部 BGP ピアからの類似ルートは比較されません。 • ルータ ID の比較：ディセーブル

表 38-9 BGP のデフォルト設定 (続き)

機能	デフォルト設定
BGP コミュニティ リスト	<ul style="list-style-type: none"> 番号：未定義 コミュニティ番号を示す特定の値を許可すると、許可されていないその他すべてのコミュニティ番号は、暗黙の拒否にデフォルト設定されます。 フォーマット：シスコ デフォルト フォーマット (32 ビット番号)
BGP 連合 ID/ピア	<ul style="list-style-type: none"> ID：未設定 ピア：識別なし
BGP 高速外部フォールオーバー	イネーブル
BGP ローカル初期設定	100。指定できる範囲は 0 ~ 4294967295 です (大きな値を推奨)。
BGP ネットワーク	指定なし。バックドア ルートのアドバタイズメントなし。
BGP ルート ダンプング化	デフォルトでディセーブル イネーブルの場合は、次のようになります。 <ul style="list-style-type: none"> 半減期は 15 分 再使用は 750 (10 秒増分) 抑制は 2000 (10 秒増分) 最大抑制時間は半減期の 4 倍 (60 分)
BGP ルータ ID	ループバック インターフェイスに IP アドレスが設定されている場合は、ループバック インターフェイスの IP アドレス、またはルータの物理インターフェイスに対して設定された最大の IP アドレス
デフォルトの情報送信元 (プロトコルまたはネットワーク再配信)	ディセーブル
デフォルト メトリック	自動メトリック変換 (組み込み)
距離	<ul style="list-style-type: none"> 外部ルート管理距離：20 (有効値は 1 ~ 255) 内部ルート管理距離：200 (有効値は 1 ~ 255) ローカル ルート管理距離：200 (有効値は 1 ~ 255)
ディストリビュート リスト	<ul style="list-style-type: none"> 入力 (アップデート中に受信されたネットワークをフィルタリング)：ディセーブル 出力 (アップデート中のネットワークのアドバタイズを抑制)：ディセーブル
内部ルート再配信	ディセーブル
IP プレフィクス リスト	未定義
Multi Exit Discriminator (MED)	<ul style="list-style-type: none"> 常に比較：ディセーブル 異なる AS 内のネイバーからのパスに対して、MED を比較しません。 最適パスの比較：ディセーブル 最悪パスである MED の除外：ディセーブル 決定的な MED 比較：ディセーブル

表 38-9 BGP のデフォルト設定 (続き)

機能	デフォルト設定
ネイバー	<ul style="list-style-type: none"> • アドバタイズメント インターバル：外部ピアの場合は 30 秒、内部ピアの場合は 5 秒 • ロギング変更：イネーブル • 条件付きアドバタイズメント：ディセーブル • デフォルト送信元：ネイバーに送信されるデフォルト ルートはなし • 説明：なし • ディストリビュート リスト：未定義 • 外部 BGP マルチホップ：直接接続されたネイバーだけを許可 • フィルタ リスト：使用しない • 受信したプレフィックスの最大数：制限なし • ネクスト ホップ (BGP ネイバーのネクスト ホップとなるルータ)：ディセーブル • パスワード：ディセーブル • ピア グループ：定義なし。割り当てメンバーなし • プレフィックス リスト：指定なし • リモート AS (ネイバー BGP テーブルへのエントリ追加)：ピア定義なし • プライベート AS 番号の削除：ディセーブル • ルート マップ：ピアへの適用なし • コミュニティ アトリビュート送信：ネイバーへの送信なし • シャットダウンまたはソフト再設定：ディセーブル • タイマー：キープアライブ：60 秒。ホールドタイム：180 秒。 • アップデート送信元：最適ローカル アドレス • バージョン：BGP バージョン 4 • ウェイト：BGP ピアによって学習されたルート：0。ローカル ルータから取得されたルート：32768。
NSF ¹ 認識	<p>ディセーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、近接する NSF 対応ルータからのパケットを転送し続けることができます。</p> <p>(注) NSF 認識は、グレースフル リスタートをイネーブルすることにより、IP サービス イメージが稼働しているスイッチの IPv4 に対してイネーブルにできます。</p>
ルート リフレクタ	未設定
同期化 (BGP および IGP)	イネーブル
テーブル マップ アップデート	ディセーブル
タイマー	キープアライブ：60 秒。ホールドタイム：180 秒。

1. NSF = Nonstop Forwarding

NSF 認識

BGP NSF 認識機能が IP サービス イメージの IPv4 でサポートされます。BGP ルーティングでこの機能をイネーブルにするには、グレースフル リスタートをイネーブルにする必要があります。近接ルータが NSF 対応で、この機能がイネーブルである場合、レイヤ 3 スイッチでは、ルータに障害が発生してプライマリ RP がバックアップ RP によって引き継がれる間、または処理を中断させずにソフトウェア アップグレードを行うためにプライマリ RP を手動でリロードしている間、近接ルータからパケットを転送し続けます。

詳細については、次の URL の『*BGP Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015fed.html

BGP ルーティングのイネーブル化

BGP ルーティングをイネーブルにするには、BGP ルーティング プロセスを確立し、ローカル ネットワークを定義します。BGP はネイバーとの関係を完全に認識する必要があるため、BGP ネイバーも指定する必要があります。

BGP は、内部および外部の 2 種類のネイバーをサポートします。内部ネイバーは同じ AS 内に、外部ネイバーは異なる AS 内にあります。通常の場合、外部ネイバーは相互に隣接し、1 つのサブネットを共有しますが、内部ネイバーは同じ AS 内の任意の場所に存在します。

スイッチではプライベート AS 番号を使用できます。プライベート AS 番号は通常サービス プロバイダーによって割り当てられ、ルートが外部ネイバーにアドバタイズされないシステムに設定されます。プライベート AS 番号の範囲は 64512 ~ 65535 です。AS パスからプライベート AS 番号を削除するように外部ネイバーを設定するには、**neighbor remove-private-as** ルータ コンフィギュレーション コマンドを使用します。この結果、外部ネイバーにアップデートを渡すとき、AS パス内にプライベート AS 番号が含まれている場合は、これらの番号が削除されます。

AS が別の AS からさらに別の AS にトラフィックを渡す場合は、アドバタイズメント対象のルートに矛盾が存在しないことが重要です。BGP がルートをアドバタイズしてから、ネットワーク内のすべてのルータが IGP を通してルートを学習した場合、AS は一部のルータがルーティングできなかったトラフィックを受信することがあります。このような事態を避けるため、BGP は IGP が AS に情報を伝播し、BGP が IGP と同期化されるまで、待機する必要があります。同期化は、デフォルトでイネーブルに設定されています。AS が特定の AS から別の AS にトラフィックを渡さない場合、または AS 内のすべてのルータで BGP が稼働している場合は、同期化をディセーブルにし、IGP 内で伝送されるルート数を少なくして、BGP がより短時間で収束するようにします。



(注) BGP をイネーブルにするには、スタック マスター上で IP サービス イメージが稼働している必要があります。

BGP ルーティングをイネーブルにして BGP ルーティング プロセスを確立し、ネイバーを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip routing</code>	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合に限り必須)。

コマンド	目的
ステップ 3 router bgp <i>autonomous-system</i>	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。指定できる AS 番号は 1 ~ 65535 です。64512 ~ 65535 は、プライベート AS 番号専用です。
ステップ 4 network <i>network-number</i> [mask <i>network-mask</i>] [route-map <i>route-map-name</i>]	この AS に対してローカルとなるようにネットワークを設定し、BGP テーブルにネットワークを格納します。
ステップ 5 neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i>	BGP ネイバー テーブルに設定を追加し、IP アドレスによって識別されるネイバーが、指定された AS に属することを示します。 EBGP の場合、通常ネイバーは直接接続されており、IP アドレスは接続のもう一方の端におけるインターフェイスのアドレスです。 IBGP の場合、IP アドレスにはルータ インターフェイス内の任意のアドレスを指定できます。
ステップ 6 neighbor { <i>ip-address</i> <i>peer-group-name</i> } remove-private-as	(任意) 発信ルーティング アップデート内の AS パスからプライベート AS 番号を削除します。
ステップ 7 no synchronization	(任意) BGP と IGP の同期化をディセーブルにします。
ステップ 8 no auto-summary	(任意) 自動ネットワーク サマライズをディセーブルにします。デフォルトでは、IGP から BGP にサブネットが再配信された場合、ネットワーク ルートだけが BGP テーブルに追加されます。
ステップ 9 bgp fast-external-fallover	(任意) 外部ネイバー間のリンクが切断された場合、BGP セッションを自動的にリセットします。デフォルトで、セッションは即座にリセットされません。
ステップ 10 bgp graceful-restart	(任意) NSF 認識をスイッチでイネーブルにします。NSF 認識はデフォルトではディセーブルです。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show ip bgp network <i>network-number</i> または show ip bgp neighbor	設定を確認します。 NSF 認識 (グレースフル リスタート) がネイバーでイネーブルにされていることを確認します。 スイッチおよびネイバーで NSF 認識がイネーブルである場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised and received</i> スイッチで NSF 認識がイネーブルであり、ネイバーでディセーブルである場合は、次のメッセージが表示されます。 <i>Graceful Restart Capability: advertised</i>
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP AS を削除するには、**no router bgp *autonomous-system*** グローバル コンフィギュレーション コマンドを使用します。BGP テーブルからネットワークを削除するには、**no network *network-number*** ルータ コンフィギュレーション コマンドを使用します。ネイバーを削除するには、**no neighbor {*ip-address* | *peer-group-name*} remote-as *number*** ルータ コンフィギュレーション コマンドを使用します。ネイバーにアップデート内のプライベート AS 番号を追加するには、**no neighbor {*ip-address* | *peer-group-name*} remove-private-as** ルータ コンフィギュレーション コマンドを使用します。同期化を再度イネーブルにするには、**synchronization** ルータ コンフィギュレーション コマンドを使用します。

次に、図 38-5 に示されたルータ上で BGP を設定する例を示します。

ルータ A :

```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

ルータ B :

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

ルータ C :

```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

ルータ D :

```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

BGP ピアが稼動していることを確認するには、**show ip bgp neighbors** 特権 EXEC コマンドを使用します。次に、ルータ A にこのコマンドを実行した場合の出力例を示します。

```
Switch# show ip bgp neighbors
```

```
BGP neighbor is 129.213.1.1, remote AS 200, external link
  BGP version 4, remote router ID 175.220.212.1
  BGP state = established, table version = 3, up for 0:10:59
  Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
  Minimum time between advertisement runs is 30 seconds
  Received 2828 messages, 0 notifications, 0 in queue
  Sent 2826 messages, 0 notifications, 0 in queue
  Connections established 11; dropped 10
```

state = established 以外の情報が出力された場合、ピアは稼動していません。リモート ルータ ID は、ルータ（または最大のループバック インターフェイス）上の最大の IP アドレスです。テーブルが新規情報でアップデートされるたびに、テーブルのバージョン番号は増加します。継続的にテーブルバージョン番号が増加している場合は、ルートがフラッピングし、ルーティング アップデートが絶えず発生しています。

外部プロトコルの場合、**network** ルータ コンフィギュレーション コマンドから IP ネットワークへの参照によって制御されるのは、アドバタイズされるネットワークだけです。これは、**network** コマンドを使用してアップデートの送信先を指定する IGP（EIGRP など）と対照的です。

BGP 設定の詳細については、『*Cisco IOS IP Configuration Guide*』 Release 12.2 の「IP Routing Protocols」を参照してください。特定コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocol*』 Release 12.2 を参照してください。表示されているにもかかわらずスイッチでサポートされない BGP コマンドについては、付録 D 「Cisco IOS Release 12.2(52)SE でサポートされていないコマンド」を参照してください。

ルーティング ポリシー変更の管理

ピアのルーティング ポリシーには、着信または発信ルーティング テーブル アップデートに影響する可能性があるすべての設定が含まれます。BGP ネイバーとして定義された 2 台のルータは、BGP 接続を形成し、ルーティング情報を交換します。このあとで BGP フィルタ、ウェイト、距離、バージョン、またはタイマーを変更する場合、または同様の設定変更を行う場合は、BGP セッションをリセットし、設定の変更を有効にする必要があります。

リセットには、ハードリセットとソフトリセットの 2 つのタイプがあります。事前に設定を行わなくても、ソフトリセットを使用できます。事前設定なしにソフトリセットを使用するには、両方の BGP ピアでソフト ルート リフレッシュ機能がサポートされていなければなりません。この機能は、ピアによって TCP セッションが確立されたときに送信される OPEN メッセージに格納されてアドバタイズされます。ソフトリセットを使用すると、BGP ルータ間でルート リフレッシュ要求およびルーティング情報を動的に交換したり、それぞれの発信ルーティング テーブルをあとで再アドバタイズできます。

- ソフトリセットによってネイバーから着信アップデートが生成された場合、このリセットは *ダイナミック着信ソフトリセット* といいます。
- ソフトリセットによってネイバーに一連のアップデートが送信された場合、このリセットは *発信ソフトリセット* といいます。

ソフト着信リセットが発生すると、新規着信ポリシーが有効になります。ソフト発信リセットが発生すると、BGP セッションがリセットされずに、新規ローカル発信ポリシーが有効になります。発信ポリシーのリセット中に新しい一連のアップデートが送信されると、新規着信ポリシーも有効になる場合があります。

表 38-10 に、ハードリセットとソフトリセットの利点および欠点を示します。

表 38-10 ハードリセットとソフトリセットの利点および欠点

リセットタイプ	利点	欠点
ハードリセット	メモリ オーバーヘッドが発生しません。	ネイバーから提供された BGP、IP、および Forwarding Information Base (FIB; 転送情報ベース) テーブルのプレフィクスが失われます。推奨しません。
発信ソフトリセット	ルーティング テーブル アップデートが設定、保管されません。	着信ルーティング テーブル アップデートがリセットされません。
ダイナミック着信ソフトリセット	BGP セッションおよびキャッシュがクリアされません。 ルーティング テーブル アップデートを保管する必要がなく、メモリ オーバーヘッドが発生しません。	両方の BGP ルータでルート リフレッシュ機能をサポートする必要があります。

BGP ピアがルート リフレッシュ機能をサポートするかどうかを学習して、BGP セッションをリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>show ip bgp neighbors</code>	ネイバーがルート リフレッシュ機能をサポートするかどうかを表示します。サポートされている場合は、ルータに関する次のメッセージが表示されます。 <i>Received route refresh capability from peer.</i>
ステップ 2	<code>clear ip bgp {* address peer-group-name}</code>	指定された接続上でルーティング テーブルをリセットします。 <ul style="list-style-type: none"> すべての接続をリセットする場合は、アスタリスク (*) を入力します。 特定の接続をリセットする場合は、IP アドレスを入力します。 ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 3	<code>clear ip bgp {* address peer-group-name} soft out</code>	(任意) 指定された接続上で着信ルーティング テーブルをリセットするには、発信ソフト リセットを実行します。このコマンドは、ルート リフレッシュがサポートされている場合に使用してください。 <ul style="list-style-type: none"> すべての接続をリセットする場合は、アスタリスク (*) を入力します。 特定の接続をリセットする場合は、IP アドレスを入力します。 ピア グループをリセットする場合は、ピア グループ名を入力します。
ステップ 4	<code>show ip bgp</code> <code>show ip bgp neighbors</code>	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。

BGP 判断アトリビュートの設定

BGP スピーカーが複数の AS から受信したアップデートが、同じ宛先に対して異なるパスを示している場合、BGP スピーカーはその宛先に到達する最適パスを 1 つ選択する必要があります。選択されたパスは BGP ルーティング テーブルに格納され、ネイバーに伝播されます。この判断は、アップデートに格納されているアトリビュート値、および BGP で設定可能な他の要因に基づいて行われます。

BGP ピアはネイバー AS からプレフィクスに対する 2 つの EBGP パスを学習するとき、最適パスを選択して IP ルーティング テーブルに挿入します。BGP マルチパス サポートがイネーブルで、同じネイバー AS から複数の EBGP パスを学習する場合、単一の最適パスの代わりに、複数のパスが IP ルーティング テーブルに格納されます。そのあと、パケット スイッチング中に、複数のパス間でパケット単位または宛先単位のロード バランシングが実行されます。**maximum-paths** ルータ コンフィギュレーション コマンドは、許可されるパス数を制御します。

これらの要因により、BGP が最適パスを選択するためにアトリビュートを評価する順序が決まります。

1. パスで指定されているネクスト ホップが到達不能な場合、このアップデートは削除されます。BGP のネクスト ホップのアトリビュート (ソフトウェアによって自動判別される) は、宛先に到達するために使用されるネクスト ホップの IP アドレスです。EBGP の場合、通常このアドレスは **neighbor remote-as** ルータ コンフィギュレーション コマンドで指定されたネイバーの IP アドレスです。ネクスト ホップの処理をディセーブルにするには、ルート マップまたは **neighbor next-hop-self** ルータ コンフィギュレーション コマンドをネクスト ホップ使用します。
2. 最大ウェイトのパスを推奨します (シスコ独自のパラメータ)。ウェイト アトリビュートはルータにローカルであるため、ルーティング アップデートで伝播されません。デフォルトでは、ルータ送信元のパスに関するウェイト アトリビュートは 32768 で、それ以外のパスのウェイト アトリビュートは 0 です。最大ウェイトのルート を推奨します。ウェイトを設定するには、アクセス リスト、ルート マップ、または **neighbor weight** ルータ コンフィギュレーション コマンドを使用します。

3. ローカル初期設定値が最大のルートを推奨します。ローカル初期設定はルーティング アップデートに含まれ、同じ AS 内のルータ間で交換されます。ローカル初期設定アトリビュートのデフォルト値は 100 です。ローカル初期設定を設定するには、**bgp default local-preference** ルータ コンフィギュレーション コマンドまたはルート マップを使用します。
4. ローカル ルータ上で稼動する BGP から送信されたルートを推奨します。
5. AS パスが最短のルートを推奨します。
6. 送信元タイプが最小のルートを推奨します。内部ルートまたは IGP は、EGP によって学習されたルートよりも小さく、EGP で学習されたルートは、未知の送信元のルートまたは別の方法で学習されたルートよりも小さくなります。
7. 想定されるすべてのルートについてネイバー AS が同じである場合は、MED メトリック アトリビュートが最小のルートを推奨します。MED を設定するには、ルート マップまたは **default-metric** ルータ コンフィギュレーション コマンドを使用します。IBGP ピアに送信されるアップデートには、MED が含まれます。
8. 内部 (IBGP) パスより、外部 (EBGP) パスを推奨します。
9. 最も近い IGP ネイバー (最小の IGP メトリック) を通って到達できるルートを推奨します。ルータは、AS 内の最短の内部パス (BGP のネクスト ホップへの最短パス) を使用し、宛先に到達するためです。
10. 次の条件にすべて該当する場合は、このパスのルートを IP ルーティング テーブルに挿入してください。
 - 最適ルートと目的のルートがともに外部ルートである
 - 最適ルートと目的のルートの両方が、同じネイバー AS からのルートである
 - **maximum-paths** がイネーブルである
11. マルチパスがイネーブルでない場合は、BGP ルータ ID の IP アドレスが最小であるルートを推奨します。通常、ルータ ID はルータ上の最大の IP アドレスまたはループバック (仮想) アドレスですが、実装に依存することがあります。

同じ判断アトリビュートを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 router bgp <i>autonomous-system</i>	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3 bgp best-path as-path ignore	(任意) ルート選択中に AS パス長を無視するようにルータを設定します。
ステップ 4 neighbor {<i>ip-address</i> <i>peer-group-name</i>} next-hop-self	(任意) ネクスト ホップ アドレスの代わりに使用される特定の IP アドレスを入力し、ネイバーへの BGP アップデートに関するネクスト ホップの処理をディセーブルにします。
ステップ 5 neighbor {<i>ip-address</i> <i>peer-group-name</i>} weight <i>weight</i>	(任意) ネイバー接続にウェイトを割り当てます。指定できる値は 0 ~ 65535 です。最大ウェイトのルートを推奨します。別の BGP ピアから学習されたルートのデフォルト ウェイトは 0 です。ローカル ルータから送信されたルートのデフォルト ウェイトは 32768 です。
ステップ 6 default-metric <i>number</i>	(任意) 推奨パスを外部ネイバーに設定するように MED メトリックを設定します。MED を持たないすべてのルータも、この値に設定されます。指定できる範囲は 1 ~ 4294967295 です。最小値を推奨します。

	コマンド	目的
ステップ 7	<code>bgp bestpath med missing-as-worst</code>	(任意) MED がない場合は無限の値が指定されていると見なし、MED 値を持たないパスが最も望ましくないパスになるように、スイッチを設定します。
ステップ 8	<code>bgp always-compare med</code>	(任意) 異なる AS 内のネイバーからのパスに対して、MED を比較するようにスイッチを設定します。デフォルトでは、MED は同じ AS 内のパス間だけで比較されます。
ステップ 9	<code>bgp bestpath med confed</code>	(任意) 連合内の異なるサブ AS によってアドバタイズされたパスから特定のパスを選択する場合に、MED を考慮するようにスイッチを設定します。
ステップ 10	<code>bgp deterministic med</code>	(任意) 同じ AS 内の異なるピアによってアドバタイズされたルートから選択する場合に、MED 変数を考慮するようにスイッチを設定します。
ステップ 11	<code>bgp default local-preference value</code>	(任意) デフォルトのローカル初期設定値を変更します。指定できる範囲は 0 ~ 4294967295 です。デフォルトは 100 です。最大のローカル初期設置値を推奨します。
ステップ 12	<code>maximum-paths number</code>	(任意) IP ルーティング テーブルに追加するパスの数を設定します。デフォルトでは、最適パスだけがルーティング テーブルに追加されます。指定できる範囲は 1 ~ 16 です。複数の値を指定すると、パス間のロード バランシングが可能になります (スイッチ ソフトウェア では最大 32 の等価コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません)。
ステップ 13	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<code>show ip bgp</code> <code>show ip bgp neighbors</code>	ルーティング テーブルおよび BGP ネイバーに関する情報をチェックし、リセットされたことを確認します。
ステップ 15	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ステートに戻すには、このコマンドの **no** 形式を使用します。

ルート マップによる BGP フィルタリングの設定

BGP 内でルート マップを使用すると、ルーティング情報を制御、変更したり、ルーティング ドメイン間でルートを再配信する条件を定義できます。ルート マップの詳細については、「[ルート マップによるルーティング情報の再配信](#)」(P.38-99) を参照してください。各ルート マップには、ルート マップを識別する名前 (マップ タグ) およびオプションのシーケンス番号が付いています。

ルート マップを使用してネクスト ホップ処理をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>route-map map-tag [[permit deny] sequence-number]</code>	ルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3 <code>set ip next-hop ip-address [...ip-address] [peer-address]</code>	(任意) ネクスト ホップ処理をディセーブルにするようにルート マップを設定します。 <ul style="list-style-type: none"> 着信ルート マップの場合は、一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクスト ホップを上書きします。 BGP ピアの発信ルート マップの場合は、ネクスト ホップをローカル ルータのピア アドレスに設定して、ネクスト ホップ計算をディセーブルにします。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show route-map [map-name]</code>	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート マップを削除するには、`no route-map map-tag` コマンドを使用します。ネクスト ホップ処理を再びイネーブルにするには、`no set ip next-hop ip-address` コマンドを使用します。

ネイバーによる BGP フィルタリングの設定

BGP アドバタイズメントをフィルタリングするには、`as-path access-list` グローバル コンフィギュレーション コマンドや `neighbor filter-list` ルータ コンフィギュレーション コマンドなどの AS パス フィルタを使用します。`neighbor distribute-list` ルータ コンフィギュレーション コマンドとアクセス リストを併用することもできます。`distribute-list` フィルタはネットワーク番号に適用されます。`distribute-list` コマンドの詳細については、「[ルーティング アップデートのアドバタイズメントおよび処理の制御](#)」(P.38-108) を参照してください。

ネイバー単位でルート マップを使用すると、アップデートをフィルタリングしたり、各アトリビュートを変更できます。ルート マップは、着信アップデートまたは発信アップデートのいずれかに適用できます。ルート マップを渡すルートだけが、アップデート内で送信または許可されます。着信および発信の両方のアップデートで、AS パス、コミュニティ、およびネットワーク番号に基づくマッチングがサポートされています。AS パスのマッチングには `match as-path access-list` ルート マップ コマンド、コミュニティに基づくマッチングには `match community-list` ルート マップ コマンド、ネットワークに基づくマッチングには `ip access-list` グローバル コンフィギュレーション コマンドが必要です。

ネイバー単位のルート マップを適用するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>router bgp autonomous-system</code>	BGP ルーティング プロセスをイネーブルにして AS 番号を割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 3 <code>neighbor {ip-address peer-group name} distribute-list {access-list-number name} {in out}</code>	(任意) アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。 (注) <code>neighbor prefix-list</code> ルータ コンフィギュレーション コマンドを使用して、アップデートをフィルタリングすることもできますが、両方のコマンドを使用して同じ BGP ピアを設定することはできません。

	コマンド	目的
ステップ 4	neighbor { <i>ip-address</i> <i>peer-group name</i> } route-map <i>map-tag</i> { in out }	(任意) ルート マップを適用し、着信または発信ルートをフィルタリングします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip bgp neighbors	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ネイバーからアクセス リストを削除するには、**no neighbor distribute-list** コマンドを使用します。ネイバーからルート マップを削除するには、**no neighbor route-map map-tag** ルータ コンフィギュレーション コマンドを使用します。

BGP AS パスに基づいて着信および発信の両方のアップデートにアクセス リスト フィルタを指定して、フィルタリングすることもできます。各フィルタは、正規表現に基づくアクセス リストです (正規表現の作成方法については、『Cisco IOS Dial Technologies Command Reference』 Release 12.2 の付録「Regular Expressions」を参照してください)。この方法を使用するには、AS パスのアクセス リストを定義し、特定のネイバーに対して送受信されるアップデートに適用します。

BGP パス フィルタリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip as-path access-list <i>access-list-number</i> { permit deny } <i>as-regular-expressions</i>	BGP 関連アクセス リストを定義します。
ステップ 3	router bgp <i>autonomous-system</i>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4	neighbor { <i>ip-address</i> <i>peer-group name</i> } filter-list { <i>access-list-number</i> <i>name</i> } { in out weight <i>weight</i> }	アクセス リストに基づいて、BGP フィルタを確立します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip bgp neighbors [<i>paths</i> <i>regular-expression</i>]	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP フィルタリング用のプレフィクス リストの設定

neighbor distribute-list ルータ コンフィギュレーション コマンドを含む多数の BGP ルート フィルタリング コマンドでは、アクセス リストの代わりにプレフィクス リストを使用できます。プレフィクス リストを使用すると、大規模リストのロードおよび検索パフォーマンスが改善し、差分更新がサポートされ、CLI (コマンドライン インターフェイス) 設定が簡素化され、柔軟性が増すなどの利点が生じます。

プレフィクス リストによるフィルタリングでは、アクセス リストの照合の場合と同様に、プレフィクス リストに記載されたプレフィクスとルートのプレフィクスが照合されます。一致が存在する場合は、一致したルートが使用されます。プレフィクスが許可されるか、または拒否されるかは、次に示す規則に基づいて決定されます。

- 空のプレフィクス リストはすべてのプレフィクスを許可します。
- 指定されたプレフィクスがプレフィクス リスト内のどのエントリとも一致しない場合は、暗黙の拒否が使用されます。

- 指定されたプレフィクスと一致するエントリがプレフィクス リスト内に複数存在する場合は、シーケンス番号が最小であるプレフィクス リスト エントリが識別されます。

デフォルトでは、シーケンス番号は自動生成され、5 ずつ増分します。シーケンス番号の自動生成をディセーブルにした場合は、エントリごとにシーケンス番号を指定する必要があります。シーケンス番号を指定する場合の増分値に制限はありません。増分値が 1 の場合は、このリストに追加エントリを挿入できません。増分値が大きい場合は、値がなくなることがあります。

コンフィギュレーション エントリを削除する場合は、シーケンス番号を指定する必要はありません。**show** コマンドの出力には、シーケンス番号が含まれます。

コマンド内でプレフィクス リストを使用する場合は、あらかじめプレフィクス リストを設定しておく必要があります。プレフィクス リストを作成したり、プレフィクス リストにエントリを追加するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip prefix-list list-name [seq seq-value] deny permit network/len [ge ge-value] [le le-value]	一致条件のために、アクセスを拒否 (deny) または許可 (permit) するプレフィクス リストを作成します。シーケンス番号を指定することもできます。少なくとも 1 つの permit コマンドまたは deny コマンドを入力する必要があります。 <ul style="list-style-type: none"> network/len は、ネットワーク番号およびネットワーク マスクの長さ (ビット単位) です。 (任意) ge および le の値は、照合するプレフィクス長の範囲を指定します。指定された ge-value および le-value は、次の条件を満たす必要があります。$len < ge-value < le-value < 32$
ステップ 3 ip prefix-list list-name seq seq-value deny permit network/len [ge ge-value] [le le-value]	(任意) プレフィクス リストにエントリを追加し、そのエントリにシーケンス番号を割り当てます。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show ip prefix list [detail summary] name [network/len] [seq seq-num] [longer] [first-match]	プレフィクス リストまたはプレフィクス リスト エントリに関する情報を表示して、設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

プレフィクス リストまたはそのエントリをすべて削除する場合は、**no ip prefix-list list-name** グローバル コンフィギュレーション コマンドを使用します。プレフィクス リストから特定のエントリを削除する場合は、**no ip prefix-list seq seq-value** グローバル コンフィギュレーション コマンドを使用します。シーケンス番号の自動生成をディセーブルにするには **no ip prefix-list sequence number** コマンドを、自動生成を再びイネーブルにするには **ip prefix-list sequence number** コマンドを使用します。プレフィクス リスト エントリのヒット数テーブルをクリアするには、**clear ip prefix-list** 特権 EXEC コマンドを使用します。

BGP コミュニティ フィルタリングの設定

BGP コミュニティ フィルタリングは、COMMUNITIES アトリビュートの値に基づいてルーティング情報の配信を制御する BGP の方法の 1 つです。このアトリビュートによって、宛先はコミュニティにグループ化され、コミュニティに基づいてルーティング判断が適用されます。この方法を使用すると、ルーティング情報の配信制御を目的とする BGP スピーカーの設定が簡単になります。

コミュニティは、共通するいくつかのアトリビュートを共有する宛先のグループです。各宛先は複数のコミュニティに属します。AS 管理者は、宛先が属するコミュニティを定義できます。デフォルトでは、すべての宛先が一般的なインターネット コミュニティに属します。コミュニティは、過渡的でグローバルな、オプションの COMMUNITIES アトリビュート (1 ~ 4294967200) によって識別されます。事前に定義された既知のコミュニティの一部を、次に示します。

- **internet** : このルートをインターネット コミュニティにアドバタイズします。すべてのルータが所属します。
- **no-export** : EBGp ピアにこのルートをアドバタイズしません。
- **no-advertise** : いずれのピア (内部または外部) にもこのルートをアドバタイズしません。
- **local-as** : ローカルな AS 外部のピアにこのルートをアドバタイズしません。

コミュニティに基づき、他のネイバーに許可、送信、配信するルーティング情報を制御できます。BGP スピーカーは、ルートを学習、アドバタイズ、または再配信するときに、ルートのコミュニティを設定、追加、または変更します。ルートを集約すると、作成された集約内の COMMUNITIES アトリビュートに、すべての初期ルートの全コミュニティが含まれます。

コミュニティ リストを使用すると、ルート マップの **match** ステートメントで使用されるコミュニティ グループを作成できます。さらに、アクセス リストの場合と同様、一連のコミュニティ リストを作成することもできます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

コミュニティに基づいて COMMUNITIES アトリビュートおよび **match** コマンドを設定するには、「[ルート マップによるルーティング情報の再配信](#)」(P.38-99) に記載されている **match community-list** および **set community** ルート マップ コンフィギュレーション コマンドを参照してください。

デフォルトでは、COMMUNITIES アトリビュートはネイバーに送信されません。COMMUNITIES アトリビュートが特定の IP アドレスのネイバーに送信されるように指定するには、**neighbor send-community** ルータ コンフィギュレーション コマンドを使用します。

コミュニティ リストを作成、適用するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip community-list community-list-number {permit deny} community-number	コミュニティ リストを作成し、番号を割り当てます。 <ul style="list-style-type: none"> • community-list-number は 1 ~ 99 の整数です。この値は、コミュニティの許可または拒否グループを 1 つまたは複数識別します。 • community-number は、set community ルートマップ コンフィギュレーション コマンドで設定される番号です。
ステップ 3 router bgp autonomous-system	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 4 neighbor {ip-address peer-group name} send-community	この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 5 set comm-list list-num delete	(任意) ルート マップで指定された標準または拡張コミュニティ リストと一致する着信または発信アップデートのコミュニティ アトリビュートから、コミュニティを削除します。
ステップ 6 exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 7 ip bgp-community new-format	(任意) AA:NN のフォーマットで、BGP コミュニティを表示、解析します。 BGP コミュニティは、2 つの部分からなる 2 バイト長フォーマットで表示されます。シスコのデフォルトのコミュニティフォーマットは NNAA です。BGP に関する最新の RFC では、コミュニティは AA:NN の形式をとります。最初の部分は AS 番号で、その次の部分は 2 バイトの数値です。
ステップ 8 end	特権 EXEC モードに戻ります。
ステップ 9 show ip bgp community	設定を確認します。
ステップ 10 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ネイバーおよびピア グループの設定

通常、BGP ネイバーの多くは同じアップデート ポリシー (同じ発信ルート マップ、配信リスト、フィルタ リスト、アップデート送信元など) を使用して設定されます。アップデート ポリシーが同じネイバーをピア グループにまとめると設定が簡単になり、アップデートの効率が高まります。多数のピアを設定した場合は、この方法を推奨します。

BGP ピア グループを設定するには、ピア グループを作成し、そこにオプションを割り当てて、ピア グループ メンバーとしてネイバーを追加します。ピア グループを設定するには、**neighbor** ルータ コンフィギュレーション コマンドを使用します。デフォルトでは、ピア グループ メンバーは **remote-as** (設定されている場合)、**version**、**update-source**、**out-route-map**、**out-filter-list**、**out-dist-list**、**minimum-advertisement-interval**、**next-hop-self** など、ピア グループの設定オプションをすべて継承します。すべてのピア グループ メンバーは、ピア グループに対する変更を継承します。また、発信アップデートに影響しないオプションを無効にするように、メンバーを設定することもできます。

各ネイバーに設定オプションを割り当てるには、ネイバーの IP アドレスを使用し、次に示すルータ コンフィギュレーション コマンドのいずれかを指定します。ピア グループにオプションを割り当てるには、ピア グループ名を使用し、いずれかのコマンドを指定します。**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用すると、すべての設定情報を削除せずに、BGP ピアまたはピア グループをディセーブルにできます。

BGP ピアを設定するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 router bgp autonomous-system	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3 neighbor peer-group-name peer-group	BGP ピア グループを作成します。
ステップ 4 neighbor ip-address peer-group peer-group-name	BGP ネイバーをピア グループのメンバーにします。
ステップ 5 neighbor {ip-address peer-group-name} remote-as number	BGP ネイバーを指定します。 remote-as number を使用してピア グループが設定されていない場合は、このコマンドを使用し、EBGP ネイバーを含むピア グループを作成します。指定できる範囲は 1 ~ 65535 です。
ステップ 6 neighbor {ip-address peer-group-name} description text	(任意) ネイバーに記述子を関連付けます。

■ BGP の設定

	コマンド	目的
ステップ 7	neighbor { <i>ip-address</i> <i>peer-group-name</i> } default-originate [<i>route-map map-name</i>]	(任意) BGP スピーカー (ローカル ルータ) にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。
ステップ 8	neighbor { <i>ip-address</i> <i>peer-group-name</i> } send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 9	neighbor { <i>ip-address</i> <i>peer-group-name</i> } update-source <i>interface</i>	(任意) IBGP セッションに、TCP 接続に関するすべての操作インターフェイスの使用を許可します。
ステップ 10	neighbor { <i>ip-address</i> <i>peer-group-name</i> } ebgp-multihop	(任意) ネイバーがセグメントに直接接続されていない場合でも、BGP セッションを使用可能にします。マルチホップ ピア アドレスへの唯一のルートがデフォルト ルート (0.0.0.0) の場合、マルチホップ セッションは確立されません。
ステップ 11	neighbor { <i>ip-address</i> <i>peer-group-name</i> } local-as <i>number</i>	(任意) ローカル AS として使用する AS 番号を指定します。指定できる範囲は 1 ~ 65535 です。
ステップ 12	neighbor { <i>ip-address</i> <i>peer-group-name</i> } advertisement-interval <i>seconds</i>	(任意) BGP ルーティング アップデートを送信する最小インターバルを設定します。
ステップ 13	neighbor { <i>ip-address</i> <i>peer-group-name</i> } maximum-prefix <i>maximum</i> [<i>threshold</i>]	(任意) ネイバーから受信できるプレフィクス数を制御します。指定できる範囲は 1 ~ 4294967295 です。 <i>threshold</i> (任意) は、警告メッセージが生成される基準となる最大値 (パーセント) です。デフォルト値は 75% です。
ステップ 14	neighbor { <i>ip-address</i> <i>peer-group-name</i> } next-hop-self	(任意) ネイバー宛の BGP アップデートに関して、ネクストホップでの処理をディセーブルにします。
ステップ 15	neighbor { <i>ip-address</i> <i>peer-group-name</i> } password <i>string</i>	(任意) TCP 接続での MD5 認証を BGP ピアに設定します。両方の BGP ピアに同じパスワードを設定する必要があります。そうしないと、BGP ピア間に接続が作成されません。
ステップ 16	neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>map-name</i> { <i>in</i> <i>out</i> }	(任意) 着信または発信ルートにルート マップを適用します。
ステップ 17	neighbor { <i>ip-address</i> <i>peer-group-name</i> } send-community	(任意) この IP アドレスのネイバーに送信する COMMUNITIES アトリビュートを指定します。
ステップ 18	neighbor { <i>ip-address</i> <i>peer-group-name</i> } timers <i>keepalive holdtime</i>	(任意) ネイバーまたはピア グループ用のタイマーを設定します。 <ul style="list-style-type: none"> <i>keepalive</i> インターバルは、キープアライブ メッセージがピアに送信される間隔です。指定できる範囲は 1 ~ 4294967295 秒です。デフォルトは 60 秒です。 <i>holdtime</i> は、キープアライブ メッセージを受信しなかった場合、ピアが非アクティブと宣言されるまでのインターバルです。指定できる範囲は 1 ~ 4294967295 秒です。デフォルトは 180 秒です。
ステップ 19	neighbor { <i>ip-address</i> <i>peer-group-name</i> } weight <i>weight</i>	(任意) ネイバーからのすべてのルートに関するウェイトを指定します。
ステップ 20	neighbor { <i>ip-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-number</i> <i>name</i> } { <i>in</i> <i>out</i> }	(任意) アクセス リストの指定に従って、ネイバーに対して送受信される BGP ルーティング アップデートをフィルタリングします。
ステップ 21	neighbor { <i>ip-address</i> <i>peer-group-name</i> } filter-list <i>access-list-number</i> { <i>in</i> <i>out</i> weight <i>weight</i> }	(任意) BGP フィルタを確立します。

	コマンド	目的
ステップ 22	neighbor { <i>ip-address</i> <i>peer-group-name</i> } version <i>value</i>	(任意) ネイバーと通信するときに使用する BGP バージョンを指定します。
ステップ 23	neighbor { <i>ip-address</i> <i>peer-group-name</i> } soft-reconfiguration inbound	(任意) 受信したアップデートの保管を開始するようにソフトウェアを設定します。
ステップ 24	end	特権 EXEC モードに戻ります。
ステップ 25	show ip bgp neighbors	設定を確認します。
ステップ 26	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存の BGP ネイバーまたはネイバー ピア グループをディセーブルにするには、**neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。ディセーブル化されている既存のネイバーまたはネイバー ピア グループをイネーブルにするには、**no neighbor shutdown** ルータ コンフィギュレーション コマンドを使用します。

集約アドレスの設定

CIDR を使用すると、集約ルート（またはスーパーネット）を作成して、ルーティング テーブルのサイズを最小化できます。BGP 内に集約ルートを設定するには、集約ルートを BGP に再配信するか、または BGP ルーティング テーブル内に集約エントリを作成します。BGP テーブル内に特定のエントリがさらに 1 つまたは複数存在する場合は、BGP テーブルに集約アドレスが追加されます。

ルーティング テーブル内に集約アドレスを作成するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router bgp <i>autonomous-system</i>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	aggregate-address <i>address mask</i>	BGP ルーティング テーブル内に集約エントリを作成します。集約ルートは AS からのルートとしてアドバタイズされます。情報が失われた可能性があることを示すため、アトミック集約アトリビュートが設定されます。
ステップ 4	aggregate-address <i>address mask as-set</i>	(任意) AS 設定パス情報を生成します。このコマンドは、この前のコマンドと同じ規則に従う集約エントリを作成します。ただし、アドバタイズされるパスは、すべてのパスに含まれる全要素で構成される AS_SET です。多くのパスを集約するときは、このキーワードを使用しないでください。このルートは絶えず取り消され、更新されます。
ステップ 5	aggregate-address <i>address-mask summary-only</i>	(任意) サマリー アドレスだけをアドバタイズします。
ステップ 6	aggregate-address <i>address mask suppress-map</i> <i>map-name</i>	(任意) 選択された、より具体的なルートを抑制します。
ステップ 7	aggregate-address <i>address mask advertise-map</i> <i>map-name</i>	(任意) ルート マップによって指定された設定に基づいて、集約を生成します。
ステップ 8	aggregate-address <i>address mask attribute-map</i> <i>map-name</i>	(任意) ルート マップで指定されたアトリビュートを持つ集約を生成します。
ステップ 9	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 10	<code>show ip bgp neighbors [advertised-routes]</code>	設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

集約エントリを削除するには、`no aggregate-address address mask` ルータ コンフィギュレーション コマンドを使用します。オプションをデフォルト値に戻すには、キーワードを指定してコマンドを使用します。

ルーティング ドメイン連合の設定

IBGP メッシュを削減する方法の 1 つは、AS を複数のサブ AS に分割して、単一の AS として認識される単一の連合にグループ化することです。各 AS は内部で完全にメッシュ化されていて、同じ連合内の他の AS との間には数本の接続があります。異なる AS 内にあるピアでは EBGP セッションが使用されますが、ルーティング情報は IBGP ピアと同様な方法で交換されます。特に、ネクスト ホップ、MED、およびローカル初期設定情報が維持されるため、すべての AS で単一の IGP を使用できます。

BGP 連合を設定するには、AS システム グループの AS 番号として機能する連合 ID を指定する必要があります。

BGP 連合を設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bgp confederation identifier autonomous-system</code>	BGP 連合 ID を設定します。
ステップ 4	<code>bgp confederation peers autonomous-system [autonomous-system ...]</code>	連合に属する AS、および特殊な EBGP ピアとして処理する AS を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp neighbor</code> <code>show ip bgp network</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルート リフレクタの設定

BGP では、すべての IBGP スピーカーを完全メッシュ構造にする必要があります。外部ネイバーからルートを受信したルータは、そのルートをすべての内部ネイバーにアドバタイズする必要があります。ルーティング情報のループを防ぐには、すべての IBGP スピーカーを接続する必要があります。内部ネイバーは、内部ネイバーから取得されたルートを他の内部ネイバーに送信しません。

ルート リフレクタを使用すると、取得されたルートをネイバーに渡す場合に他の方法が使用されるため、すべての IBGP スピーカーを完全メッシュ構造にする必要はありません。IBGP ピアをルート リフレクタに設定すると、その IBGP ピアは IBGP によって取得されたルートを一連の IBGP ネイバーに送信するようになります。ルート リフレクタの内部ピアには、クライアント ピアと非クライアント ピア (AS 内の他のすべてのルータ) の 2 つのグループがあります。ルート リフレクタは、これらの 2 つのグループ間でルートを反映させます。ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。非クライアント ピアは相互に完全メッシュ構造にする必要がありますが、クライアント ピアはその必要はありません。クラスタ内のクライアントは、そのクラスタ外の IBGP スピーカーと通信しません。

アドバタイズされたルートを受信したルート リフレクタは、ネイバーに応じて、次のいずれかのアクションを実行します。

- EBGSP スピーカーからのルートですべてのクライアントおよび非クライアント ピアにアドバタイズします。
- 非クライアント ピアからのルートですべてのクライアントにアドバタイズします。
- クライアントからのルートですべてのクライアントおよび非クライアント ピアにアドバタイズします。したがって、クライアントを完全メッシュ構造にする必要はありません。

通常、クライアントのクラスタにはルート リフレクタが 1 つあり、クラスタはルート リフレクタのルータ ID で識別されます。冗長性を高めて、シングル ポイントでの障害を回避するには、クラスタに複数のルート リフレクタを設定する必要があります。このように設定した場合は、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるように、クラスタ内のすべてのルート リフレクタに同じクラスタ ID (4 バイト) を設定する必要があります。クラスタを処理するすべてのルート リフレクタは完全メッシュ構造にし、一連の同一なクライアント ピアおよび非クライアント ピアを設定する必要があります。

ルート リフレクタおよびクライアントを設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system</code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>neighbor ip-address peer-group-name route-reflector-client</code>	ローカル ルータを BGP ルート リフレクタに、指定されたネイバーをクライアントに設定します。
ステップ 4	<code>bgp cluster-id cluster-id</code>	(任意) クラスタに複数のルート リフレクタが存在する場合、クラスタ ID を設定します。
ステップ 5	<code>no bgp client-to-client reflection</code>	(任意) クライアント間のルート反映をディセーブルにします。デフォルトでは、ルート リフレクタ クライアントからのルートは、他のクライアントに反映されます。ただし、クライアントが完全メッシュ構造の場合、ルート リフレクタはルートをクライアントに反映させる必要はありません。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip bgp</code>	設定を確認します。送信元の ID およびクラスタリスト アトリビュートを表示します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート ダンプ化の設定

ルート フラップ ダンプ化は、インターネットワーク内でフラッピング ルートの伝播を最小化するための BGP 機能です。ルートがフラッピングと見なされるのは、ルートが使用可能、使用不可能、使用可能、使用不可能のように、状態が継続的に変化する場合です。ルート ダンプ化がイネーブルの場合は、フラッピングしているルートに *penalty* 値が割り当てられます。ルートの累積ペナルティが設定された制限値に到達すると、ルートが稼働している場合であっても、BGP はルートのアドバタイズメントを抑制します。再使用限度は、ペナルティと比較される設定可能な値です。ペナルティが再使用限度より小さくなると、起動中の抑制されたルートのアドバタイズメントが再開されます。

IBGP によって取得されたルートには、ダンプ化が適用されません。このポリシーにより、IBGP ピアのペナルティが AS 外部のルートよりも大きくなることはありません。

BGP ルート ダンピング化を設定するには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp <i>autonomous-system</i></code>	BGP ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>bgp dampening</code>	BGP ルート ダンピング化をイネーブルにします。
ステップ 4	<code>bgp dampening <i>half-life reuse suppress max-suppress [route-map map]</i></code>	(任意) ルート ダンピング化係数のデフォルト値を変更します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip bgp flap-statistics [{<i>regexp regexp</i>} {<i>filter-list list</i>} {<i>address mask [longer-prefix]</i>}]</code>	(任意) フラッピングしているすべてのパスのフラップをモニタします。ルートの抑制が終了し、安定状態になると、統計情報が削除されます。
ステップ 7	<code>show ip bgp dampened-paths</code>	(任意) 抑制されるまでの時間を含めて、ダンピングされたルートを表示します。
ステップ 8	<code>clear ip bgp flap-statistics [{<i>regexp regexp</i>} {<i>filter-list list</i>} {<i>address mask [longer-prefix]</i>}]</code>	(任意) BGP フラップ統計情報を消去して、ルートがダンピング化される可能性を小さくします。
ステップ 9	<code>clear ip bgp dampening</code>	(任意) ルート ダンピング情報を消去して、ルートの抑制を解除します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フラップ ダンピング化をディセーブルにするには、キーワードを指定しないで **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。ダンピング係数をデフォルト値に戻すには、値を指定して **no bgp dampening** ルータ コンフィギュレーション コマンドを使用します。

BGP のモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。この作業は、特定の構造の内容が無効になる場合、または無効である疑いがある場合に必要となります。

BGP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。さらに、リソースの利用率を取得したり、ネットワーク問題を解決するための情報を使用することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のルーティングパスを検出することもできます。

表 38-8 に、BGP を消去および表示するために使用する特権 EXEC コマンドを示しています。画面に表示されるフィールドについては、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセス可能です。

表 38-11 IP BGP の clear および show コマンド

コマンド	目的
<code>clear ip bgp <i>address</i></code>	特定の BGP 接続をリセットします。
<code>clear ip bgp *</code>	すべての BGP 接続をリセットします。
<code>clear ip bgp peer-group <i>tag</i></code>	BGP ピア グループのすべてのメンバーを削除します。

表 38-11 IP BGP の clear および show コマンド (続き)

コマンド	目的
<code>show ip bgp prefix</code>	プレフィクスがアドバタイズされるピア グループ、またはピアグループに含まれないピアを表示します。ネクスト ホップやローカルプレフィクスなどのプレフィクス アトリビュートも表示されます。
<code>show ip bgp cidr-only</code>	サブネットおよびスーパーネット ネットワーク マスクを含むすべての BGP ルートを表示します。
<code>show ip bgp community [community-number] [exact]</code>	指定されたコミュニティに属するルートを表示します。
<code>show ip bgp community-list community-list-number [exact-match]</code>	コミュニティ リストで許可されたルートを表示します。
<code>show ip bgp filter-list access-list-number</code>	指定された AS パス アクセス リストによって照合されたルートを表示します。
<code>show ip bgp inconsistent-as</code>	送信元の AS と矛盾するルートを表示します。
<code>show ip bgp regexp regular-expression</code>	コマンドラインに入力された特定の正規表現と一致する AS パスを持つルートを表示します。
<code>show ip bgp</code>	BGP ルーティング テーブルの内容を表示します。
<code>show ip bgp neighbors [address]</code>	各ネイバーとの BGP 接続および TCP 接続に関する詳細情報を表示します。
<code>show ip bgp neighbors [address] [advertised-routes dampened-routes flap-statistics paths regular-expression received-routes routes]</code>	特定の BGP ネイバーから取得されたルートを表示します。
<code>show ip bgp paths</code>	データベース内のすべての BGP パスを表示します。
<code>show ip bgp peer-group [tag] [summary]</code>	BGP ピア グループに関する情報を表示します。
<code>show ip bgp summary</code>	すべての BGP 接続のステータスを表示します。

また、`bgp log-neighbor changes` ルータ コンフィギュレーション コマンドを使用し、BGP ネイバーをリセット、起動、またはダウンさせるときに生成されるメッセージのログギングをイネーブルにすることもできます。

ISO CLNS ルーティングの設定

International Organization for Standardization (ISO; 国際標準化機構) の Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) プロトコルは、Open System Interconnection (OSI; オープン システム インターコネクション) モデルのネットワーク層の標準です。ISO ネットワーク アーキテクチャでのアドレスは、Network Service Access Point (NSAP; ネットワーク サービス アクセス ポイント) および Network Entity Title (NET) と呼ばれます。OSI ネットワーク内の各ノードには、1 つ以上の NET が設定されています。さらに、各ノードには多数の NSAP アドレスがあります。

スイッチで `clns routing` グローバル コンフィギュレーション コマンドを使用してコネクションレス ルーティングをイネーブルにすると、スイッチは転送決定だけを行い、ルーティング関連の機能は実行しません。ダイナミック ルーティングの場合は、ルーティング プロトコルもイネーブルにする必要があります。スイッチは、ISO CLNS ネットワーク用の OSI ルーティング プロトコルに基づく Intermediate System-to-Intermediate System (IS-IS) ダイナミック ルーティング プロトコルをサポートします。

ダイナミックにルーティングを行うときは、IS-IS を使用します。このルーティング プロトコルは、エリアの概念をサポートします。エリア内では、すべてのルータはすべてのシステム ID への到達方法を認識しています。エリア間では、ルータは適切なエリアへの到達方法を認識しています。IS-IS は、ステーションルーティング (エリア内) とエリアルーティング (エリア間) という 2 つのレベルのルーティングをサポートします。

ISO IGRP および IS-IS NSAP のアドレス指定方式の重要な違いは、エリア アドレスの定義に関する部分です。どちらもレベル 1 のルーティング (エリア内のルーティング) にはシステム ID を使用します。一方、エリア ルーティングでのアドレスの指定方法は異なります。ISO IGRP NSAP のアドレスには、ドメイン、エリア、およびシステム ID という 3 つの異なるフィールドがルーティング用に含まれます。IS-IS のアドレスには、単一の連続したエリアフィールド (ドメイン フィールドとエリア フィールドを含みます) およびシステム ID という 2 つのフィールドが含まれます。



(注)

ISO CLNS の詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide』 Release 12.2 を参照してください。この章で使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference』 Release 12.2 を参照するか、IOS コマンドリファレンス マスター インデックスを使用するか、オンラインで検索してください。

IS-IS ダイナミック ルーティングの設定

IS-IS は、ISO のダイナミック ルーティング プロトコルです (ISO 105890 で説明されています)。他のルーティング プロトコルとは異なり、IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく特定のインターフェイスに割り当てる必要があります。マルチエリアの IS-IS 設定構文を使用して、レイヤ 3 のスイッチまたはルータごとに複数の IS-IS ルーティング プロセスを指定できます。その場合、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワーク内のすべてのルータを含む単一のエリアとして構築します。ネットワークの規模が拡大したら、通常、すべてのエリアのすべてのレベル 2 ルータを接続して構成されるバックボーン エリアとしてネットワークを再編成し、これをローカル エリアに接続します。ローカル エリア内では、ルータはすべてのシステム ID への到達方法を認識しています。エリア間では、ルータはバックボーンへの到達方法を認識し、バックボーン ルータは他のエリアへの到達方法を認識しています。

ルータは、ローカル エリア内のルーティング (ステーション ルーティング) を実行するために、レベル 1 の隣接関係を確立します。ルータは、レベル 1 エリア間のルーティング (エリア ルーティング) を実行するために、レベル 2 の隣接関係を確立します。

1 台のシスコ ルータで、最大 29 エリアのルーティングに参加し、バックボーン内のレベル 2 ルーティングを実行できます。一般に、各ルーティング プロセスはエリアに対応します。デフォルトでは、最初に設定されるルーティング プロセスのインスタンスが、レベル 1 とレベル 2 の両方のルーティングを実行します。追加のルータ インスタンスを設定でき、追加インスタンスは自動的にレベル 1 エリアとして扱われます。IS-IS ルーティング プロセスのインスタンスごとに個別にパラメータを設定する必要があります。

IS-IS マルチエリア ルーティングの場合、レベル 2 ルーティングを実行するように設定できるプロセスは 1 つだけですが、各シスコ ユニッツは最大で 29 のレベル 1 エリアを定義できます。いずれかのプロセスでレベル 2 ルーティングを設定した場合、すべての追加プロセスは自動的にレベル 1 として設定されます。レベル 2 ルーティングを設定したプロセスは、同時にレベル 1 ルーティングを実行するように設定できます。レベル 2 ルーティングがルータ インスタンスに必要ない場合は、**is-type** グローバル コンフィギュレーション コマンドを使用してレベル 2 機能を削除します。別のルータ インスタンスをレベル 2 ルータとして設定する場合にも、**is-type** コマンドを使用します。



(注) IS-IS の詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 の「IP Routing Protocols」を参照してください。ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS IP Command Reference』 Release 12.2 を参照してください。

ここでは、IS-IS ルーティングの設定方法について簡単に説明します。次の情報が含まれます。

- 「IS-IS のデフォルト設定」 (P.38-71)
- 「IS-IS ルーティングのイネーブル化」 (P.38-72)
- 「IS-IS グローバル パラメータの設定」 (P.38-74)
- 「IS-IS インターフェイス パラメータの設定」 (P.38-77)

IS-IS のデフォルト設定

表 38-12 に、IS-IS のデフォルト設定を示します。

表 38-12 IS-IS のデフォルト設定

機能	デフォルト設定
Link-State PDU (LSP; リンクステート PDU) エラーの無視	イネーブル。
IS-IS タイプ	従来型の IS-IS : ルータはレベル 1 (ステーション) およびレベル 2 (エリア) の両方のルータとして動作します。 マルチエリア IS-IS : IS-IS ルーティング プロセスの最初のインスタンスは、レベル 1-2 ルータです。それ以外のインスタンスはレベル 1 ルータです。
デフォルト情報送信元	ディセーブル。
IS-IS 隣接関係ステート変更ログ	ディセーブル。
LSP 生成スロットリング タイマー	連続する 2 つの発生間の最大間隔 : 5 秒。 初期 LSP 生成遅延 : 50 ミリ秒。 1 番めと 2 番めの LSP 生成の間のホールド タイム : 5000 ミリ秒。
LSP 最大存続時間 (リフレッシュなし)	LSP パケットが削除されるまでに 1200 秒 (20 分)。
LSP リフレッシュ インターバル	900 秒 (15 分) ごとに LSP リフレッシュを送信。
最大 LSP パケット サイズ	1497 バイト。
NSG 認識 ¹ (Cisco IOS Release 12.2(25)SEG 以降)。	イネーブル レイヤ 3 スイッチでは、ハードウェアやソフトウェアの変更中に、近接する NSF 対応ルータからのパケットを転送し続けることができます。
Partial Route Computation (PRC) スロットリング タイマー	最大 PRC 待機インターバル : 5 秒。 トポロジ変更後の最初の PRC 計算遅延 : 2000 ミリ秒。 1 番めと 2 番めの PRC 計算の間のホールド タイム : 5000 ミリ秒。
パーティション回避	ディセーブル。
パスワード	エリアまたはドメインのパスワードは定義されておらず、認証はディセーブルです。
set-overload-bit	ディセーブル。イネーブルにして、引数を入力しない場合は、過負荷ビットがすぐに設定されて、 no set-overload-bit コマンドを入力するまで設定状態を維持します。

表 38-12 IS-IS のデフォルト設定 (続き)

機能	デフォルト設定
Shortest Path First (SPF) スロットリング タイマー	連続する SPF 間の最大インターバル: 10 秒。 トポロジ変更後の最初の SPF 計算: 5500 ミリ秒。 1 番めと 2 番めの SPF 計算の間のホールドタイム: 5500 ミリ秒。
サマリー アドレス	ディセーブル。

1. NSF = Nonstop Forwarding

NSF 認識

IPv4 に対して統合された IS-IS NSF 認識機能がサポートされています。この機能を使用することにより、NSF 認識である Customer Premises Equipment (CPE; 宅内装置) のルータは、NSF 対応のルータによるパケットの NSF を補助できます。ローカル ルータは NSF を実行しない場合もありますが、NSF を認識することで、近接する NSF 対応ルータのルーティング データベースおよびリンクステート データベースの整合性と正確さを、スイッチオーバー プロセスの間に維持できます。

この機能は自動的にイネーブルになり、設定を行う必要はありません。この機能の詳細については、次の URL の『*Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a00801541c7.s.html

IS-IS ルーティングのイネーブル化

IS-IS をイネーブルにするには、ルーティング プロセスごとに名前と NET を指定します。その後、インターフェイスで IS-IS ルーティングをイネーブルにし、ルーティング プロセスの各インスタンスに対してエリアを指定します。

IS-IS をイネーブルにして、IS-IS ルーティング プロセスの各インスタンスにエリアを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clns routing</code>	スイッチ上で ISO コネクションレス ルーティングをイネーブルに設定します。
ステップ 3	<code>router isis [area tag]</code>	指定したルーティング プロセスの IS-IS ルーティングをイネーブルにし、IS-IS ルーティングのコンフィギュレーション モードを開始します。 (任意) <code>area tag</code> 引数を使用して、IS-IS ルータの割り当て先のエリアを指定します。複数の IS-IS エリアを設定している場合は、値を入力する必要があります。 最初に設定した IS-IS インスタンスは、デフォルトでレベル 1-2 になります。以降のインスタンスは自動的にレベル 1 になります。 <code>is-type</code> グローバル コンフィギュレーション コマンドを使用して、ルーティングのレベルを変更できます。
ステップ 4	<code>net network-entity-title</code>	ルーティング プロセスに対して NET を設定します。マルチエリア IS-IS を設定している場合は、ルーティング プロセスごとに NET を指定します。NET およびアドレスの名前を指定できます。

コマンド	目的
ステップ 5 is-type { level-1 level-1-2 level-2-only }	(任意) ルータは、レベル 1 (ステーション) ルータとして、マルチエリア ルーティングのレベル 2 (エリア) ルータとして、またはその両方 (デフォルト) として動作するように設定できます。 <ul style="list-style-type: none"> • レベル 1 : ステーション ルータとしてのみ動作します。 • レベル 1-2 : ステーション ルータおよびエリア ルータの両方として動作します。 • レベル 2 : エリア ルータとしてのみ動作します。
ステップ 6 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7 interface <i>interface-id</i>	IS-IS をルーティングするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとしてまだ設定されていない場合は、 no switchport コマンドを入力してレイヤ 3 モードにします。
ステップ 8 ip router isis [<i>area tag</i>]	インターフェイスで ISO CLNS に対する IS-IS ルーティングプロセスを設定し、エリア デジグネータをルーティング プロセスに結合します。
ステップ 9 clns router isis [<i>area tag</i>]	インターフェイスで ISO CLNS をイネーブルにします。
ステップ 10 ip address <i>ip-address-mask</i>	インターフェイスの IP アドレスを定義します。いずれか 1 つのインターフェイスでも IS-IS ルーティング用に設定する場合は、IS-IS をイネーブルにするエリア内のすべてのインターフェイスで IP アドレスが必要です。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show isis [<i>area tag</i>] database detail	設定を確認します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IS-IS ルーティングをディセーブルにするには、**no router isis area-tag** ルータ コンフィギュレーション コマンドを使用します。

次に、IP ルーティング プロトコルとして従来型の IS-IS を実行するように 3 つのルータを設定する例を示します。従来型の IS-IS では、すべてのルータが (デフォルトで) レベル 1 およびレベル 2 のルータとして動作します。

ルータ A

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ B

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

ルータ C

```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

IS-IS グローバル パラメータの設定

必要に応じて設定できる IS-IS グローバル パラメータがいくつかあります。

- ルート マップで制御されるデフォルト ルートを設定することで、IS-IS ルーティング ドメインにデフォルト ルートを強制的に適用できます。ルート マップで設定可能な他のフィルタリング オプションを指定することもできます。
- 受信した IS-IS LSP に内部チェックサム エラーがある場合は無視するように、または壊れている LSP を削除するように、ルータを設定できます。このようにすると、LSP の発信側は LSP を再生成します。
- エリアおよびドメインにパスワードを割り当てることができます。
- ルーティング テーブルでサマリー アドレスによって表される集約アドレスを作成できます (ルート サマライズ)。他のルーティング プロトコルから学習されたルートもサマライズできます。サマリーのアドバタイズに使用されるメトリックは、特定のルート全体の中で最小のメトリックです。
- 過負荷ビットを設定できます。
- LSP リフレッシュ インターバル、および LSP がリフレッシュされないでルータのデータベースに残っていることのできる最大時間を設定できます。
- LSP 生成のスロットリング タイマー、SPF 計算、および PRC を設定できます。
- IS-IS の隣接関係のステータスが (アップまたはダウンに) 変化したときにログ メッセージを生成するように、スイッチを設定できます。
- ネットワーク内のリンクの Maximum Transmission Unit (MTU; 最大伝送ユニット) のサイズが 1500 バイト未満の場合、そのような状況でもルーティングが発生するように LSP MTU を小さくすることができます。
- partition avoidance ルータ コンフィギュレーション コマンドは、レベル 1-2 境界ルータ、隣接するレベル 1 ルータ、およびエンド ホストの間の完全な接続が失われたときに、エリアが分割されるのを防ぎます。

IS-IS パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clns routing</code>	スイッチ上で ISO コネクションレス ルーティングをイネーブルに設定します。

	コマンド	目的
ステップ 3	router isis	IS-IS ルーティング プロトコルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	default-information originate [route-map map-name]	(任意) 強制的に IS-IS ルーティング ドメインにデフォルト ルートを適用します。 route-map map-name を入力すると、ルート マップが満たされている場合、ルーティング プロセスはデフォルト ルートを生成します。
ステップ 5	ignore-lsp-errors	(任意) 内部チェックサム エラーのある LSP を、削除するのではなく無視するようにルータを設定します。このコマンドは、デフォルトでイネーブルになります (壊れている LSP は廃棄されます)。壊れている LSP を削除するには、 no ignore-lsp-errors ルータ コンフィギュレーション コマンドを入力します。
ステップ 6	area-password password	(任意) エリア認証パスワードを設定します。パスワードはレベル 1 (ステーションルータ レベル) の LSP に挿入されます。
ステップ 7	domain-password password	(任意) ルーティング ドメイン認証パスワードを設定します。パスワードはレベル 2 (エリアルータ レベル) の LSP に挿入されます。
ステップ 8	summary-address address mask [level-1 level-1-2 level-2]	(任意) 特定のレベルのアドレスのサマリーを作成します。
ステップ 9	set-overload-bit [on-startup { <i>seconds</i> wait-for-bgp }]	(任意) 過負荷ビット (hippity ビット) を設定し、問題のあるルータを他のルータが SPF 計算で無視できるようにします。 <ul style="list-style-type: none"> (任意) on-startup : 起動時にのみ過負荷ビットを設定します。on-startup を指定しないと、過負荷ビットがすぐに設定されて、no set-overload-bit コマンドを入力するまで設定状態を維持します。on-startup を指定する場合は、秒数または wait-for-bgp を入力する必要があります。 seconds : on-startup キーワードを設定すると、過負荷ビットはシステムの起動時に設定されて、この秒数だけ設定状態を維持します。指定できる範囲は 5 ~ 86400 秒です。 wait-for-bgp : on-startup キーワードを設定すると、過負荷ビットはシステムの起動時に設定されて、BGP がコンバージするまで設定状態を維持します。BGP がコンバージする信号 IS-IS ではない場合は、IS-IS は 10 分後に過負荷ビットをオフにします。
ステップ 10	lsp-refresh-interval seconds	(任意) LSP リフレッシュ インターバルを秒単位で設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルトでは、900 秒 (15 分) ごとに LSP リフレッシュが送信されます。
ステップ 11	max-lsp-lifetime seconds	(任意) LSP パケットをリフレッシュしないでルータ データベースに留めておく最大時間を設定します。指定できる範囲は 1 ~ 65535 秒です。デフォルトは 1200 秒 (20 分) です。指定したタイム インターバルの後、LSP パケットは削除されます。
ステップ 12	lsp-gen-interval [level-1 level-2] <i>lsp-max-wait</i> [<i>lsp-initial-wait</i> <i>lsp-second-wait</i>]	(任意) IS-IS LSP 生成スロットリング タイマーを設定します。 <ul style="list-style-type: none"> <i>lsp-max-wait</i> : 連続して生成される 2 つの LSP 間の最大インターバル (秒) です。指定できる範囲は 1 ~ 120 です。デフォルトは 5 です。 <i>lsp-initial-wait</i> : 初期 LSP 生成の遅延 (ミリ秒) です。指定できる範囲は 1 ~ 10000 です。デフォルトは 50 です。 <i>lsp-second-wait</i> : 1 番めと 2 番めの LSP 生成の間のホールドタイム (ミリ秒) です。指定できる範囲は 1 ~ 10000 です。デフォルトは 5000 です。

コマンド	目的
ステップ 13 spf-interval [level-1 level-2] <i>spf-max-wait</i> [<i>spf-initial-wait</i> <i>spf-second-wait</i>]	(任意) IS-IS の SPF スロットリング タイマーを設定します。 <ul style="list-style-type: none"> <i>spf-max-wait</i> : 連続する SFP の間の最大インターバル (秒) です。指定できる範囲は 1 ~ 120 です。デフォルトは 10 です。 <i>spf-initial-wait</i> : トポロジ変更後の最初の SFP 計算 (ミリ秒) です。指定できる範囲は 1 ~ 10000 です。デフォルトは 5500 です。 <i>spf-second-wait</i> : 1 番めと 2 番めの SFP 計算の間のホールドタイム (ミリ秒) です。指定できる範囲は 1 ~ 10000 です。デフォルトは 5500 です。
ステップ 14 prc-interval <i>prc-max-wait</i> [<i>prc-initial-wait</i> <i>prc-second-wait</i>]	(任意) IS-IS の PRC スロットリング タイマーを設定します。 <ul style="list-style-type: none"> <i>prc-max-wait</i> : 連続する 2 つの PRC 計算の間の最大インターバル (秒) です。指定できる範囲は 1 ~ 120 です。デフォルトは 5 です。 <i>prc-initial-wait</i> : トポロジ変更後の最初の PRC 計算の遅延 (ミリ秒) です。指定できる範囲は 1 ~ 10,000 です。デフォルトは 2000 です。 <i>prc-second-wait</i> : 1 番めと 2 番めの PRC 計算の間のホールドタイム (ミリ秒) です。指定できる範囲は 1 ~ 10,000 です。デフォルトは 5000 です。
ステップ 15 log-adjacency-changes [all]	(任意) IS-IS 隣接関係ステータスの変化をログに記録するようにルータを設定します。 all を入力すると、End System-to-Intermediate System PDU や Link State Packet (LSP; リンク ステータス パケット) など、Intermediate System-to-Intermediate System Hellos に関係のないイベントによって生成されるすべての変更が含まれます。
ステップ 16 p-mtu size	(任意) 最大 LSP パケット サイズをバイト単位で指定します。指定できる範囲は 128 ~ 4352 です。デフォルトは 1497 バイトです。 (注) ネットワーク内のいずれかのリンクで小さい MTU サイズが設定されている場合は、ネットワーク内のすべてのルータで LSP MTU サイズを変更する必要があります。
ステップ 17 partition avoidance	(任意) 境界ルータ、隣接するすべてのレベル 1 ルータ、およびエンドホストの間の完全な接続が失われたとき、IS-IS レベル 1-2 境界ルータはレベル 2 バックボーンへのレベル 1 エリアプレフィックスのアドバタイズを停止します。
ステップ 18 end	特権 EXEC モードに戻ります。
ステップ 19 show clns	設定を確認します。
ステップ 20 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ルートの生成をディセーブルにするには、**no default-information originate** ルータ コンフィギュレーション コマンドを使用します。パスワードをディセーブルにするには、**no area-password** または **no domain-password** ルータ コンフィギュレーション コマンドを使用します。LSP MTU の設定をディセーブルにするには、**no lsp mtu** ルータ コンフィギュレーション コマンドを使用します。サマリー アドレス指定、LSP リフレッシュ インターバル、LSP 存続時間、LSP タイマー、SFP タイマー、PRC タイマーをデフォルトの設定に戻すには、コマンドの **no** 形式を使用します。出力フォーマットをディセーブルにするには、**no partition avoidance** ルータ コンフィギュレーション コマンドを使用します。

IS-IS インターフェイス パラメータの設定

必要に応じて、接続されている他のルータとは別個に、特定のインターフェイス固有の IS-IS パラメータを設定できます。ただし、係数やタイム インターバルなどの一部の値をデフォルトから変更する場合は、複数のルータおよびインターフェイスでも変更しないと意味がありません。ほとんどのインターフェイス パラメータは、レベル 1、レベル 2、または両方に対して設定できます。

設定できるインターフェイス レベル パラメータの一部を次に示します。

- インターフェイスのデフォルト メトリック。IS-IS メトリックの値として使用され、Quality of Service (QoS) ルーティングが実行されていないときに割り当てられます。
- hello インターバル (インターフェイスで送信される hello パケット間の時間の長さ)、または IS-IS hello パケットで送信されるホールド タイムを決定するためにインターフェイスで使用されるデフォルトの hello パケット係数。ホールド タイムにより、ネイバーがネイバー ダウンを宣言する前に別の hello パケットを待機する時間の長さが決定されます。これにより、障害リンクまたはネイバーが検出されてルートを再計算できるまでの時間が決まります。hello パケットが頻繁に失われて、IS-IS 隣接関係の障害が必要以上に発生する環境では、hello 係数を変更してください。hello 係数を大きくし、それに対応して hello インターバルを小さくすることで、リンク障害の検出に必要な時間を延ばすことなく、hello プロトコルの信頼性を高めることができます。
- 他には、次のようなタイム インターバルがあります。
 - Complete Sequence Number PDU (CSNP) インターバル。CSNP は、データベースの同期を維持するために指定されているルータによって送信されます。
 - 再送信インターバル。ポイントツーポイント リンクに対する IS-IS LSP の再送信間の時間です。
 - IS-IS LSP 再送信スロットル インターバル。ポイントツーポイント リンクで IS-IS LSP が再送信される最大速度 (パケット間のミリ秒数) です。このインターバルは、同じ LSP の連続する再送信の間の時間である再送信インターバルとは異なります。
- 代表ルータ選出プライオリティ。マルチアクセス ネットワークで必要な隣接関係の数を減らすことができます。その結果、ルーティング プロトコル トラフィックの量およびトポロジ データベースのサイズが減ります。
- インターフェイス回線タイプ。指定したインターフェイス上のネイバーに適した隣接関係のタイプです。
- インターフェイスのパスワード認証。

IS-IS インターフェイス パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスがレイヤ 3 インターフェイスとしてまだ設定されていない場合は、 <code>no switchport</code> コマンドを入力してレイヤ 3 モードにします。
ステップ 3	<code>isis metric default-metric [level-1 level-2]</code>	(任意) 指定したインターフェイスのメトリック (コスト) を設定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 10 です。レベルを入力しないと、デフォルトとしてレベル 1 およびレベル 2 の両方のルータに適用されます。

コマンド	目的
ステップ 4 isis hello-interval { <i>seconds</i> <i>minimal</i> } [<i>level-1</i> <i>level-2</i>]	(任意) スイッチによって送信される hello パケット間の時間の長さを指定します。デフォルトでは、hello インターバルの <i>seconds</i> の 3 倍の値が、送信される hello パケットの <i>holdtime</i> としてアドバタイズされます。hello インターバルを小さくすると、トポロジ変化の検出は早くなりますが、ルーティングトラフィックが増加します。 <ul style="list-style-type: none"> minimal : システムは、結果のホールドタイムが 1 秒になるように、hello 係数に基づいて hello インターバルを計算します。 seconds : 指定できる範囲は 1 ~ 65535 です。デフォルト値は 10 秒です。
ステップ 5 isis hello-multiplier <i>multiplier</i> [<i>level-1</i> <i>level-2</i>]	(任意) ルータが隣接関係をダウンとして宣言するためにネイバーが失う必要のある、IS-IS hello パケットの数を指定します。指定できる範囲は 3 ~ 1000 です。デフォルト値は 3 です。hello-multiplier を小さくするほどコンバージェンスは速くなりますが、ルーティングが不安定になる可能性があります。
ステップ 6 isis csnp-interval <i>seconds</i> [<i>level-1</i> <i>level-2</i>]	(任意) インターフェイスに対する IS-IS の CSNP インターバルを設定します。指定できる範囲は 0 ~ 65535 です。デフォルト値は 10 秒です。
ステップ 7 isis retransmit-interval <i>seconds</i>	(任意) ポイントツーポイントリンクに対する IS-IS LSP の再送信間の秒数を設定します。ネットワーク上の任意の 2 ルータ間で予想される往復遅延より大きい整数を指定する必要があります。指定できる範囲は 0 ~ 65535 です。デフォルト値は 5 秒です。
ステップ 8 isis retransmit-throttle-interval <i>milliseconds</i>	(任意) IS-IS LSP 再送信スロットルインターバルを設定します。これは、IS-IS LSP がポイントツーポイントリンクで再送信される最大速度 (パケット間のミリ秒数) です。指定できる範囲は 0 ~ 65535 です。デフォルトは、 isis lsp-interval コマンドによって決定されます。
ステップ 9 isis priority <i>value</i> [<i>level-1</i> <i>level-2</i>]	(任意) 代表ルータ選出に使用するプライオリティを設定します。指定できる範囲は 0 ~ 127 です。デフォルト値は 64 です。
ステップ 10 isis circuit-type { <i>level-1</i> <i>level-1-2</i> <i>level-2-only</i> }	(任意) 指定したインターフェイス (インターフェイスの回線タイプを指定) のネイバーに適した隣接関係のタイプを設定します。 <ul style="list-style-type: none"> level-1 : このノードとそのネイバーの両方に共通するエリアアドレスが 1 つでもある場合、レベル 1 の隣接関係が確立されます。 level-1-2 : ネイバーもレベル 1 およびレベル 2 の両方として設定されていて、共通のエリアが 1 つでもある場合、レベル 1 および 2 の隣接関係が確立されます。共通のエリアがない場合は、レベル 2 の隣接関係が確立されます。これがデフォルトです。 level 2 : レベル 2 の隣接関係が確立されます。ネイバー ルータがレベル 1 ルータの場合、隣接関係は確立されません。
ステップ 11 isis password <i>password</i> [<i>level-1</i> <i>level-2</i>]	(任意) インターフェイスの認証パスワードを設定します。認証は、デフォルトではディセーブルに設定されています。レベル 1 またはレベル 2 を指定すると、それぞれ、レベル 1 またはレベル 2 のルーティングに対してだけパスワードがイネーブルになります。レベルを指定しないと、デフォルトでレベル 1 およびレベル 2 になります。
ステップ 12 end	特権 EXEC モードに戻ります。
ステップ 13 show clns interface <i>interface-id</i>	設定を確認します。
ステップ 14 copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルトの設定に戻すには、コマンドの **no** 形式を使用します。

ISO IGRP と IS-IS のモニタおよびメンテナンス

CLNS キャッシュのすべての内容を削除したり、特定のネイバーまたはルート情報を削除したりできます。ルーティング テーブル、キャッシュ、データベースの内容など、CLNS または IS-IS の特定の統計情報を表示できます。また、特定のインターフェイス、フィルタ、またはネイバーについての情報も表示できます。

表 38-13 に、ISO CLNS と IS-IS ルーティングを消去および表示するために使用する特権 EXEC コマンドを示します。表示フィールドの詳細については、『Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference』Release 12.2 を参照するか、Cisco IOS コマンドリファレンス マスター インデックスを使用するか、オンラインで検索してください。

表 38-13 ISO CLNS と IS-IS の clear および show コマンド

コマンド	目的
<code>clear clns cache</code>	CLNS ルーティング キャッシュを消去して再初期化します。
<code>clear clns es-neighbors</code>	隣接関係データベースからエンドシステム (ES) のネイバー情報を削除します。
<code>clear clns is-neighbors</code>	隣接関係データベースから中継システム (IS) のネイバー情報を削除します。
<code>clear clns neighbors</code>	隣接関係データベースから CLNS のネイバー情報を削除します。
<code>clear clns route</code>	動的に抽出される CLNS ルーティング情報を削除します。
<code>show clns</code>	CLNS ネットワークに関する情報を表示します。
<code>show clns cache</code>	CLNS ルーティング キャッシュのエントリを表示します。
<code>show clns es-neighbors</code>	ES ネイバー エントリを表示します。関連付けられたエリアを含みます。
<code>show clns filter-expr</code>	フィルタ式を表示します。
<code>show clns filter-set</code>	フィルタ セットを表示します。
<code>show clns interface [interface-id]</code>	各インターフェイスに関する CLNS 固有の情報または ES-IS の情報を表示します。
<code>show clns neighbor</code>	IS-IS ネイバーに関する情報を表示します。
<code>show clns protocol</code>	このルータの各 IS-IS または ISO IGRP ルーティング プロセスに対するプロトコル固有の情報を一覧表示します。
<code>show clns route</code>	このルータが CLNS パケットのルーティング方法を知っているすべての宛先を表示します。
<code>show clns traffic</code>	このルータが検出した CLNS パケットに関する情報を表示します。
<code>show ip route isis</code>	ISIS IP ルーティング テーブルの現在のステートを表示します。
<code>show isis database</code>	IS-IS リンクステート データベースを表示します。
<code>show isis routes</code>	IS-IS レベル 1 ルーティング テーブルを表示します。
<code>show isis spf-log</code>	IS-IS に対する SPF 計算の履歴を表示します。
<code>show isis topology</code>	全エリアで接続されているすべてのルータの一覧を表示します。
<code>show route-map</code>	設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
<code>trace clns destination</code>	ネットワーク内のパケットによって、指定した宛先に対して取得されたパスを検出します。
<code>which-route {nsap-address clns-name}</code>	指定した CLNS の宛先が含まれるルーティング テーブルを表示します。

マルチ VRF CE の設定

Virtual Private Network (VPN; バーチャルプライベートネットワーク) は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマー サイトは、1 つまたは複数のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VPN Routing/Forwarding (VRF) テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

Catalyst 3750 スイッチは、スイッチで IP サービス イメージが稼動中の場合に、Customer Edge (CE; カスタマー エッジ) デバイスの multiple VPN Routing/Forwarding (multi-VRF; マルチ VRF) インスタンスをサポートします (マルチ VRF CE)。サービス プロバイダーは、マルチ VRF CE により、重複する IP アドレスで複数の VPN をサポートできます。IP ベース イメージが稼動しているスイッチでこれを設定しようとする、エラー メッセージが表示されます。IP ベース イメージが稼動しているスイッチで、マルチ VRF CE と EIGRP スタブルーティングを同時に設定することは許可されていません。



(注)

スイッチでは、VPN のサポートのために Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) が使用されません。MPLS VRF に関する詳細については、『Cisco IOS Switching Services Configuration Guide』Release 12.2 を参照してください。これには、Cisco.com のホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセス可能です。

- 「マルチ VRF CE の概要」 (P.38-80)
- 「マルチ VRF CE のデフォルト設定」 (P.38-82)
- 「マルチ VRF CE の設定時の注意事項」 (P.38-83)
- 「VRF の設定」 (P.38-84)
- 「VRF 認識サービスの設定」 (P.38-85)
- 「VPN ルーティング セッションの設定」 (P.38-89)
- 「BGP PE/CE ルーティング セッションの設定」 (P.38-89)
- 「マルチ VRF CE の設定例」 (P.38-90)
- 「マルチ VRF CE ステータスの表示」 (P.38-94)

マルチ VRF CE の概要

マルチ VRF CE は、サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能です。マルチ VRF CE は入力インターフェイスを使用して、さまざまな VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスと各 VRF を関連付けて仮想パケット転送テーブルを形成します。VRF 内のインターフェイスは、イーサネット ポートのように物理的なもの、または VLAN SVI のように論理的なものにもできますが、複数の VRF に属することはできません。



(注)

マルチ VRF CE インターフェイスは、レイヤ 3 インターフェイスである必要があります。

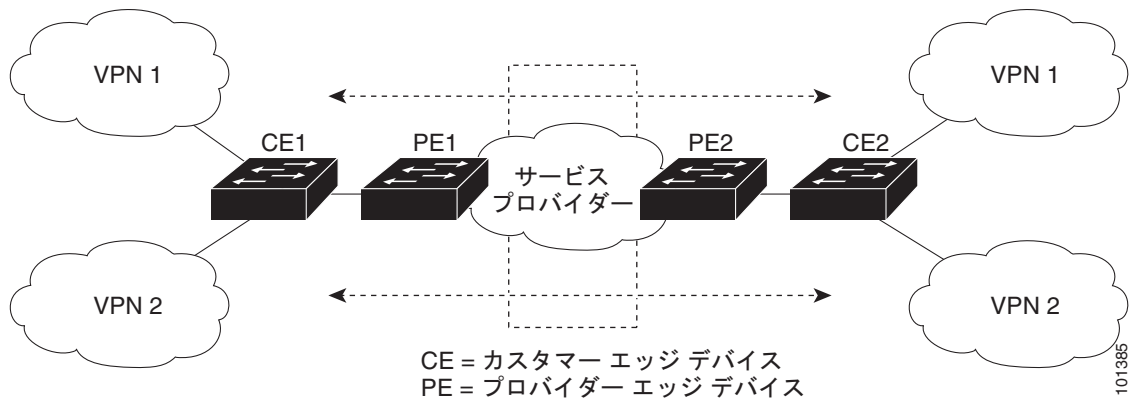
マルチ VRF CE には、次のデバイスが含まれます。

- お客様は、CE デバイスにより、1 つまたは複数の Provider Edge (PE; プロバイダー エッジ) ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカルルートをルータにアドバタイズし、リモート VPN ルートをそこから学習します。Catalyst 3750 スイッチは、CE にすることができます。
- PE ルータは、スタティック ルーティング、または BGP、RIPv2、OSPF、EIGRP などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。PE では、直接接続している VPN の VPN ルートだけを維持すればよく、すべてのサービス プロバイダー VPN ルートを維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- CE デバイ스에 接続していないサービス プロバイダー ネットワークのルータは、プロバイダー ルータやコア ルータになります。

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

図 38-6 は、Catalyst 3750 スイッチを複数の仮想 CE として使用した設定を示しています。このシナリオは、中小企業など、VPN サービスの帯域幅要件の低いお客様に適しています。そのような場合、Catalyst 3750 スイッチではマルチ VRF CE のサポートが必要です。マルチ VRF CE はレイヤ 3 機能なので、VRF のそれぞれのインターフェイスはレイヤ 3 インターフェイスである必要があります。

図 38-6 複数の仮想 CE として機能するスイッチ



CE スイッチは、レイヤ 3 インターフェイスを VRF に追加するコマンドを受信すると、マルチ VRF CE 関連のデータ構造で VLAN ID と Policy Label (PL; ポリシー ラベル) の間に適切なマッピングを設定し、VLAN ID と PL を VLAN データベースに追加します。

マルチ VRF CE を設定すると、レイヤ 3 転送テーブルは、次の 2 つのセクションに概念的に分割されます。

- マルチ VRF CE ルーティング セクションには、さまざまな VPN からのルートが含まれます。
- グローバル ルーティング セクションには、インターネットなど、VPN 以外のネットワークへのルートが含まれます。

さまざまな VRF の VLAN ID はさまざまなポリシー ラベルにマッピングされ、処理中に VRF を区別するために使用されます。レイヤ 3 設定機能では、学習した新しい VPN ルートごとに、入力ポートの VLAN ID を使用してポリシー ラベルを取得し、マルチ VRF CE ルーティング セクションにポリシー ラベルおよび新しいルートを挿入します。ルーテッド ポートからパケットを受信した場合は、ポート 内部 VLAN ID 番号が使用されます。SVI からパケットを受信した場合は、VLAN 番号が使用されま

す。

マルチ VRF CE 対応ネットワークのパケット転送処理は次のとおりです。

- スイッチは、VPN からパケットを受信すると、入力ポリシー ラベル番号に基づいてルーティング テーブルを検索します。ルートが見つかり、スイッチはパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかり、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、通常のルート検索を実行します。ルートが見つかり、パケットを正しい隣接デバイスに転送します。
- CE は、出力 PE からパケットを受信すると、入力ポリシー ラベルを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかり、パケットを VPN 内で転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に関連するレイヤ 3 インターフェイスを指定します。次に、VPN、および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバック ボーンで VPN ルーティング情報を配信する場合は、BGP が望ましいルーティング プロトコルです。マルチ VRF CE ネットワークには、次の 3 つの主要コンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティのその他すべてのメンバーのリスト。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバーに VRF 到達可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワークを介し、全 VPN コミュニティ メンバー間で、全トラフィックを伝送します。

マルチ VRF CE のデフォルト設定

表 38-14 に、VRF のデフォルト設定を示します。

表 38-14 VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	ファスト イーサネット スイッチ：8000。 ギガビット イーサネット スイッチ：12000。
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

マルチ VRF CE の設定時の注意事項



(注)

マルチ VRF CE を使用するには、IP サービス イメージをスイッチにインストールする必要があります。

ネットワークに VRF を設定する場合は、次のことに注意してください。

- マルチ VRF CE を含むスイッチは複数のお客様によって共有され、各お客様には独自のルーティング テーブルがあります。
- お客様は別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- マルチ VRF CE では、複数のお客様が、PE と CE の間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。それぞれのお客様には独自の VLAN があります。
- マルチ VRF CE ではサポートされない MPLS-VRF 機能があります。ラベル交換、LDP 隣接関係、ラベル付きパケットはサポートされません。
- PE ルータの場合、マルチ VRF CE の使用と複数の CE の使用に違いはありません。図 38-6 では、複数の仮想レイヤ 3 インターフェイスがマルチ VRF CE デバイスに接続されています。
- スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。SVI は、アクセス ポートまたはトランク ポートで接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- Catalyst 3750 スイッチは、1 つのグローバル ネットワークおよび最大 26 の VRF をサポートします。
- CE と PE の間では、ほとんどのルーティング プロトコル (BGP、OSPF、RIP、およびスタティック ルーティング) を使用できます。ただし、次の理由から External BGP (EBGP) を使用することを推奨します。
 - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
 - BGP は、さまざまな管理者によって稼動するシステム間でルーティング情報を渡すように設計されています。
 - BGP では、ルートのアトリビュートを CE に簡単に渡すことができます。
- マルチ VRF CE は、パケットのスイッチング レートに影響しません。
- VPN マルチキャストはサポートされません。
- マルチ VRF CE 内のラインレート マルチキャスト転送をサポートしています。
- マルチキャスト VRF は、同一インターフェイス上でプライベート VLAN と共存することができません。
- 最大 1000 のマルチキャスト ルータがサポートされていて、すべての VRF で共有可能です。
- VRF を設定しない場合は、105 のポリシーを設定できます。
- VRF を 1 つでも設定する場合は、41 のポリシーを設定できます。
- 41 より多いポリシーを設定する場合は、VRF を設定できません。

- VRF とプライベート VLAN は相互に排他的です。プライベート VLAN では VRF をイネーブルにすることはできません。同じように、VLAN インターフェイスで VRF が設定されている VLAN では、プライベート VLAN をイネーブルにはできません。
- VRF と Policy-Based Routing (PBR; ポリシーベースルーティング) は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにすることはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、PBR をイネーブルにはできません。
- VRF と Web Cache Communication Protocol (WCCP) は、スイッチ インターフェイス上で相互に排他的です。インターフェイスで WCCP がイネーブルになっているときは、VRF をイネーブルにすることはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、WCCP をイネーブルにはできません。

VRF の設定

1 つまたは複数の VRF を設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティングをイネーブルにします
ステップ 3	ip vrf vrf-name	VRF に名前を付けて VRF コンフィギュレーション モードを開始します。
ステップ 4	rd route-distinguisher	ルート識別子を指定し、VRF テーブルを作成します。AS 番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。
ステップ 5	route-target {export import both} route-target-ext-community	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。 <i>route-target-ext-community</i> は、ステップ 4 で入力した <i>route-distinguisher</i> と同一にする必要があります。
ステップ 6	import map route-map	(任意) ルート マップを VRF に関連付けます。
ステップ 7	interface interface-id	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 8	ip vrf forwarding vrf-name	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show ip vrf [brief detail interfaces] [vrf-name]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf vrf-name** グローバル コンフィギュレーション コマンドを使用します。VRF からあるインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

マルチキャスト VRF の設定

VRF テーブル内にマルチキャストを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの構文と使用方法の詳細については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』 Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	IP ルーティング モードをイネーブルにします。
ステップ 3	ip vrf vrf-name	VRF に名前を付けて VRF コンフィギュレーション モードを開始します。
ステップ 4	rd route-distinguisher	ルート識別子を指定し、VRF テーブルを作成します。AS 番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。
ステップ 5	route-target {export import both} route-target-ext-community	指定した VRF のインポート コミュニティ、エクスポート コミュニティ、またはインポートとエクスポートのルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。 <i>route-target-ext-community</i> は、ステップ 4 で入力した <i>route-distinguisher</i> と同一にする必要があります。
ステップ 6	import map route-map	(任意) ルート マップを VRF に関連付けます。
ステップ 7	ip multicast-routing vrf vrf-name distributed	(任意) VRF テーブルのグローバル マルチキャスト ルーティングをイネーブルにします。
ステップ 8	interface interface-id	VRF に関連付けるレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッドポートまたは SVI に設定できます。
ステップ 9	ip vrf forwarding vrf-name	VRF をレイヤ 3 インターフェイスに関連付けます。
ステップ 10	ip address ip-address mask	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	ip pim sparse-dense mode	VRF 関連レイヤ 3 インターフェイス上で PIM をイネーブルにします。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ip vrf [brief detail interfaces] [vrf-name]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト VRF CE 内でのマルチキャストの設定に関する詳細については、『Cisco IOS IP Configuration Guide』 Release 12.4 を参照してください。

VRF 認識サービスの設定

IP サービスはグローバル インターフェイス上に設定することが可能で、これらのサービスをグローバル ルーティング インスタンス内で実行することができます。IP サービスは、複数のルーティング インスタンスで実行されるように拡張されていて、これが VRF 認識です。システム内に設定された VRF は、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF とは、Cisco IOS で複数のルーティング インスタンスのことです。各プラットフォームには独自のサポート VRF 数の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行することができます。
- ARP エントリは個別の VRF で学習されます。ユーザは、特定の VRF の ARP アドレス解決プロトコル) エントリを表示することができます。

これらのサービスは VRF 認識です。

- ARP
- ping
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)
- Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)
- Syslog
- traceroute
- FTP と TFTP



(注) VRF 認識サービスは Unicast Reverse Path Forwarding (uRPF; ユニキャスト RPF) をサポートしません。

ARP のユーザ インターフェイス

ARP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

コマンド	目的
<code>show ip arp vrf vrf-name</code>	指定された VRF 内の ARP テーブルを表示します。

ping のユーザ インターフェイス

ping の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

コマンド	目的
<code>ping vrf vrf-name ip-host</code>	指定された VRF 内の ARP テーブルを表示します。

SNMP のユーザ インターフェイス

SNMP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server trap authentication vrf	VRF 上のパケットの SNMP トラップをイネーブルにします。
ステップ 3	snmp-server engineID remote <host> vrf <vpn instance> <engine-id string>	スイッチ上のリモート SNMP エンジンの名前を指定します。
ステップ 4	snmp-server host <host> vrf <vpn instance> traps <community>	SNMP トラップ動作の受信側を指定して、SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ 5	snmp-server host <host> vrf <vpn instance> informs <community>	SNMP 情報動作の受信側を指定して、SNMP 情報の送信に使用される VRF テーブルを指定します。
ステップ 6	snmp-server user <user> <group> remote <host> vrf <vpn instance> <security model>	SNMP アクセス用に、VRF 上にあるリモート ホストの SNMP グループにユーザを追加します。
ステップ 7	end	特権 EXEC モードに戻ります。

HSRP のユーザ インターフェイス

VRF の HSRP サポートにより、HSRP 仮想 IP アドレスが確実に正しい IP ルーティング テーブルに追加されます。

HSRP の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『Cisco IOS Switching Services Command Reference』 Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	no switchport	物理インターフェイスの場合、レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します。
ステップ 4	ip vrf forwarding <vrf-name>	インターフェイス上で VRF をイネーブルにします。
ステップ 5	ip address ip address	インターフェイスの IP アドレスを入力します。
ステップ 6	standby 1 ip ip address	HSRP をイネーブルにして、仮想 IP アドレスを設定します。
ステップ 7	end	特権 EXEC モードに戻ります。

Syslog のユーザ インターフェイス

Syslog の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンド リファレンス、および『Cisco IOS Switching Services Command Reference』 Release 12.2 を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging on	ストレージルータ イベント メッセージのロギングをイネーブルにしたり、一時的にディセーブルにしたりします。

	コマンド	目的
ステップ 3	<code>logging host ip address vrf vrf name</code>	ロギングメッセージが送信される syslog サーバのホストアドレスを指定します。
ステップ 4	<code>logging buffered logging buffered size debugging</code>	内部バッファへのメッセージを記録します。
ステップ 5	<code>logging trap debugging</code>	Syslog サーバに送信されるロギングメッセージを制限します。
ステップ 6	<code>logging facility facility</code>	システム ロギングメッセージをロギング ファシリティに送信します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。

traceroute のユーザ インターフェイス

traceroute の VRF 認識サービスを設定するには、特権 EXEC モードで次の手順を実行します。コマンドの完全な構文と使用方法については、このリリースのスイッチのコマンドリファレンス、および『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

	コマンド	目的
	<code>traceroute vrf vrf-name ipaddress</code>	VPN VRF 内の宛先アドレスを検索するために VPN VRF の名前を指定します。

FTP および TFTP のユーザ インターフェイス

FTP と TFTP が VRF 認識とするためには、いくつかの FTP/TFTP CLI を設定する必要があります。たとえば、インターフェイスに添付されている VRF テーブルを使用する場合、E1/0 であれば、CLI `ip [t]ftp source-interface E1/0` を設定して、特定のルーティング テーブルを使用するように [t]ftp に通知します。この例では、VRF テーブルが宛先 IP アドレスを検索するために使用されます。これらの変更には下位互換性があり、既存の動作には影響しません。つまり、VRF がそのインターフェイスに設定されていなくても、送信元インターフェイス CLI を使用してパケットを特定のインターフェイスに送信することができます。

FTP 接続の IP アドレスを指定するには、`ip ftp source-interface show mode` コマンドを使用します。接続が行われているインターフェイスのアドレスを使用するには、`no` 形式のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip ftp source-interface interface-type interface-number</code>	FTP 接続の送信元 IP アドレスを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

TFTP 接続の送信元アドレスとしてインターフェイスの IP アドレスを指定するには、`ip tftp source-interface show mode` コマンドを使用します。デフォルトに戻するには、`no` 形式のコマンドを使用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	<code>ip tftp source-interface interface-type interface-number</code>	TFTP 接続の送信元 IP アドレスを指定します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされている任意のルーティング プロトコル (RIP、OSPF、EIGRP、BGP)、またはスタティック ルーティングで設定できます。ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。



(注) VRF インスタンス内で稼動するように EIGRP ルーティング プロセスを設定するには、**autonomous-system autonomous-system-number** アドレスファミリー コンフィギュレーション モード コマンドを入力して AS 番号を設定する必要があります。

VPN 内で OSPF を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router ospf process-id vrf vrf-name</code>	OSPF ルーティングをイネーブルにして VPN 転送テーブルを指定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>log-adjacency-changes</code>	(任意) 隣接関係ステータスの変更をログします。これがデフォルトのステータスです。
ステップ 4	<code>redistribute bgp autonomous-system-number subnets</code>	BGP ネットワークから OSPF ネットワークに情報を再配信するようにスイッチを設定します。
ステップ 5	<code>network network-number area area-id</code>	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip ospf process-id</code>	OSPF ネットワークの設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf process-id vrf vrf-name** グローバル コンフィギュレーション コマンドを使用します。

BGP PE/CE ルーティング セッションの設定

BGP PE/CE ルーティング セッションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router bgp autonomous-system-number</code>	その他の BGP ルータに AS 番号を渡す BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

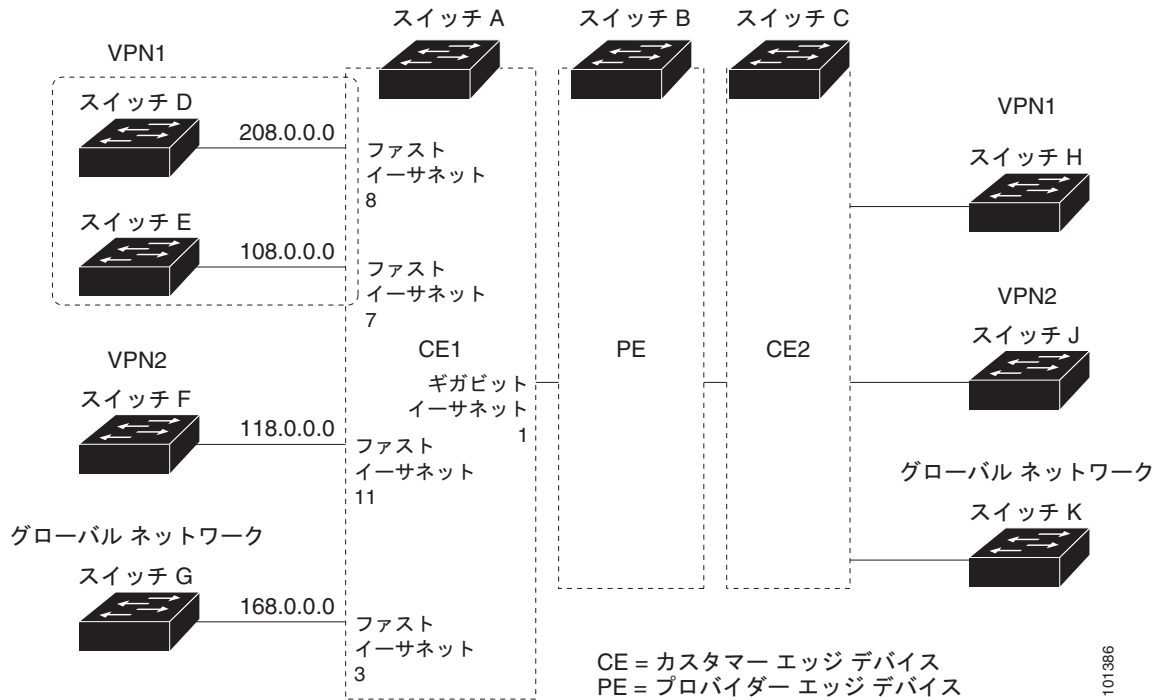
	コマンド	目的
ステップ 3	<code>network network-number mask network-mask</code>	ネットワークとマスクを指定し、BGP の使用を宣言します。
ステップ 4	<code>redistribute ospf process-id match internal</code>	OSPF 内部ルートを再配信するようにスイッチを設定します。
ステップ 5	<code>network network-number area area-id</code>	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	<code>address-family ipv4 vrf vrf-name</code>	PE/CE ルーティング セッションの BGP パラメータを定義し、VRF アドレスファミリ モードを開始します。
ステップ 7	<code>neighbor address remote-as as-number</code>	PE と CE ルータ間の BGP セッションを定義します。
ステップ 8	<code>neighbor address activate</code>	IPv4 アドレス ファミリのアドバタイズメントをアクティブにします。
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>show ip bgp [ipv4] [neighbors]</code>	BGP 設定を確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング プロセスを削除するには、`no router bgp autonomous-system-number` グローバル コンフィギュレーション コマンドを使用します。ルーティング特性を削除するには、コマンドにキーワードを指定してこのコマンドを使用します。

マルチ VRF CE の設定例

図 38-7 は、図 38-6 と同じネットワークの物理接続を簡素化した例です。VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。図のあとに続く出力は、Catalyst 3750 スイッチを CE スイッチ A として設定する例、およびカスタマー スイッチ D と F の VRF 設定を示しています。CE スイッチ C とその他のカスタマー スイッチを設定するコマンドは含まれていませんが、内容は同じです。この例には、PE ルータとして動作する Catalyst 6000 スイッチまたは Catalyst 6500 スイッチのスイッチ A へのトラフィックを設定するコマンドも含まれています。

図 38-7 マルチ VRF CE の設定例



101386

スイッチ A の設定

スイッチ A では、ルーティングをイネーブルにして VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ A のループバックおよび物理インターフェイスを設定します。ギガビットイーサネットポート 1 は PE へのトランク接続です。ファストイーサネットポート 8 と 11 は VPN に接続されます。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

```
Switch(config)# interface fastethernet1/0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit
```

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ A で使用する VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 と 208 は、それぞれスイッチ F とスイッチ D を含む VPN に使用されます。

```
Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit
```

```
Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 と VPN2 で OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf v11
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf v12
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE/PE ルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf v12
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit
```



```
Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ D の設定

スイッチ D は VPN 1 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ F の設定

スイッチ F は VPN 2 に属します。次のコマンドを使用して、スイッチ A への接続を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ B の設定

このコマンドをスイッチ B (PE ルータ) で使用すると、CE デバイス、スイッチ A に対する接続だけが設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
```

```

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitEthernet00/01/01.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitEthernet00/01/01.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end

```

マルチ VRF CE ステータスの表示

マルチ VRF CE の設定とステータスに関する情報を表示するには、表 38-15 の特権 EXEC コマンドを使用します。

表 38-15 マルチ VRF CE 情報を表示するコマンド

コマンド	目的
<code>show ip protocols vrf vrf-name</code>	VRF に関するルーティング プロトコル情報を表示します。
<code>show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]</code>	VRF に関する IP ルーティング テーブル情報を表示します。
<code>show ip vrf [brief detail interfaces] [vrf-name]</code>	定義した VRF インスタンスに関する情報を表示します。

表示される情報の詳細については、『Cisco IOS Switching Services Command Reference』Release 12.2 を参照してください。

プロトコル独立機能の設定

ここでは、IP ルーティング プロトコルに依存しない機能の設定方法について説明します。これらの機能は、IP ベース イメージまたは IP サービス イメージが稼動するスイッチ上で使用できますが、IP ベース イメージ [ジ] 付属のプロトコル関連機能は RIP だけで使用できます。この章の IP ルーティング プロトコル独立コマンドの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』 Release 12.2 の「IP Routing Protocol-Independent Commands」の章を参照してください。このマニュアルには、Cisco.com ホームページ ([Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]) からアクセスできます。

ここでは、次の設定情報について説明します。

- 「dCEF の設定」 (P.38-95)
- 「等価コスト ルーティング パスの個数の設定」 (P.38-97)
- 「スタティック ユニキャスト ルートの設定」 (P.38-97)
- 「デフォルトのルートおよびネットワークの指定」 (P.38-98)
- 「ルート マップによるルーティング情報の再配信」 (P.38-99)
- 「PBR の設定」 (P.38-103)
- 「ルーティング情報のフィルタリング」 (P.38-107)
- 「認証鍵の管理」 (P.38-110)

dCEF の設定

Cisco Express Forwarding (CEF) は、ネットワーク パフォーマンスを最適化するために使用されるレイヤ 3 IP スイッチング技術です。CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。Catalyst 3750 スイッチ スタックでは、ハードウェアはスタックの dCEF を使用します。動的なネットワークでは、ルーティングの変更によって、高速スイッチング キャッシュ エントリが頻繁に無効となります。高速スイッチング キャッシュ エントリが無効になると、トラフィックがルート キャッシュによって高速スイッチングされずに、ルーティング テーブルによってプロセス スイッチングされることがあります。CEF および dCEF は Forwarding Information Base (FIB; 転送情報ベース) 検索テーブルを使用して、宛先ベースの IP パケット スイッチングを実行します。

dCEF の 2 つの主要な構成要素は、分散 FIB と分散隣接テーブルです。

- FIB はルーティング テーブルや情報ベースと同様、IP ルーティング テーブルに転送情報のミラー イメージが保持されます。ネットワーク内でルーティングまたはトポロジが変更されると、IP ルーティング テーブルがアップデートされ、これらの変更が FIB に反映されます。FIB には、IP ルーティング テーブル内の情報に基づいて、ネクスト ホップのアドレス情報が保持されます。FIB にはルーティング テーブル内の既知のルートがすべて格納されているため、CEF はルート キャッシュをメンテナンスする必要がなく、トラフィックのスイッチングがより効率化され、トラフィック パターンの影響も受けません。
- リンク レイヤ上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEF は隣接テーブルを使用し、レイヤ 2 アドレッシング情報を付加します。隣接テーブルには、すべての FIB エントリに対する、レイヤ 2 のネクスト ホップのアドレスが保持されます。

スイッチ スタックは、ギガビット速度の回線レート IP トラフィックを達成するため Application Specific Integrated Circuit (ASIC; 特定用途向け IC) を使用しているため、dCEF 転送はソフトウェア転送パス (CPU により転送されるトラフィック) にだけ適用されます。

デフォルトで、dCEF はグローバルでイネーブルに設定されています。何らかの理由でこれがディセーブルになった場合は、**ip cef distributed** グローバル コンフィギュレーション コマンドを使用し、再度イネーブルに設定できます。

デフォルト設定では、すべてのレイヤ 3 インターフェイスで dCEF がイネーブルです。 **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドを入力すると、ソフトウェアが転送するトラフィックに対して CEF がディセーブルになります。このコマンドは、ハードウェア転送パスには影響しません。CEF をディセーブルにして **debug ip packet detail** 特権 EXEC コマンドを使用すると、ソフトウェア転送トラフィックをデバッグするのに便利です。ソフトウェア転送パス用のインターフェイスで CEF をイネーブルにするには、**ip route-cache cef** インターフェイス コンフィギュレーション コマンドを使用します。


注意

CLI には、インターフェイス上で CEF をディセーブルにする **no ip route-cache cef** インターフェイス コンフィギュレーション コマンドが表示されますが、デバッグ以外の目的でインターフェイス上で dCEF をディセーブルにしないようにしてください。

ディセーブルである dCEF をグローバルにイネーブルにしたり、ソフトウェア転送トラフィックのインターフェイス上でイネーブルにするには、特権 EXEC モードで、次の手順を実行します。

	コマン h	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip cef distributed	CEF の動作をイネーブルにします。
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 4	ip route-cache cef	ソフトウェア転送トラフィック用のインターフェイスで CEF をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip cef	すべてのインターフェイスの CEF ステータスを表示します。
ステップ 7	show cef linecard [slot-number] [detail]	スタック内のすべてのスイッチ、または指定されたスイッチに対して、スタック メンバー別に CEF 関連インターフェイス情報を表示します。 (任意) <i>slot-number</i> には、スタック メンバーのスイッチ番号を入力します。
ステップ 8	show cef interface [interface-id]	すべてのインターフェイスまたは指定されたインターフェイスの詳細な CEF 情報を表示します。
ステップ 9	show adjacency	CEF の隣接テーブル情報を表示します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

等価コスト ルーティング パスの個数の設定

同じネットワークへ向かう同じメトリックのルートが複数ルータに格納されている場合、これらのルートは等価コストを保有していると見なされます。ルーティング テーブルに複数の等価コスト ルートが含まれる場合は、これらをパラレルパスと呼ぶこともあります。ネットワークへの等価コストパスがルータに複数格納されている場合、ルータはこれらを同時に使用できます。パラレルパスを使用すると、パスに障害が発生した場合に冗長性を確保できます。また、使用可能なパスにパケットの負荷を分散し、使用可能な帯域幅を有効利用することもできます。等価コスト ルートは、スタック内の各スイッチでサポートされます。

等価コスト ルートはルータによって自動的に取得、設定されますが、ルーティング テーブルの IP ルーティング プロトコルでサポートされるパラレルパスの最大数は制御可能です。スイッチ ソフトウェアでは最大 32 の等価コスト ルーティングが許可されていますが、スイッチ ハードウェアはルートあたり 17 パス以上は使用しません。

ルーティング テーブルに格納されるパラレルパスのデフォルトの最大数を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>maximum-paths maximum</code>	プロトコル ルーティング テーブルのパラレルパスの最大数を設定します。指定できる範囲は 1 ~ 16 です。ほとんどの IP ルーティング プロトコルでデフォルトは 4 ですが、BGP の場合は 1 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip protocols</code>	<i>Maximum path</i> フィールドの設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト値に戻すには、`no maximum-paths` ルータ コンフィギュレーション コマンドを使用します。

スタティック ユニキャスト ルートの設定

スタティック ユニキャスト ルートは、特定のパスを通過して送信元と宛先間でパケットを送受信するユーザ定義のルートです。ルータが特定の宛先へのルートを構築できない場合、スタティック ルートは重要で、到達不能なすべてのパケットが送信される最終ゲートウェイを指定する場合に有効です。

スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip route prefix mask {address interface} [distance]</code>	スタティック ルートを確立します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip route</code>	設定を確認するため、ルーティング テーブルの現在のステータスを表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

スタティック ルートを削除するには、**no ip route prefix mask {address | interface}** グローバル コンフィギュレーション コマンドを使用します。

ユーザによって削除されるまで、スタティック ルートはスイッチに保持されます。ただし、管理距離の値を割り当て、スタティック ルートをダイナミック ルーティング情報で上書きできます。各ダイナミック ルーティング プロトコルには、デフォルトの管理距離が設定されています (表 38-16 を参照)。ダイナミック ルーティング プロトコルの情報でスタティック ルートを上書きする場合は、スタティック ルートの管理距離がダイナミック プロトコルの管理距離よりも大きな値になるように設定します。

表 38-16 ダイナミック ルーティング プロトコルのデフォルトの管理距離

ルート送信元	デフォルト距離
接続されたインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
EBGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IBGP	200
不明	225

インターフェイスを指し示すスタティック ルートは、RIP、IGRP、およびその他のダイナミック ルーティング プロトコルを通してアドバタイズされます。**redistribute** スタティック ルータ コンフィギュレーション コマンドが、これらのルーティング プロトコルに対して指定されているかどうかは関係ありません。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。ただし、**network** コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute** スタティック コマンドを指定しないかぎり、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。転送ルータのアドレスとして指定されたアドレスへ向かう有効なネクスト ホップがスタティック ルート内に見つからない場合は、IP ルーティング テーブルからそのスタティック ルートも削除されます。

デフォルトのルートおよびネットワークの指定

ルータが他のすべてのネットワークへのルートを学習することはできません。完全なルーティング機能を実現するには、一部のルータをスマート ルータとして使用し、それ以外のルータのデフォルト ルートをスマート ルータ宛に指定します (スマート ルータには、インターネットワーク全体のルーティング テーブル情報が格納されます)。これらのデフォルト ルートは動的に学習されるか、ルータごとに設定されます。ほとんどのダイナミックな内部ルーティング プロトコルには、スマート ルータを使用してデフォルト情報をダイナミックに生成し、他のルータに転送するメカニズムがあります。

指定されたデフォルト ネットワークに直接接続されたインターフェイスがルータに存在する場合は、そのデバイス上で動作するダイナミック ルーティング プロトコルによってデフォルト ルートが生成されます。RIP の場合は、疑似ネットワーク 0.0.0.0 がアドバタイズされます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルト ルートも指定する必要があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを經由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ネットワークへのスタティック ルートをスタティック デフォルト ルートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip default-network network number	デフォルト ネットワークを指定します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip route	最終ゲートウェイで選択されたデフォルト ルートを表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルートを削除するには、**no ip default-network network number** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ルーティング プロトコルによってデフォルト情報を送信するときは、特に設定する必要はありません。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。IGRP ネットワークでは、システムのデフォルト ネットワークの候補が複数存在する場合があります。シスコのルータでは、デフォルト ルートまたは最終ゲートウェイを設定するため、管理距離およびメトリック情報を使用します。

ダイナミックなデフォルト情報がシステムに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。このネットワークが任意の送信元のルーティング テーブルに格納されている場合は、デフォルト ルートの候補としてフラグ付けされます。ルータにデフォルト ネットワークのインターフェイスが存在しなくても、そこへのパスが格納されている場合、そのネットワークは 1 つの候補と見なされ、最適なデフォルト パスへのゲートウェイが最終ゲートウェイになります。

ルート マップによるルーティング情報の再配信

スイッチでは複数のルーティング プロトコルを同時に実行し、ルーティング プロトコル間で情報を再配信できます。ルーティング プロトコル間での情報の再配信は、サポートされているすべての IP ベース ルーティング プロトコルに適用されます。

2 つのドメイン間で拡張パケット フィルタまたはルート マップを定義することにより、ルーティング ドメイン間でルートの再配信を条件付きで制御することもできます。**match** および **set** ルート マップ コンフィギュレーション コマンドは、ルート マップの条件部分を定義します。**match** コマンドは、一致しなければならない条件を指定します。**set** コマンドは、ルーティング アップデートが **match** コマンドによって定義される条件と一致した場合に実行されるアクションを指定します。再配信はプロトコルに依存しない機能ですが、**match** および **set** ルート マップ コンフィギュレーション コマンドの一部は特定のプロトコル固有のものであります。

route-map コマンドのあとに、**match** コマンドおよび **set** コマンドをそれぞれ 1 つまたは複数指定します。**match** コマンドを指定しない場合は、すべて一致すると見なされます。**set** コマンドを指定しない場合、一致以外の処理はすべて実行されません。このため、少なくとも 1 つの **match** または **set** コマンドを指定する必要があります。



(注) **set** ルート マップ コンフィギュレーション コマンドが指定されていないルート マップは CPU に送信され、CPU の利用率が高くなります。

ルートマップ ステートメントは、**permit** または **deny** として識別することもできます。ステートメントが拒否としてマークされている場合、一致基準を満たすパケットは通常の転送チャンネルを通じて送り返されます（宛先ベース ルーティング）。ステートメントが許可としてマークされている場合は、一致基準を満たすパケットに **set** コマンドが適用されます。一致基準を満たさないパケットは、通常のルーティング チャンネルを通じて転送されます。

BGP ルート マップ **continue** コマンドを使用すると、**match** および **set** コマンドが正常に実行されたあと、ルート マップの他のエントリを実行することができます。**continue** コマンドを使用することで、よりモジュール化したポリシー定義の構成と編成ができるので、同じルート マップ内に特定のポリシー設定を繰り返す必要がなくなります。スイッチでは、発信ポリシーに **continue** コマンドを使用できます。ルート マップ **continue** コマンドの使用の詳細については、次の URL で、『BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guides_list.html



(注)

次に示すステップ 3 ~ 14 はそれぞれ任意ですが、少なくとも 1 つの **match** ルート マップ コンフィギュレーション コマンド、および 1 つの **set** ルート マップ コンフィギュレーション コマンドを入力する必要があります。

再配信用のルート マップを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	route-map map-tag [permit deny] [sequence number]	再配信を制御するために使用するルート マップを定義し、ルートマップ コンフィギュレーション モードを開始します。 <i>map-tag</i> : ルート マップ用のわかりやすい名前を指定します。 redistribute ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 (任意) permit が指定され、このルート マップの一致条件が満たされている場合は、 set アクションの制御に従ってルートが再配信されます。 deny が指定されている場合、ルートは再配信されません。 <i>sequence number</i> (任意) : 同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を指定する番号です。
ステップ 3	match as-path path-list-number	BGP AS パス アクセス リストと一致させます。
ステップ 4	match community-list community-list-number [exact]	BGP コミュニティ リストと一致させます。
ステップ 5	match ip address {access-list-number access-list-name} [...access-list-number ...access-list-name]	名前または番号を指定し、標準アクセス リストと一致させます。1 ~ 199 の整数を指定できます。
ステップ 6	match metric metric-value	指定されたルート メトリックと一致させます。 <i>metric-value</i> には、0 ~ 4294967295 の値が指定された、EIGRP のメトリックを指定できます。

	コマンド	目的
ステップ 7	match ip next-hop { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	指定されたアクセスリスト (番号 1 ~ 199) のいずれかで送信される、ネクスト ホップのルータ アドレスと一致させます。
ステップ 8	match tag tag value [... <i>tag-value</i>]	1 つまたは複数のルート タグ値からなるリスト内の指定されたタグ値と一致させます。0 ~ 4294967295 の整数を指定できます。
ステップ 9	match interface type number [... <i>type number</i>]	指定されたインターフェイスの 1 つから、指定されたネクスト ホップへのルートと一致させます。
ステップ 10	match ip route-source { <i>access-list-number</i> <i>access-list-name</i> } [... <i>access-list-number</i> ... <i>access-list-name</i>]	指定されたアドバタイズ済みアクセスリストによって指定されるアドレスと一致させます。
ステップ 11	match route-type { local internal external [type-1 type-2]}	指定された route-type と一致させます。 <ul style="list-style-type: none"> • local : ローカルに生成された BGP ルート • internal : OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート • external : OSPF 外部ルート (タイプ 1 またはタイプ 2) または EIGRP 外部ルート
ステップ 12	set dampening <i>half-life</i> <i>reuse</i> <i>suppress</i> <i>max-suppress-time</i>	BGP ルート ダンピング係数を設定します。
ステップ 13	set local-preference <i>value</i>	ローカル BGP パスに値を割り当てます。
ステップ 14	set origin { igp egp <i>as</i> incomplete }	BGP の送信元コードを設定します。
ステップ 15	set as-path { tag prepend <i>as-path-string</i> }	BGP AS パスを変更します。
ステップ 16	set level { level-1 level-2 level-1-2 stub-area backbone }	ルーティング ドメインの指定エリアにアドバタイズされるルートのレベルを設定します。 stub-area および backbone は、OSPF NSSA およびバックボーン エリアです。
ステップ 17	set metric <i>metric value</i>	再配信されるルートに指定するメトリック値を設定します (EIGRP 専用)。 <i>metric value</i> は -294967295 ~ 294967295 の整数です。
ステップ 18	set metric <i>bandwidth</i> <i>delay</i> <i>reliability</i> <i>loading</i> <i>mtu</i>	再配信されるルートに指定するメトリック値を設定します (EIGRP 専用)。 <ul style="list-style-type: none"> • <i>bandwidth</i> : 0 ~ 4294967295 の範囲のルートのメトリック値または IGRP 帯域幅 (キロビット/秒単位) • <i>delay</i> : 0 ~ 4294967295 の範囲のルート遅延 (10 マイクロ秒単位) • <i>reliability</i> : 0 ~ 255 の数値で表されるパケット伝送の成功可能性。255 は信頼性が 100% であること、0 は信頼性がないことを意味します。 • <i>loading</i> : 0 ~ 255 の数値で表されるルートの有効帯域幅 (255 は 100% の負荷) • <i>mtu</i> : ルートの MTU の最小サイズ (バイト単位)。範囲は 0 ~ 4294967295 です。
ステップ 19	set metric-type { type-1 type-2 }	再配信されるルートに OSPF 外部メトリック タイプを設定します。

	コマンド	目的
ステップ 20	set metric-type internal	ネクスト ホップの IGP メトリックと一致するように、EBGP ネイバーにアドバタイズされるプレフィックスの MED 値を設定します。
ステップ 21	set weight	ルーティング テーブルの BGP ウェイトを設定します。指定できる値は 1 ~ 65535 です。
ステップ 22	end	特権 EXEC モードに戻ります。
ステップ 23	show route-map	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 24	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、**no route-map map tag** グローバル コンフィギュレーション コマンド、または **no match** や **no set** ルートマップ コンフィギュレーション コマンドを使用します。

ルーティング ドメイン間でルートを送信したり、ルート再配信を制御できます。

ルート再配信を制御するには、特権 EXEC モードで次の手順を実行します。キーワードは前述の手順で定義されたキーワードと同じです。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router {bgp rip ospf eigrp}	ルータ コンフィギュレーション モードを開始します。
ステップ 3	redistribute protocol [process-id] {level-1 level-1-2 level-2} [metric metric-value] [metric-type type-value] [match internal external type-value] [tag tag-value] [route-map map-tag] [weight weight] [subnets]	ルーティング プロトコル間でルートを送信します。route-map を指定しないと、すべてのルートが再配信されます。キーワード route-map に map-tag を指定しないと、ルートは配信されません。
ステップ 4	default-metric number	現在のルーティング プロトコルが、再配信されたすべてのルートに対して同じメトリック値を使用するように設定します (BGP、RIP、OSPF)。
ステップ 5	default-metric bandwidth delay reliability loading mtu	EIGRP ルーティング プロトコルが、EIGRP 以外で再配信されたすべてのルートに対して同じメトリック値を使用するように設定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show route-map	設定を確認するため、設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再配信をディセーブルにするには、そのコマンドの **no** 形式を使用します。

ルーティング プロトコルのメトリックを、必ずしも別のルーティング プロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントで、IGRP メトリックは 5 つの特性の組み合わせです。このような場合は、メトリックを独自に設定し、再配信されたルートに割り当てます。ルーティング情報を制御せずにさまざまなルーティング プロトコル間で交換するとルーティング ループが発生し、ネットワーク動作が著しく低下することもあります。

メトリック変換の代わりに使用されるデフォルトの再配信メトリックが定義されていない場合は、ルーティング プロトコル間で自動的にメトリック変換が発生することもあります。

- RIP はスタティック ルートを自動的に再配信できます。スタティック ルートにはメトリック 1 (直接接続) が割り当てられます。
- デフォルト モードになっている場合、どのプロトコルも他のルーティング プロトコルを再配信できます。

PBR の設定

PBR を使用すると、トラフィック フローに定義済みポリシーを設定できます。PBR を使用してルーティングをより細かく制御するには、ルーティング プロトコルから取得したルートの信頼度を小さくします。PBR は、次の基準に基づいて、パスを許可または拒否するルーティング ポリシーを設定したり、実装したりできます。

- 特定のエンド システムの ID
- 説明
- プロトコル

PBR を使用すると、等価アクセスや送信元依存ルーティング、双方向対バッチ トラフィックに基づくルーティング、専用リンクに基づくルーティングを実現できます。たとえば、在庫記録を本社に送信する場合は広帯域で高コストのリンクを短時間使用し、電子メールなど日常的に使用するアプリケーション データは狭帯域で低コストのリンクで送信できます。

PBR がイネーブルの場合は、Access Control List (ACL; アクセス コントロール リスト) を使用してトラフィックを分類し、各トラフィックがそれぞれ異なるパスを経由するようにします。PBR は着信パケットに適用されます。PBR がイネーブルのインターフェイスで受信されたすべてのパケットは、ルート マップを通過します。ルート マップで定義された基準に基づいて、パケットは適切なネクスト ホップに転送 (ルーティング) されます。

- パケットがルート マップ ステートメントと一致しない場合は、すべての `set` コマンドが適用されません。
- ステートメントが許可とマークされている場合、どのルートマップ ステートメントとも一致しないパケットは通常の転送チャネルを通じて送信され、宛先ベースのルーティングが実行されます。
- PBR に対して、拒否のマークが付いているルートマップ ステートメントはサポートされていません。

ルート マップの設定の詳細については、「[ルート マップによるルーティング情報の再配信](#)」(P.38-99) を参照してください。

標準 IP ACL を使用すると、アプリケーション、プロトコル タイプ、またはエンド ステーションに基づいて一致基準を指定するように、送信元アドレスまたは拡張 IP ACL の一致基準を指定できます。一致が見つかるまで、ルート マップにこのプロセスが行われます。不一致が見つからない場合は、通常の宛先ベース ルーティングが発生します。match ステートメント リストの末尾には、暗黙の拒否エントリがあります。

match コマンドが満たされた場合は、set コマンドを使用して、パス内のネクスト ホップ ルータを識別する IP アドレスを指定できます。

PBR コマンドおよびキーワードの詳細については、『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2 を参照してください。表示されているにもかかわらずスイッチでサポートされない PBR コマンドについては、[付録 D 「Cisco IOS Release 12.2\(52\)SE でサポートされていないコマンド」](#) を参照してください。

PBR 設定はスタック全体に適用され、すべてのスイッチでスタック マスターの設定が使用されます。



(注) このソフトウェア リリースは、IPv4 および IPv6 トラフィック処理時に PBR をサポートしません。

PBR 設定時の注意事項

PBR の設定を開始する前に、次の点に注意してください。

- PBR を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。
- マルチキャスト トラフィックには、ポリシーによるルーティングが行われません。PBR が適用されるのはユニキャスト トラフィックだけです。
- ルーテッド ポートまたは SVI 上で、PBR をイネーブルにできます。
- スイッチは、PBR の **route-map deny** ステートメントをサポートしていません。
- レイヤ 3 モードの EtherChannel ポート チャンネルにはポリシー ルート マップを適用できますが、EtherChannel のメンバーである物理インターフェイスには適用できません。適用しようとすると、コマンドが拒否されます。ポリシー ルート マップが適用されている物理インターフェイスは、EtherChannel のメンバーになることができません。
- スイッチ スタックには最大 246 個の IP ポリシー ルート マップを定義できます。
- スイッチ スタックには、PBR 用として最大 512 個の Access Control Entry (ACE; アクセス コントロール エントリ) を定義できます。
- ルート マップに一致基準を設定するときには、次の注意事項に従ってください。
 - ローカル アドレス宛の packets を許可する ALC と一致させないでください。PBR はこれらの packets を転送しますが、ping や Telnet 障害またはルート プロトコル フラッピングが発生する可能性があります。
 - 拒否 ACE のある ACL と一致させないでください。拒否 ACE と一致する packets が CPU に送信されると、CPU の利用率が高くなる可能性があります。
- PBR を使用するには、**sdm prefer routing** グローバル コンフィギュレーション コマンドを使用して、まずルーティング テンプレートをイネーブルにする必要があります。VLAN またはデフォルト テンプレートでは、PBR がサポートされません。SDM テンプレートの詳細については、[第 8 章「SDM テンプレートの設定」](#)を参照してください。
- VRF と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、VRF をイネーブルにすることはできません。同じように、インターフェイスで VRF がイネーブルになっているときは、PBR をイネーブルにはできません。
- WCCP と PBR は、スイッチ インターフェイス上で相互に排他的です。PBR がインターフェイスでイネーブルになっているときは、WCCP をイネーブルにすることはできません。同じように、インターフェイスで WCCP がイネーブルになっているときは、PBR をイネーブルにすることはできません。
- PBR で使用される Ternary CAM (TCAM) エントリ数は、ルート マップ自体、使用される ACL、ACL およびルート マップ エントリの順序によって異なります。
- パケット長、Type of Service (ToS; サービス タイプ)、set interface、set default next hop、または set default interface に基づく PBR は、サポートされていません。有効な set アクションがないか、または set アクションが *Don't Fragment* に設定されているポリシー マップは、サポートされていません。

- スイッチは PBR ルート マップでの Quality of Service (QoS) DSCP および IP precedence の一致をサポートしていて、次のような制限事項があります。
 - QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用することができません。
 - 透過的な DSCP と PBR DSCP ルート マップを同一スイッチに設定することはできません。
 - PBR と QoS DSCP を設定する際に、QoS をイネーブルに設定 (**mls qos** グローバル コンフィギュレーション コマンドを入力) するか、ディセーブルに設定 (**no mls qos** グローバル コンフィギュレーション コマンドを入力) することができます。QoS がイネーブルの場合、トラフィックの DSCP 値が変更されないようにするには、**mls qos trust dscp** インターフェイス コンフィギュレーション コマンドを入力して、スイッチの入力トラフィック ポートで DSCP 信頼状態を設定します。信頼状態が DSCP でない場合、デフォルトですべての信頼されていないトラフィックの DSCP 値が 0 に設定されます。

PBR のイネーブル化

デフォルトでは、PBR はスイッチ上でディセーブルです。PBR をイネーブルにするには、一致基準およびすべての **match** コマンドと一致した場合の動作を指定するルート マップを作成する必要があります。次に、特定のインターフェイスでそのルート マップ用の PBR をイネーブルにします。指定したインターフェイスに着信したパケットのうち、**match** コマンドと一致したものはすべて PBR の対象になります。

PBR は、スイッチの速度低下を引き起こさない速度で、高速転送したり実装したりできます。高速スイッチングされた PBR では、ほとんどの **match** および **set** コマンドを使用できます。PBR の高速スイッチングをイネーブルにするには、事前に PBR をイネーブルにする必要があります。PBR の高速スイッチングは、デフォルトでディセーブルです。

スイッチで生成されたパケットまたはローカル パケットは、通常どおりにポリシー ルーティングされません。スイッチ上でローカル PBR をグローバルにイネーブルにすると、そのスイッチから送信されたすべてのパケットがローカル PBR の影響を受けます。ローカル PBR は、デフォルトでディセーブルに設定されています。



(注) PBR をイネーブルにするには、スタック マスター上で IP サービス イメージが稼動している必要があります。

PBR を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>route-map map-tag [permit] [sequence number]</code>	<p>パケットの出力場所を制御するために使用するルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> <code>map-tag</code> : ルート マップ用のわかりやすい名前を指定します。ip policy route-map インターフェイス コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。 (任意) permit が指定され、このルート マップの一致条件が満たされている場合は、set アクションの制御に従ってルートがポリシールーティングされます。 <p>(注) route-map deny ステートメントは、インターフェイスに適用される PBR ルート マップでサポートされていません。</p> <ul style="list-style-type: none"> <code>sequence number</code> (任意) : 同じ名前によってすでに設定されているルート マップのリスト内で、新しいルート マップの位置を示す番号です。
ステップ 3	<code>match ip address {access-list-number access-list-name} [...access-list-number ...access-list-name]</code>	<p>1 つまたは複数の標準または拡張アクセス リストで許可されている送信元および宛先 IP アドレスを照合します。</p> <p>(注) 拒否 ACE のある ACL またはローカル アドレス宛の packets を許可する ACL を入力しないでください。</p> <p>match コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。</p>
ステップ 4	<code>set ip next-hop ip-address [...ip-address]</code>	基準と一致するパケットの動作を指定します。パケットのルーティング先となるネクスト ホップを設定します (ネクスト ホップは隣接していなければなりません)。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 7	<code>ip policy route-map map-tag</code>	<p>レイヤ 3 インターフェイス上で PBR をイネーブルにし、使用するルート マップを識別します。1 つのインターフェイスに設定できるルート マップは、1 つだけです。ただし、異なるシーケンス番号を持つ複数のルート マップ エントリを設定できます。これらのエントリは、最初の一致が見つかるまで、シーケンス番号順に評価されます。一致が見つからない場合、パケットは通常どおりにルーティングされます。</p> <p>(注) IP ポリシー ルート マップに deny ステートメントが含まれる場合、設定に失敗します。</p>
ステップ 8	<code>ip route-cache policy</code>	(任意) PBR の高速スイッチングをイネーブルにします。PBR の高速スイッチングをイネーブルにするには、まず PBR をイネーブルにする必要があります。
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 10 ip local policy route-map map-tag	(任意) ローカル PBR をイネーブルにして、スイッチから送信されるパケットに PBR を実行します。ローカル PBR は、スイッチによって生成されるパケットに適用されます。着信パケットには適用されません。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show route-map [map-name]	(任意) 設定を確認するため、設定されたすべてのルートマップ、または指定されたルートマップだけを表示します。
ステップ 13 show ip policy	(任意) インターフェイスに付加されたポリシー ルートマップを表示します。
ステップ 14 show ip local policy	(任意) ローカル PBR がイネーブルであるかどうか、およびイネーブルである場合は使用されているルートマップを表示します。
ステップ 15 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

エントリを削除するには、**no route-map map-tag** グローバル コンフィギュレーション コマンド、または **no match** または **no set** ルートマップ コンフィギュレーション コマンドを使用します。インターフェイス上で PBR をディセーブルにするには、**no ip policy route-map map-tag** インターフェイス コンフィギュレーション コマンドを使用します。PBR の高速スイッチングをディセーブルにするには、**no ip route-cache policy** インターフェイス コンフィギュレーション コマンドを使用します。スイッチから送信されるパケットに対して PBR をディセーブルにするには、**ip local policy route-map map-tag** グローバル コンフィギュレーション コマンドを使用します。

ルーティング情報のフィルタリング

ルーティング プロトコル情報をフィルタリングする場合は、次の作業を実行します。



(注) OSPF プロセス間でルートが再配信される場合、OSPF メトリックは保持されません。

パッシブ インターフェイスの設定

ローカル ネットワーク上の他のルータが動的にルートを取得しないようにするには、**passive-interface** ルータ コンフィギュレーション コマンドを使用し、ルーティング アップデート メッセージがルータ インターフェイスから送信されないようにします。OSPF プロトコルでこのコマンドを使用すると、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたルータ インターフェイスから送受信されません。

多数のインターフェイスが存在するネットワークで、インターフェイスを手動でパッシブに設定する作業を回避するには、**passive-interface default** ルータ コンフィギュレーション コマンドを使用し、すべてのインターフェイスをデフォルトでパッシブになるように設定します。このあとで、隣接関係が必要なインターフェイスを手動で設定します。

パッシブ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>passive-interface interface-id</code>	指定されたレイヤ 3 インターフェイス経由のルーティング アップデートの送信を抑制します。
ステップ 4	<code>passive-interface default</code>	(任意) すべてのインターフェイスを、デフォルトでパッシブとなるように設定します。
ステップ 5	<code>no passive-interface interface type</code>	(任意) 隣接関係を送信する必要があるインターフェイスだけをアクティブにします。
ステップ 6	<code>network network-address</code>	(任意) ルーティング プロセス用のネットワーク リストを指定します。 <i>network-address</i> は IP アドレスです。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

パッシブとしてイネーブルにしたインターフェイスを確認するには、`show ip ospf interface` などのネットワーク モニタ用特権 EXEC コマンドを使用します。アクティブとしてイネーブルにしたインターフェイスを確認するには、`show ip interface` 特権 EXEC コマンドを使用します。

ルーティング アップデートの送信を再度イネーブルにするには、`no passive-interface interface-id` ルータ コンフィギュレーション コマンドを使用します。`default` キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。次に、`no passive-interface` ルータ コンフィギュレーション コマンドを使用し、隣接関係を必要とする各インターフェイスを個別に設定します。`default` キーワードは、ほとんどの配信ルータに 200 を超えるインターフェイスが備わっているインターネット サービス プロバイダーや大規模な企業ネットワークの場合に役立ちます。

ルーティング アップデートのアドバタイズメントおよび処理の制御

ACL と `distribute-list` ルータ コンフィギュレーション コマンドを組み合わせて使用すると、ルーティング アップデート中にルートのアドバタイズメントを抑制し、他のルータが 1 つまたは複数のルートを取得しないようにできます。この機能を OSPF で使用した場合は外部ルートだけに適用されるため、インターフェイス名を指定することはできません。

`distribute-list` ルータ コンフィギュレーション コマンドを使用し、着信したアップデートのリストのうち特定のルート进行处理しないようにすることもできます (OSPF にこの機能は適用されません)。

ルーティング アップデートのアドバタイズメントまたは処理を制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>distribute-list {access-list-number access-list-name} out [interface-name routing process autonomous-system-number]</code>	アクセス リスト内のアクションに応じて、ルーティング アップデート内のルートのアドバタイズメントを許可または拒否します。
ステップ 4	<code>distribute-list {access-list-number access-list-name} in [type-number]</code>	アップデートにリストされたルートの処理を抑制します。

	コマンド	目的
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを変更またはキャンセルするには、**no distribute-list in** ルータ コンフィギュレーション コマンドを使用します。アップデート中のネットワーク アドバタイズメントの抑制をキャンセルするには、**no distribute-list out** ルータ コンフィギュレーション コマンドを使用します。

ルーティング情報の送信元のフィルタリング

一部のルーティング情報が他の情報よりも正確な場合があるため、フィルタリングを使用して、さまざまな送信元から送られる情報にプライオリティを設定できます。「管理距離」は、ルータやルータのグループなど、ルーティング情報の送信元の信頼性を示す数値です。大規模ネットワークでは、他のルーティング プロトコルよりも信頼できるルーティング プロトコルが存在する場合があります。管理距離の値を指定すると、ルータはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティング プロトコルの管理距離が最短（値が最小）であるルートが選択されます。

表 38-16 (P.38-98) に、さまざまなルーティング情報送信元のデフォルトの管理距離を示しています。

各ネットワークには独自の要件があるため、管理距離を割り当てる一般的な注意事項はありません。

ルーティング情報の送信元をフィルタリングするには、特権 EXEC モードで、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>router {bgp rip ospf eigrp}</code>	ルータ コンフィギュレーション モードを開始します。
ステップ 3	<code>distance weight {ip-address {ip-address mask}}</code> <code>[ip access list]</code>	管理距離を定義します。 <i>weight</i> : 管理距離は 10 ~ 255 の整数です。単独で使用した場合、 <i>weight</i> はデフォルトの管理距離を指定します。ルーティング情報の送信元に他の指定がない場合に使用されます。管理距離が 255 のルートはルーティング テーブルに格納されません。 (任意) <i>ip access list</i> : 着信ルーティング アップデートに適用される IP 標準または IP 拡張アクセス リストです。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip protocols</code>	指定されたルーティング プロセス用のデフォルトの管理距離を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

管理距離の定義を削除するには、**no distance** ルータ コンフィギュレーション コマンドを使用します。

認証鍵の管理

鍵管理を使用すると、ルーティングプロトコルで使用される認証鍵を制御できます。一部のプロトコルでは、鍵管理を使用することができません。認証鍵は EIGRP および RIP バージョン 2 で使用できます。

認証鍵を管理する前に、認証をイネーブルにする必要があります。プロトコルに対して認証をイネーブルにする方法については、該当するプロトコルについての説明を参照してください。認証鍵を管理するには、キーチェーンを定義してそのキーチェーンに属する鍵を識別し、各鍵の有効期間を指定します。各鍵には、ローカルに格納される独自の鍵 ID (**key number** キーチェーンコンフィギュレーションコマンドで指定) があります。鍵 ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5 (MD5) 認証鍵が一意に識別されます。

有効期間が指定された複数の鍵を設定できます。存在する有効な鍵の個数に関係なく、1 つの認証パケットだけが送信されます。鍵番号は小さい方から大きい方へ順に調べられ、最初に見つかった有効な鍵が使用されます。鍵変更中は、有効期間が重なっても問題ありません。これらの有効期間は、ルータに通知する必要があります。

認証鍵を管理するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	key chain name-of-chain	キーチェーンを識別し、キーチェーンコンフィギュレーションモードを開始します。
ステップ 3	key number	鍵番号を識別します。指定できる範囲は 0 ~ 2147483647 です。
ステップ 4	key-string text	キーstringを識別します。stringには 1 ~ 80 文字の大文字および小文字の英数字を指定できますが、最初の文字に数字を指定することはできません。
ステップ 5	accept-lifetime start-time {infinite end-time duration seconds}	(任意) 鍵を受信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトはデフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および duration は infinite です。
ステップ 6	send-lifetime start-time {infinite end-time duration seconds}	(任意) 鍵を送信する期間を指定します。 <i>start-time</i> および <i>end-time</i> 構文には、 <i>hh:mm:ss Month date year</i> または <i>hh:mm:ss date Month year</i> のいずれかを使用できます。デフォルトはデフォルトの <i>start-time</i> 以降、無制限です。指定できる最初の日付は 1993 年 1 月 1 日です。デフォルトの <i>end-time</i> および duration は infinite です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show key chain	認証鍵情報を表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

キーチェーンを削除するには、**no key chain name-of-chain** グローバルコンフィギュレーションコマンドを使用します。

IP ネットワークのモニタおよびメンテナンス

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定の統計情報を表示することもできます。ルートを消去したり、ステータスを表示するには、表 38-17 に示す特権 EXEC コマンドを使用します。

表 38-17 IP ルートの消去またはルートステータスの表示を行うコマンド

コマンド	目的
<code>clear ip route {network [mask *]}</code>	IP ルーティング テーブルから 1 つまたは複数のルートを消去します。
<code>show ip protocols</code>	アクティブなルーティング プロトコル プロセスのパラメータおよびステータスを表示します。
<code>show ip route [address [mask] [longer-prefixes]] [protocol [process-id]]</code>	ルーティング テーブルの現在のステータスを表示します。
<code>show ip route summary</code>	ルーティング テーブルの現在のステータスをサマリー形式で表示します。
<code>show ip route supernets-only</code>	スーパーネットを表示します。
<code>show ip cache</code>	IP トラフィックのスイッチングに使用されるルーティング テーブルを表示します。
<code>show route-map [map-name]</code>	設定されたすべてのルート マップ、または指定されたルート マップだけを表示します。



CHAPTER 39

IPv6 ユニキャスト ルーティングの設定

この章では、Catalyst 3750 スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定については、第 40 章「IPv6 MLD スヌーピングの設定」を参照してください。IPv6 Access Control List (ACL; アクセス コントロール リスト) の設定については、第 41 章「IPv6 ACL の設定」を参照してください。IPv4 ユニキャスト ルーティングの設定については、第 38 章「IP ユニキャスト ルーティングの設定」を参照してください。

この機能を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。

IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートを使用するようにスイッチを設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」(P.39-6) を参照してください。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で説明するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「IPv6 の概要」(P.39-1)
- 「IPv6 の設定」(P.39-11)
- 「IPv6 の表示」(P.39-28)

IPv6 の概要

IPv4 ユーザは IPv6 に移行して、エンドツーエンドセキュリティ、QoS (Quality of Service)、グローバルに一意なアドレスなどのサービスを利用することができます。IPv6 のアドレス空間の使用により、プライベートアドレスと、ネットワーク エッジ上の境界ルータで Network Address Translation (NAT; ネットワーク アドレス変換) 処理を使用する必要性が削減されます。

シスコシステムズの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

この章に記載されている IPv6 およびその他の機能の詳細については、次の情報を参照してください。

- 次の URL にある『*Cisco IOS IPv6 Configuration Library*』を参照してください。
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t.html
- Cisco IOS ソフトウェア マニュアルを検索する場合は、[検索] フィールドを使用してください。たとえば、スタティック ルートに関する情報が必要な場合は、[検索] フィールドに *Implementing Static Routes for IPv6* と入力すればスタティック ルートに関する次のマニュアルを入手できます。
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ここでは、スイッチへの IPv6 の実装について説明します。内容は次のとおりです。

- 「IPv6 アドレス」(P.39-2)
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」(P.39-3)
- 「サポートされていない IPv6 ユニキャスト ルーティング機能」(P.39-9)
- 「制限事項」(P.39-9)
- 「IPv6 とスイッチ スタック」(P.39-10)

IPv6 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。サイトローカルなユニキャスト アドレス、エニーキャスト アドレス、またはマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド (n:n:n:n:n:n:n:n の形式) で表されます。次に、IPv6 アドレスの例を示します。

```
2031:0000:130F:0000:0000:09C0:080F:130B
```

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

```
2031:0:130F:0:0:9C0:80F:130B
```

2 つのコロン (::) を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回だけです。

```
2031:0:130F::09C0:080F:130B
```

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章にある以下のセクションの内容は、Catalyst 3750 スイッチに適用されます。

- 「IPv6 Address Formats」
- 「IPv6 Address Type: Unicast」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコルの機能について説明します。

- 「128 ビット幅のユニキャスト アドレス」 (P.39-3)
- 「IPv6 DNS」 (P.39-4)
- 「IPv6 ユニキャストのパス MTU ディスカバリ」 (P.39-4)
- 「ICMPv6」 (P.39-4)
- 「近接ディスカバリ」 (P.39-4)
- 「デフォルト ルータ プリファレンス」 (P.39-5)
- 「IPv6 のステートレス自動設定および重複アドレス検出」 (P.39-5)
- 「IPv6 アプリケーション」 (P.39-5)
- 「デュアル IPv4/IPv6 プロトコル スタック」 (P.39-6)
- 「IPv6 DHCP アドレス割り当て」 (P.39-6)
- 「IPv6 のスタティック ルート」 (P.39-7)
- 「IPv6 RIP」 (P.39-7)
- 「IPv6 OSPF」 (P.39-7) (IP サービス イメージが稼動しているスイッチのみ)
- 「EIGRP IPv6」 (P.39-7) (IP サービス イメージが稼動しているスイッチのみ)
- 「HSRP IPv6」 (P.39-7) (IP サービス イメージが稼動しているスイッチのみ)
- 「IPv6 による SNMP および Syslog」 (P.39-8)
- 「IPv6 による HTTP (S)」 (P.39-8)

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

スイッチは、ネイティブ イーサネット Inter-Switch Link (ISL; スイッチ間リンク) または 802.1Q トランク ポートによる IPv6 ルーティング機能 (スタティック ルートの場合)、IPv6 対応の Routing Information Protocol (RIP)、および Open Shortest Path First (OSPF) バージョン 3 プロトコルを提供します。等価コスト ルートは 16 までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

これらのアドレスはグローバル ルーティング プレフィクス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001 (2000::/3) で開始するアドレス範囲が使用されます。プレフィクスが 2000::/3 (001) ~ E000::/3 (111) のアドレスには、Extended Unique Identifier (EUI) -64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィクス FE80::/10 (1111 1110 10) およびインターフェイス ID を使用します。Neighbor Discovery Protocol (NDP) およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカルリンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章の、IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 DNS

IPv6 は、Domain Name System (DNS; ドメイン ネーム システム) の名前/アドレスおよびアドレス/名前の検索プロセスにおける DNS レコード タイプをサポートしています。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートしており、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチは、IPv6 ノードへのシステム Maximum Transmission Unit (MTU; 最大伝送ユニット) のアドバタイズメントおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パス上のすべてのリンクの MTU サイズを動的に検出して、サイズに合わせて調整することができます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケットサイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。スイッチは、マルチキャスト パケットのパス MTU ディスカバリをサポートしません。

ICMPv6

IPv6 の Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理やその他の診断機能の実行時のエラーを報告します。IPv6 では、近接ディスカバリ プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

近接ディスカバリ

スイッチは、IPv6 NDP (ICMPv6 の上位で稼働するプロトコル)、および NDP をサポートしない IPv6 ステーション対応のスタティックなネイバー エントリもサポートします。IPv6 NDP は ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク (ローカルリンク) 上のネイバーのリンクレイヤ アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 ビット未満のルートに対する ICMPv6 リダイレクトをサポートします。マスク長が 64 ビットを超えるホストルートまたは集約ルートでは、ICMP リダイレクトはサポートされません。

近接ディスカバリ スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。スイッチがアクティブに解決を試みているネイバーと、後続の IPv6 パケットのネクスト ホップが同じ場合、IPv6 パケットはドロップされます。これにより CPU の余分な負荷を避けられます。

デフォルト ルータ プリファレンス

スイッチは、ルータのアドバタイズメント メッセージの拡張である IPv6 Default Router Preference (DRP; デフォルト ルータの初期設定) をサポートしています。DRP により、適切なルータを選択するホストの機能が向上します。これはホストがマルチホーミングされており、ルータが異なるリンク上にある場合に特に有効です。スイッチでは RFC 4191 の Route Information Option はサポートされていません。

IPv6 ホストはデフォルト ルータ リストを管理し、このリストを使用してオフリンク宛先向けのトラフィックに対応するルータを選択します。宛先に対応するルータを選択すると、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。到達可能であるルータまたは到達可能性の高いルータの場合、NDP は同じルータを毎回選択することもルータ リスト内から順番に選択することもできます。DRP を使用することで、2 台のルータが到達可能である場合または到達可能性が高い場合には、どちらか一方のルータを優先するように IPv6 ホストを設定できます。

IPv6 DRP の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されるため、ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動ノードはルータに送信請求を送信して、インターフェイス設定用のアドバタイズメントをルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、traceroute、Telnet、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル)、および File Transfer Protocol (FTP; ファイル転送プロトコル)
- IPv6 トランスポートによる Secure Shell (SSH; セキュア シェル)
- IPv6 トランスポートによる HTTP サーバアクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol (CDP; シスコ検出プロトコル) サポート

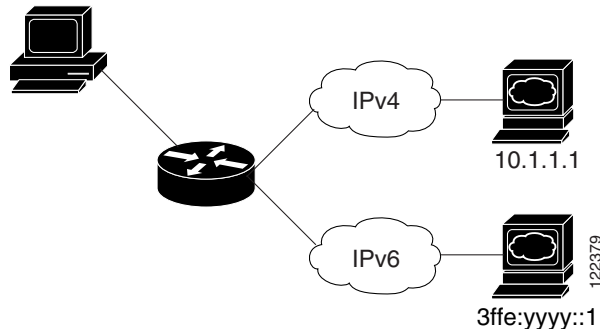
これらのアプリケーションの管理方法に関する詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方に Ternary Content Addressable Memory (TCAM) の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 39-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 39-1 インターフェイス上での IPv4/IPv6 のデュアル サポート



IPv6 ルーティングをイネーブルにするには、デュアル IPv4/IPv6 SDM テンプレートを使用します。デュアル IPv4/IPv6 SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

デュアル デスクトップおよびアグリゲータ IPv4/IPv6 テンプレートを使用することにより、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。
- IPv4 専用環境のスイッチは、IPv4 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境のスイッチは、IPv4 および IPv6 パケットをルーティングし、IPv4 QoS をハードウェアで適用します。
- IPv6 QoS のすべてはサポートされていません。IPv6 QoS trust はサポートされています。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4 および IPv6 のプロトコル スタックの詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 DHCP アドレス割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。アドレス割り当て機能により、ホストが接続されているネットワークに基づいた適切なプレフィクスで重複のないアドレス割り当てが行われます。アドレスは 1 つまたは複数のプレフィクス プールから割り当てることができます。デフォルト ドメインや DNS ネーム サーバアドレスなどのオプションもクライアントに渡すことができます。アドレス プールは、特定のインターフェイスや複数のインターフェイスで使用されるように割り当てたり、サーバが自動的に適切なプールを選択することもできます。

このマニュアルでは、DHCPv6 のアドレス割り当てについてのみ説明しています。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーク デバイス間のルートを示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 RIP

IPv6 Routing Information Protocol (RIP) は、ルーティング メトリックとしてホップ カウントを使用する距離ベクトル型プロトコルです。このプロトコルには、IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとしてサポートする機能などがあります。

IPv6 RIP の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF

IP サービス イメージが稼動するスイッチは IP のリンクステートプロトコルの IPv6 Open Shortest Path First (OSPF) をサポートしています。詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

EIGRP IPv6

IP サービス イメージが稼動するスイッチは、IPv6 対応の Enhanced Interior Gateway Routing Protocol (EIGRP) をサポートしています。EIGRP IPv6 はこのプロトコルを実行するインターフェイスに設定され、グローバル IPv6 アドレスは必要ありません。

EIGRP IPv6 のインスタンスを実行するには、明示的または黙示的なルータ ID が必要です。黙示的なルータ ID はローカル IPv4 アドレスから抽出されるため、どの IPv4 ノードにも必ず利用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードだけのネットワークで実行されていることがあり、利用可能な IPv4 ルータ ID がありません。

EIGRP IPv6 の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing EIGRP for IPv6」の章を参照してください。

HSRP IPv6

IP サービス イメージが稼動するスイッチは、IPv6 対応の Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) をサポートします。HSRP は、IPv6 トラフィック ルーティングに冗長性を提供し、1 台のルータの可用性に依存しないルーティングを可能にします。IPv6 ホストは、IPv6 近接ディスカバリ ルータ アドバタイズメント メッセージを介して利用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされる場合と、ホストによって送信請求される場合があります。

HSRP IPv6 グループは、HSRP グループ番号から抽出される仮想 MAC アドレスと、デフォルトで HSRP 仮想 MAC アドレスから抽出される仮想 IPv6 リンクローカルアドレスを持っています。HSRP グループがアクティブな場合、HSRP 仮想 IPv6 リンクローカルアドレスにメッセージが定期的に送信されます。グループがアクティブでなくなる際に最後のメッセージが送信され、メッセージは停止します。

IPv6 HSRP の設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 による SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 ネットワークの管理に IPv6 と IPv4 の両方のトランスポートが必要です。IPv6 による Syslog は、これらのトランスポートのアドレス データ タイプをサポートしています。

IPv6 による SNMP および Syslog で提供される機能は、次のとおりです。

- IPv4 と IPv6 両方のサポート
- SNMP 用の IPv6 トランスポート、および IPv6 ホストのトラップをサポートするための SNMP エージェントの変更
- IPv6 アドレッシングをサポートする SNMP 関連 MIB および Syslog 関連 MIB
- IPv6 ホストをトラップの受信側にする設定

IPv6 によるサポートの場合、SNMP は既存の IP トランスポート マッピングを変更して IPv4 と IPv6 を同時にサポートします。次の SNMP 処理は、IPv6 トランスポート管理をサポートしています。

- デフォルト設定での User Datagram Protocol (UDP; ユーザ データグラム プロトコル) SNMP ソケットのオープン
- 新しいトランスポート メカニズム (*SR_IPV6_TRANSPORT*) の提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポート対応の SNMP 名前付きアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能が IPv6 トランスポートで動作することの確認

設定手順を含めた IPv6 による SNMP に関する詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含めた IPv6 による Syslog の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP (S)

HTTP クライアントは IPv4 および IPv6 HTTP サーバの両方に要求を送信し、HTTP サーバは IPv4 および IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを使用する URL は、16 ビット値を使用したコロン区切りの 16 進形式で指定する必要があります。

アクセプト ソケット コールによって、IPv4 または IPv6 のアドレス ファミリが選択されます。アクセプト ソケットは IPv4 ソケットか IPv6 ソケットのどちらかです。リスニング ソケットは、接続を知らせる IPv4 信号と IPv6 信号の両方を待ち受けます。IPv6 リスニング ソケットは、IPv6 ワイルドカードアドレスにバインドされます。

TCP/IP の基本スタックはデュアルスタック環境をサポートします。HTTP は、ネットワークレイヤの相互作用の処理に TCP/IP スタックとソケットを使用します。

HTTP 接続が可能になるには、クライアントとサーバの間で基本的なネットワーク接続 (ping) が確立している必要があります。

詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしていません。

- IPv6 Policy-Based Routing (PBR; ポリシーベース ルーティング)
- IPv6 Virtual Private Network (VPN; バーチャル プライベート ネットワーク) Routing And Forwarding (VRF; VPN ルーティングおよび転送) テーブルのサポート
- 次の IPv6 ルーティング プロトコルのサポート : マルチプロトコル Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) および Intermediate System-to-Intermediate System (IS-IS) ルーティング
- サイトローカルなアドレス宛の IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 Unicast Reverse-Path Forwarding (uRPF; ユニキャスト RPF)
- IPv6 の一般的なプレフィクス

制限事項

IPv6 はスイッチのハードウェアに実装されるため、TCAM 内の IPv6 圧縮アドレスによるいくつかの制限があります。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- IPv6 ホスト ルート (特定のホストに到達するために使用されるルート) またはマスク長が 64 ビットを超える IPv6 ルートでは、ICMPv6 リダイレクト機能がサポートされません。スイッチは、ホストルートを介して、またはマスク長が 64 ビットを超えるルートを介して到達可能な特定の宛先の場合、より適したファースト ホップ ルータにホストをリダイレクトすることができません。
- IPv6 ホスト ルートまたはマスク長が 64 ビットを超える IPv6 ルートには、等価コストおよび不等価コスト ルートを使用するロード バランシングがサポートされません。
- スイッチは、SNAP でカプセル化された IPv6 パケットを転送できません。



(注) IPv4 SNAP でカプセル化されたパケットにも同様の制限がありますが、パケットはスイッチでドロップされ転送されません。

- スイッチは、IPv6/IPv4 および IPv4/IPv6 パケットをハードウェアでルーティングしますが、スイッチを IPv6/IPv4 または IPv4/IPv6 トンネル エンドポイントにはできません。
- ホップ単位の拡張ヘッダーを持つブリッジング済みの IPv6 パケットは、ソフトウェアで転送されます。IPv4 の場合、これらのパケットはソフトウェアでルーティングされ、ハードウェアでブリッジングされます。

- ソフトウェア コンフィギュレーション ガイドで定義された標準の SPAN および RSPAN 制限のほかに、次のような IPv6 パケット固有の制限事項があります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、SPAN 出力パケット内の送信元 MAC アドレスに誤りが生じることがあります。
 - RSPAN IPv6 ルーテッド パケットを送信した場合、宛先 MAC アドレスに誤りが生じることがあります。標準トラフィックは影響を受けません。
- スイッチはソースルート IPv6 パケットに関する QoS 分類または PBR をハードウェアで適用できません。
- スイッチはマルチキャスト パケットに対して ICMPv6 *Packet Too Big* メッセージを生成できません。

IPv6 とスイッチ スタック

スイッチは、スタック全体への IPv6 フォワーディングとスタック マスター上の IPv6 ホスト機能をサポートしています。スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。Distributed CEF (dCEF; 分散 CEF) を使用して、スタック マスターはルーティング テーブルをスタック メンバー スイッチにダウンロードします。メンバー スイッチはテーブルを受信し、転送用のハードウェア IPv6 ルートを作成します。スタック マスターはすべての IPv6 アプリケーションも実行します。



(注)

IPv6 パケット ルーティングをスタック内で機能させるために、スタック内のすべてのスイッチで IP サービス イメージを実行している必要があります。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。新しいスタック マスターが選択されてリセットする間、スイッチ スタックは IPv6 パケットを転送しません。スタックの MAC アドレスが変わると、IPv6 アドレスも変わります。 `ipv6 address ipv6-prefix/prefix length eui-64` インターフェイス コンフィギュレーション コマンドを使用して、EUI でスタックの IPv6 アドレスを指定すると、インターフェイス MAC アドレスに基づいたアドレスになります。「[IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化](#)」(P.39-12) を参照してください。

固定 MAC アドレス機能をスタックに設定してスタック マスターを変更した場合、スタック MAC アドレスは約 4 分間変更されません。詳細については、「[固定 MAC アドレスのイネーブル化](#)」(P.5-19) の第 5 章「[スイッチ スタックの管理](#)」を参照してください。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
 - IPv6 ルーティング プロトコルの実行
 - ルーティング テーブルの生成
 - dCEFv6 を使用するスタック メンバーへの CEFv6 ルーティング テーブルの配布
 - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタック メンバー (IP サービス イメージを実行している必要があります)
 - スタック マスターからの CEFv6 ルーティング テーブルの受信
 - ハードウェアへのルートのプログラミング



(注) IPv6 パケットに例外 (IPv6Option) がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

- マスターの再選択での CEFv6 テーブルのフラッシュ

IPv6 の設定

ここでは、次の IPv6 転送の設定情報について説明します。

- 「IPv6 のデフォルト設定」 (P.39-11)
- 「IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化」 (P.39-12)
- 「デフォルト ルータ プリファレンスの設定」 (P.39-14)
- 「IPv4 および IPv6 プロトコル スタックの設定」 (P.39-15)
- 「DHCP 設定による IPv6 アドレス割り当て」 (P.39-16)
- 「IPv6 ICMP レート制限の設定」 (P.39-20)
- 「IPv6 の CEF および dCEF の設定」 (P.39-20)
- 「IPv6 のスタティック ルートの設定」 (P.39-21)
- 「IPv6 RIP の設定」 (P.39-22)
- 「IPv6 OSPF の設定」 (P.39-23)
- 「EIGRP IPv6 の設定」 (P.39-25)
- 「IPv6 HSRP の設定」 (P.39-25)

IPv6 のデフォルト設定

表 39-1 に IPv6 のデフォルト設定を示します。

表 39-1 IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルトのデスクトップまたはデフォルトのアグリゲータ (Catalyst3750-12S)
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	ディセーブル (IPv4 CEF および dCEF はデフォルトでイネーブル) (注) IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6 アドレッシングの設定および IPv6 ルーティングのイネーブル化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当て、スイッチ上で IPv6 トラフィックをグローバルに転送する手順について説明します。

スイッチに IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- この章に記載されたすべての機能が、IP サービス イメージが稼動する Catalyst 3750 スイッチでサポートされているわけではありません。「サポートされていない IPv6 ユニキャスト ルーティング機能」(P.39-9) を参照してください。
- ipv6 address** インターフェイス コンフィギュレーション コマンドの *ipv6-address* および *ipv6-prefix* 変数は、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで入力する必要があります。*prefix-length* 変数（先頭にスラッシュ [/] を付加）は、プレフィクス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上で IPv6 トラフィックを転送するには、そのインターフェイスにグローバル IPv6 アドレスを設定する必要があります。インターフェイスに IPv6 アドレスを設定すると、リンクに対してローカルなアドレスが自動的に設定され、そのインターフェイスで IPv6 が有効になります。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信請求ノード マルチキャスト グループ FF02:0:0:0:1:ff00::/104（このアドレスは近接ディスカバリ プロセスに使用される）
- すべてのノードを含む、リンクに対してローカルな マルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルな マルチキャスト グループ FF02::2

IPv6 ルーティングの設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>sdm prefer dual-ipv4-and-ipv6 {default routing vlan} [desktop]</code>	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 <ul style="list-style-type: none"> default : スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 routing : IPv4 PBR などの IPv4 および IPv6 ルーティングをサポートするためにスイッチをルーティング テンプレートに設定します。 vlan : ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。 desktop : デスクトップ テンプレートの 1 つをスイッチに設定するために Catalyst 3750-12S アグリゲータ スイッチでのみサポートされます。アグリゲータ スイッチでこの設定が選択されなかった場合、アグリゲータ テンプレートが自動的に選択されます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>reload</code>	オペレーティング システムをリロードします。

	コマンド	目的
ステップ 5	configure terminal	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。
ステップ 8	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	IPv6 アドレスの下位 64 ビットの EUI を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスで IPv6 がイネーブルな場合に自動設定される、リンクに対してローカルなアドレスでなく、インターフェイス上の特定の、リンクに対してローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合に限定されます。
ステップ 9	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	ip routing	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11	ipv6 unicast-routing	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ipv6 interface interface-id	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。両方のアドレスの下位 64 ビットでは、EUI-64 インターフェイス ID が使用されます。**show ipv6 interface EXEC** コマンドの出力は、インターフェイスのリンクローカル プレフィクス FE80::/64 にインターフェイス ID (20B:46FF:FE2F:D940) を付加する方法を示しています。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/0/1
```

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/1
GigabitEthernet1/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定

ルータ アドバタイズメント メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドで設定された DRP と共に送信されます。DRP が設定されていない場合、RA は **medium** プリファレンスで送信されます。

DRP が有効なのは、リンク上の 2 つのルータが同等であっても等コスト ルーティングを提供していない場合で、ポリシーが 2 台のルータのどちらかを優先するように指定しているような場合です。

インターフェイスにルータの DRP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、DRP を指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	ipv6 nd router-preference {high medium low}	スイッチ インターフェイスにルータの DRP を指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 DRP をディセーブルにするには、**no ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ルータの DRP を **high** にしてインターフェイスに設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6 DRP の設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv4 および IPv6 プロトコル スタックの設定

IPv6 ルーティングを設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選擇する必要があります。まだ設定していない場合、**sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan} [desktop]** グローバル コンフィギュレーション コマンドを使用して IPv6 をサポートするテンプレートを設定します。新規テンプレートを選択する場合は、**reload** 特権 EXEC コマンドを使用してスイッチをリロードし、テンプレートを有効にする必要があります。

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing	スイッチ上でルーティングをイネーブルに設定します。
ステップ 3	ipv6 unicast-routing	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	no switchport	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します (物理インターフェイスの場合)。
ステップ 6	ip address ip-address mask [secondary]	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	グローバル IPv6 アドレスを指定します。ネットワーク プレフィクスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンク ローカル アドレスでなく、インターフェイスで特定のリンク ローカル アドレスを使用するように指定します。 インターフェイスに IPv6 リンクに対してローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合に限定されます。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show interface interface-id show ip interface interface-id show ipv6 interface interface-id	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv4 ルーティングをディセーブルにするには、**no ip routing** グローバル コンフィギュレーション コマンドを使用します。IPv6 ルーティングをディセーブルにするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。インターフェイスから IPv4 アドレスを削除するには、**no ip address ip-address mask** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address ipv6-prefix/prefix length eui-64** または **no ipv6 address ipv6-address link-local** インターフェイス コンフィギュレーション コマンドを使用します。手動で設定したすべての IPv6 アドレスをインターフェイスから削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

DHCP 設定による IPv6 アドレス割り当て

ここでは、IPv6 DHCP (DHCPv6) アドレス割り当ての設定方法について説明します。

- 「DHCPv6 アドレス割り当てのデフォルト設定」 (P.39-16)
- 「DHCPv6 アドレス割り当て設定の注意事項」 (P.39-16)
- 「DHCPv6 サーバ機能のイネーブル化」 (P.39-17)
- 「DHCPv6 クライアント機能のイネーブル化」 (P.39-19)

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトでは、スイッチに DHCPv6 機能は設定されていません。

DHCPv6 アドレス割り当て設定の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
 - レイヤ 3 インターフェイス上で DHCPv6 IPv6 ルーティングをイネーブルにする必要があります。
 - SVI : **interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
 - レイヤ 3 モードの EtherChannel ポート チャンネル : **interface port-channel** **port-channel-number** コマンドを使用して作成されたポートチャンネル論理インターフェイスです。
- DHCPv6 を設定する前に、IPv4 および IPv6 をサポートする SDM テンプレートを選択する必要があります。
- DHCPv6 クライアント、サーバ、またはリレー エージェントはマスター スイッチ上でのみ稼働します。スタック マスターの再選出が行われると、新しいマスター スイッチが DHCPv6 設定を保持します。ただし、DHCP サーバ データベースのリース情報のローカル RAM コピーは保持されません。

DHCPv6 サーバ機能のイネーブル化

インターフェイスで DHCPv6 サーバ機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 dhcp pool poolname</code>	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。プール名には、文字列（例：Engineering）または整数（例：0）を使用できます。
ステップ 3	<code>address prefix IPv6-prefix lifetime {tl tl infinite}</code>	<p>(任意) アドレス割り当てのアドレス プレフィックスを指定します。</p> <p>このアドレスは 16 ビット値を使用したコロン区切りの 16 進形式で指定する必要があります。</p> <p>lifetime tl tl : IPv6 アドレス プレフィックスが有効になっている期間（秒）を指定します。指定できる範囲は 5 ~ 4294967295 秒です。無期限の場合は infinite を指定します。</p>
ステップ 4	<code>link-address IPv6-prefix</code>	<p>(任意) リンクアドレスの IPv6 プレフィックスを指定します。</p> <p>着信インターフェイス上のアドレスまたはパケット内のリンクアドレスが指定の IPv6 プレフィックスと一致すると、サーバは構成情報プールを使用します。</p> <p>このアドレスは 16 ビット値を使用したコロン区切りの 16 進形式で指定する必要があります。</p>
ステップ 5	<code>vendor-specific vendor-id</code>	(任意) ベンダー固有コンフィギュレーション モードを開始し、ベンダー固有の識別番号を入力します。この番号はベンダーの IANA Private Enterprise Number (PEN) です。指定できる範囲は 1 ~ 4294967295 です。
ステップ 6	<code>suboption number {address IPv6-address ascii ASCII-string hex hex-string}</code>	(任意) ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ~ 65535 です。サブオプションパラメータの定義に従って IPv6 アドレス、ASCII テキスト、または 16 進形式の文字列を入力します。
ステップ 7	<code>exit</code>	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。

コマンド	目的
ステップ 10 ipv6 dhcp server [<i>poolname</i> automatic] [rapid-commit] [<i>preference value</i>] [allow-hint]	インターフェイスで DHCPv6 サーバ機能をイネーブルにします。 <ul style="list-style-type: none"> • poolname : (任意) IPv6 DHCP プールのユーザ定義名。プール名には、文字列 (例: Engineering) または整数 (例: 0) を使用できます。 • automatic : (任意) クライアントにアドレスを割り当てる際に、使用するプールをシステムが自動的に決定できるようにします。 • rapid-commit : (任意) 2 メッセージ交換方式を許可します。 • preference value : (任意) サーバの送信するアドバタイズ メッセージ内のプリファレンス オプションで伝送されるプリファレンス値。指定できる範囲は 0 ~ 255 です。プリファレンス値のデフォルトは 0 です。 • allow-hint : (任意) サーバが SOLICIT メッセージに含まれたクライアントの提示内容を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントの提示内容を無視します。
ステップ 11 end	特権 EXEC モードに戻ります。
ステップ 12 show ipv6 dhcp pool または show ipv6 dhcp interface	DHCPv6 プールの設定を確認します。 インターフェイスで DHCPv6 サーバ機能がイネーブルになっていることを確認します。
ステップ 13 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCPv6 プールを削除するには、**no ipv6 dhcp pool poolname** グローバル コンフィギュレーション コマンドを使用します。DHCPv6 プールの特性を変更するには、DHCP プール コンフィギュレーション モード コマンドの **no** 形式を使用します。インターフェイス上の DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレス プレフィクスを持つ *engineering* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 つのリンクアドレスと 1 つの IPv6 アドレス プレフィクスを持つ *testgroup* という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

次に、ベンダー固有のオプションを持つ 350 という名前のプールを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化

インターフェイスで DHCPv6 クライアント機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 3	<code>ipv6 address dhcp [rapid-commit]</code>	DHCPv6 サーバから IPv6 アドレスを取得するようにインターフェイスを設定します。 rapid-commit : (任意) アドレス割り当てに 2 メッセージ交換方式を許可します。
ステップ 4	<code>ipv6 dhcp client request [vendor-specific]</code>	(任意) ベンダー固有のオプションを要求するようにインターフェイスを設定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ipv6 dhcp interface</code>	インターフェイスで DHCPv6 クライアント機能がイネーブルになっていることを確認します。

DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除するには、**no ipv6 address dhcp client request** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IPv6 アドレスを取得し rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

このマニュアルでは、DHCPv6 のアドレス割り当てについてのみ説明しています。DHCPv6 クライアント、サーバ、またはリレー エージェント機能の設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ (バケットに格納される最大トークン数) は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 icmp error-interval interval [bucket-size]</code>	IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定します。 <ul style="list-style-type: none"> <code>interval</code> : バケットに追加されるトークンの間隔 (ミリ秒)。指定できる範囲は 0 ~ 2147483647 ミリ秒です。 <code>bucket-size</code> : (任意) バケットに格納される最大トークン数。指定できる範囲は 1 ~ 200 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 interface [interface-id]</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ipv6 icmp error-interval` グローバル コンフィギュレーション コマンドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 の CEF および dCEF の設定

Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) は、ネットワーク パフォーマンスを向上させるレイヤ 3 IP スイッチング技術です。Catalyst 3750 スイッチ スタックでは、ハードウェアはスタックの Distributed CEF (dCEF; 分散 CEF) を使用します。IPv6 CEF および dCEF はデフォルトでディセーブルになっていますが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ユニキャスト パケットをルーティングするには、最初に `ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト パケット フォワーディングをグローバルに設定する必要があります。そして、`ipv6 address` インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

IPv6 CEF または dCEF をディセーブルにするには、`no ipv6 cef` または `no ipv6 cef distributed` グローバル コンフィギュレーション コマンドを使用します。IPv6 CEF または dCEF をディセーブルにしたあとに再びイネーブルにするには、`ipv6 cef` または `ipv6 cef distributed` グローバル コンフィギュレーション コマンドを使用します。IPv6 ステータスを確認するには、`show ipv6 cef` 特権 EXEC コマンドを入力します。

CEF および dCEF の設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルートの設定

スタティック IPv6 ルートを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 スタティック ルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 route <i>ipv6-prefix/prefix length</i> { <i>ipv6-address</i> <i>interface-id</i> [<i>ipv6-address</i>]} [<i>administrative distance</i>]	スタティック IPv6 ルートを設定します。 <ul style="list-style-type: none"> • <i>ipv6-prefix</i> : スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • <i>/prefix length</i> : IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進値の前にスラッシュを付加する必要があります。 • <i>ipv6-address</i> : 指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。アドレスは 16 ビット値を使用したコロン区切りの 16 進形式で指定する必要があります。 • <i>interface-id</i> : Point-To-Point (ポイントツーポイント) インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当て、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 <p>(注) リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、<i>interface-id</i> を指定する必要があります (リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります)。</p> <ul style="list-style-type: none"> • <i>administrative distance</i> : (任意) 管理距離。指定できる範囲は 1 ~ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティックルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きな管理距離を使用します。
ステップ 3	end	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 4 <code>show ipv6 static [ipv6-address ipv6-prefix/prefix length] [interface interface-id] [recursive] [detail]</code> または <code>show ipv6 route static [updated]</code>	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 <ul style="list-style-type: none"> • interface interface-id : (任意) 出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートだけを表示します。 • recursive : (任意) 再帰スタティック ルートだけを表示します。 recursive キーワードは interface キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィクスが指定されているかどうかに関係なく使用できます。 • detail : (任意) 次に示す追加情報を表示します。 <ul style="list-style-type: none"> – 有効な再帰ルートの場合、出力パス セットおよび最大分解深度 – 無効なルートの場合、ルートが無効な理由
ステップ 5 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたスタティック ルートを削除するには、`no ipv6 route ipv6-prefix/prefix length {ipv6-address | interface-id [ipv6-address]} [administrative distance]` グローバル コンフィギュレーション コマンドを使用します。

次に、管理距離が 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 RIP の設定

IPv6 RIP を実行するようにスイッチを設定する前に、`ip routing` グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、`ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 RIP を設定するには、特権 EXEC モードで次の必須および任意の手順を実行します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>ipv6 router rip name</code>	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーション モードを開始します。
ステップ 3 <code>maximum-paths number-paths</code>	(任意) IPv6 RIP がサポートできる等価コスト ルートの最大数を定義します。指定できる範囲は 1 ~ 64 で、デフォルトは 4 ルートです。
ステップ 4 <code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 5 <code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6 <code>ipv6 rip name enable</code>	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。

コマンド	目的
ステップ 7 ipv6 rip name default-information {only originate}	(任意) IPv6 デフォルト ルート (:::0) を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。 (注) 任意のインターフェイスから IPv6 デフォルト ルート (:::0) を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 <ul style="list-style-type: none"> • only : デフォルト ルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • originate : デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8 end	特権 EXEC モードに戻ります。
ステップ 9 show ipv6 rip [name] [interface interface-id] [database] [next-hops] または show ipv6 route rip [updated]	IPv6 RIP プロセスに関する情報を表示します。 IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 10 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RIP ルーティング プロセスをディセーブルにするには、**no ipv6 router rip name** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して RIP ルーティング プロセスをディセーブルにするには、**no ipv6 rip name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、*cisco* という RIP ルーティング プロセスを最大等価コスト ルート数 8 で設定し、それをインターフェイス上でイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface fastethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 RIP ルーティングの設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 OSPF の設定

使用するネットワークに合わせて IPv6 OSPF をカスタマイズできます。ただし、IPv6 OSPF のデフォルト設定は、ほとんどのユーザおよび機能の要件を満たすように設定されています。

次の注意事項に従ってください。

- スイッチで IP サービス イメージが稼動している必要があります。
- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。

- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングをイネーブルにし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 OSPF を設定するには、特権 EXEC モードで次の必須および任意の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 router ospf process-id	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ~ 65535 の正の整数を指定できます。
ステップ 3	area area-id range {ipv6-prefix/prefix length} [advertise not-advertise] [cost cost]	<p>(任意) エリア境界でルートを統合し、サマライズします。</p> <ul style="list-style-type: none"> • area-id : ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィックスのどちらかを指定できます。 • ipv6-prefix/prefix length : 宛先 IPv6 ネットワーク、およびプレフィクス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進数。10 進値の前にスラッシュ (/) を付加する必要があります。 • advertise : (任意) Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。 • not-advertise : (任意) アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • cost cost : (任意) 現在のサマリー ルートのメトリックまたはコスト。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ~ 16777215 です。
ステップ 4	maximum paths number-paths	(任意) IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等価コスト ルートの最大数を定義します。指定できる範囲は 1 ~ 64 で、デフォルトは 16 です。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	ipv6 ospf process-id area area-id [instance instance-id]	<p>インターフェイス上で IPv6 OSPF をイネーブルにします。</p> <p>instance instance-id : (任意) インスタンス ID。</p>
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	show ipv6 ospf [<i>process-id</i>] [<i>area-id</i>] interface [<i>interface-id</i>] または show ipv6 ospf [<i>process-id</i>] [<i>area-id</i>]	OSPF インターフェイスの情報を表示します。 OSPF ルーティング プロセスに関する一般的な情報を表示します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

OSPF ルーティング プロセスをディセーブルするには、**no ipv6 router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。特定のインターフェイスに対して OSPF ルーティング プロセスをディセーブルにするには、**no ipv6 ospf process-id area area-id** インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 OSPF ルーティングの設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing OSPF for IPv6」の章を参照してください。

EIGRP IPv6 の設定

デフォルトでは、EIGRP IPv6 はディセーブルになっています。インターフェイスに EIGRP IPv6 を設定できます。ルータおよびインターフェイスに EIGRP の設定をしたあと、**no shutdown** 特権 EXEC コマンドを入力して EIGRP を起動します。



(注) EIGRP IPv6 がシャットダウン モードではない場合、EIGRP ルータ モード コマンドを入力してルータおよびインターフェイスを設定する前に EIGRP が実行を始める場合があります。

スイッチで IP サービス イメージが稼働している必要があります。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定されているルータ ID を確認してから **router-id** コマンドを使用します。

EIGRP IPv4 の場合と同じように、EIGRP IPv6 でも EIGRP IPv4 インターフェイスを指定してからその一部を受動インターフェイスとして選択できます。その場合は **passive-interface default** コマンドを使用してすべてのインターフェイスを受動にしてから、アクティブにするインターフェイスを指定して **no passive-interface** コマンドを使用します。受動インターフェイス上に EIGRP IPv6 を設定する必要はありません。

設定手順の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 HSRP の設定

HSRP IPv6 は、IPv6 トラフィックのルーティングに冗長性を提供し、1 台のルータの可用性に依存しないルーティングを可能にします。

スイッチで IPv6 HSRP がイネーブルの場合、IPv6 ホストは IPv6 近接ディスカバリ ルータ アドバタイズメント メッセージを介して利用可能な IPv6 ルータを学習します。HSRP の IPv6 グループは、HSRP グループ番号から抽出される仮想 MAC アドレスを持っています。また、このグループは仮想 IPv6 リンクローカル アドレスを持っています。このアドレスはデフォルトで HSRP 仮想 MAC アドレスから抽出されます。HSRP グループがアクティブな場合、HSRP 仮想 IPv6 リンクローカル アドレスにメッセージが定期的に送信されます。

スイッチで IP サービス イメージが稼動している必要があります。

IPv6 HSRP を設定する場合は、インターフェイス上で HSRP バージョン 2 (HSRPv2) をイネーブルにする必要があります。

HSRPv1 および HSRPv2 を使用する IPv6 HSRP を設定する際の設定上の注意事項については、「[HSRP 設定時の注意事項](#)」(P.42-6) および「[HSRP のトラブルシューティング](#)」(P.42-13) を参照してください。

IPv6 HSRP および HSRPv2 の詳細については、[第 42 章「HSRP の設定」](#) を参照してください。



(注)

IPv6 HSRP グループを設定する前に、`ipv6 unicast-routing` グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、IPv6 HSRP グループを設定するインターフェイス上で IPv6 をイネーブルにします。

HSRP バージョン 2 のイネーブル化

レイヤ 3 インターフェイス上で HSRP バージョン 2 をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、スタンバイ バージョンを指定するレイヤ 3 インターフェイスを入力します。
ステップ 3	<code>standby version {1 2}</code>	2 を入力して HSRP バージョンを変更します。デフォルト値は 1 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show standby</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

HSRP IPv6 グループのイネーブル化

レイヤ 3 インターフェイス上で IPv6 HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、IPv6 HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。

コマンド	目的
ステップ 3 <code>standby [group-number] ipv6 {link-local-address autoconfig}</code>	IPv6 HSRP グループを作成（またはイネーブルに）します。 <ul style="list-style-type: none"> （任意） <code>group-number</code> : HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 4095 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 ホットスタンバイ ルータ インターフェイスのリンクローカルアドレスを入力するか、または、リンクローカルプレフィクスと変更済み EUI-64 フォーマットのインターフェイス識別情報からリンクローカルアドレスが自動的に生成されるように設定にします。EUI-64 インターフェイス識別情報は、関連する HSRP 仮想 MAC アドレスから作成されます。
ステップ 4 <code>standby [group-number] preempt [delay {minimum seconds reload seconds sync seconds}]</code>	ルータを preempt に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。 <ul style="list-style-type: none"> （任意） <code>group-number</code> : コマンドが適用されるグループ番号です。 （任意） delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 秒です（1 時間）。デフォルトは 0 です（遅延なしで引き継ぎます）。 （任意） reload : リロード後のプリエンプト遅延を秒数で設定します。この遅延時間は、ルータのリロード後初めてインターフェイスがアップになる際のみ適用されます。 （任意） sync : IP 冗長クライアントの最大同期化時間を秒数で設定します。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 5 <code>standby [group-number] priority priority</code>	アクティブ ルータを選択するときに使用される priority 値を設定します。指定できる範囲は 1 ~ 255 です。デフォルトのプライオリティは 100 です。最大の値が、最高のプライオリティを表します。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show standby [interface-id [group-number]]</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	（任意） コンフィギュレーション ファイルに設定を保存します。

IPv6 HSRP をディセーブルにするには、**no standby [group-number] ipv6** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのグループ 1 で IPv6 HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、IPv6 HSRP を使用して学習されます。



(注)

これは、IPv6 HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

■ IPv6 の表示

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

IPv6 HSRP の設定の詳細については、Cisco.com にある『Cisco IOS IPv6 Configuration Library』の「Configuring First Hop Redundancy Protocols in IPv6」の章を参照してください。

IPv6 の表示

コマンドの構文と使い方については『Cisco IOS Command Reference』を参照してください。

表 39-2 に、スイッチ上で IPv6 をモニタするための特権 EXEC コマンドを示します。

表 39-2 IPv6 のモニタ用コマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 CEF を表示します。
show ipv6 interface <i>interface-id</i>	IPv6 インターフェイスのステータスおよび設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 39-3 に、EIGRP IPv6 情報を表示するための特権 EXEC コマンドを示します。

表 39-3 EIGRP IPv6 情報を表示するコマンド

コマンド	目的
show ipv6 eigrp [<i>as-number</i>] <i>interface</i>	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [<i>as-number</i>] <i>neighbor</i>	EIGRP IPv6 が検出したネイバーを表示します。
show ipv6 eigrp [<i>as-number</i>] <i>traffic</i>	送受信された EIGRP IPv6 パケット数を表示します。
show ipv6 eigrp topology [<i>as-number</i> <i>ipv6-address</i>] [<i>active</i> <i>all-links</i> <i>detail-links</i> <i>pending</i> <i>summary</i> <i>zero-successors</i>]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

表 39-4 に、IPv4 および IPv6 アドレス タイプに関する情報を表示するための特権 EXEC コマンドを示します。

表 39-4 IPv4 および IPV6 アドレス タイプを表示するコマンド

コマンド	目的
show ip http server history	HTTP サーバに対する過去 20 件の接続を表示します。アクセスした IP アドレスおよび接続を終了した時刻が含まれます。
show ip http server connection	HTTP サーバに対する現在の接続を表示します。ローカル IP アドレスおよびアクセスしているリモート IP アドレスが含まれます。
show ip http client connection	HTTP サーバに対する HTTP クライアント接続の設定値を表示します。
show ip http client history	HTTP クライアントがサーバに対して行った最後の 20 の要求を表示します。

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
  3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
<output truncated>
```

次に、**show ipv6 cef** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to FastEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to FastEthernet2/0/43
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
```

```

3FFE:C000:16A:1::/64
  attached to Loopback10
3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<output truncated>

```

次に、**show ipv6 protocols** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
  None

```

次に、**show ipv6 rip** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
  Administrative distance is 120.Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
    FastEthernet2/0/4
    FastEthernet2/0/11
    FastEthernet1/0/12
Redistribution:
  None

```

次に、**show ipv6 static** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1

```

次に、**show ipv6 neighbor** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
3FFE:C000:0:7::777                         - 0007.0007.0007 REACH V17
3FFE:C101:113:1::33                        - 0000.0000.0033 REACH Fa1/0/13

```

次に、**show ipv6 route** 特権 EXEC コマンドの出力例を示します。

```

Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L   FF00::/8 [0/0]
    via Null0, receive

```

次に、**show ipv6 traffic** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd: 1 total, 1 local destination
        0 source-routed, 0 truncated
        0 format errors, 0 hop count exceeded
        0 bad header, 0 unknown option, 0 bad source
        0 unknown protocol, 0 not a router
        0 fragments, 0 total reassembled
        0 reassembly timeouts, 0 reassembly failures
  Sent: 36861 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
        0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```




CHAPTER 40

IPv6 MLD スヌーピングの設定

Catalyst 3750 スイッチで Multicast Listener Discovery (MLD) スヌーピングを使用すれば、スイッチドネットワーク内のクライアントおよびルータへ IPv6 マルチキャストデータを効率的に配信することができます。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチスタックを意味します。



(注) IPv6 を使用するには、デュアル IPv4 および IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートが設定されている必要があります。テンプレートの選択は、**sdm prefer dual-ipv4-and-ipv6 {default | vlan} [desktop]** グローバル コンフィギュレーション コマンドで行います。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、[第 8 章「SDM テンプレートの設定」](#)を参照してください。
- スイッチの IPv6 については、[第 39 章「IPv6 ユニキャストルーティングの設定」](#)を参照してください。



(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「[MLD スヌーピングの概要](#)」 (P.40-1)
- 「[IPv6 MLD スヌーピングの設定](#)」 (P.40-5)
- 「[MLD スヌーピング情報の表示](#)」 (P.40-12)

MLD スヌーピングの概要

IP バージョン 4 (IPv4) では、レイヤ 2 スイッチは Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピングを使用して、ダイナミックにレイヤ 2 インターフェイスを設定することにより、マルチキャストトラフィックのフラッドを抑制します。そのため、マルチキャストトラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN (仮想 LAN) 内のすべてのポートにフラッドされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、直接接続されたリンク上のマルチキャストリスナー (IPv6 マルチキャスト パケットを受信するノード) の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1 (MLDv1) は IGMPv2 と、MLD バージョン 2 (MLDv2) は IGMPv3 とそれぞれ同等です。MLD は ICMP バージョン 6 (ICMPv6) のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピングは MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 Basic Snooping (MBSS) は MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。



(注)

スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 Enhanced Snooping (MESS) をサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できません。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレス テーブルはソフトウェアで構築され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。そのあと、スイッチはハードウェアで IPv6 マルチキャスト アドレスに基づくブリッジングを実行します。

次に、IPv6 MLD スヌーピングの一部のパラメータについて説明します。

- 「MLD メッセージ」 (P.40-2)
- 「MLD クエリー」 (P.40-3)
- 「マルチキャスト クライアント エージングの堅牢性」 (P.40-3)
- 「マルチキャスト ルータ検出」 (P.40-3)
- 「MLD レポート」 (P.40-4)
- 「MLD Done メッセージおよび即時脱退」 (P.40-4)
- 「TCN 処理」 (P.40-5)
- 「スイッチ スタック内の MLD スヌーピング」 (P.40-5)

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query : IGMPv2 クエリーと同等で、General Query または Multicast-Address-Specific Query (MASQ) のいずれかになります。
- Multicast Listener Report : IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ : IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに回答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびステティックな IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。



(注)

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が使用されている場合、Catalyst 6500 スイッチの拡張 VLAN で IPv6 MLD スヌーピングをイネーブルにして、Catalyst 3750 スイッチが VLAN のクエリーを受信できるようにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに回答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ (IGMP Leave メッセージと同等) を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチは メッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバシップの削除を設定できます。1 つのアドレスに対するメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合だけです。デフォルト値は 2 です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。

- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合だけです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかに関わらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出されたあとは、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してだけ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポート が受信されると、IPv6 マルチキャスト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに入力されます。そのあと、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバー ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLD Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でだけこの機能を使用します。ポートがグループの最後のメンバーである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、`ipv6 mld snooping last-listener-query count` グローバル コンフィギュレーション コマンドにより設定されます。デフォルト値は 2 です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定されます。削除されたポートがマルチキャスト アドレスの最後のメンバーである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、Topology Change Notification (TCN; トポロジ変更通知) 送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにだけマルチキャスト データの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

スイッチ スタック内の MLD スヌーピング

スイッチが IPv6 マルチキャスト グループを学習したかどうかには関係なく、MLD IPv6 グループおよび MAC アドレス データベースはスタック内のすべてのスイッチ上で保持されます。レポート抑制およびプロキシ レポーティングはスタック全体で実行されます。スイッチがレポートを受信したかどうかには関係なく、最大応答時間の間にグループに対して受信された 1 つのレポートだけがマルチキャスト ルータに転送されます。

新しいスタック マスターの選出は IPv6 マルチキャスト データの学習またはブリッジングには影響せず、スタック マスターの再選出の間も IPv6 マルチキャスト データのブリッジングは停止しません。新しいスイッチがスタックに追加されると、スタック マスターから学習した IPv6 マルチキャスト 情報との同期が取られます。同期が完了するまで、新しく追加されたスイッチに入力されたデータは不明なマルチキャスト データとして扱われます。

IPv6 MLD スヌーピングの設定

次に、IPv6 MLD スヌーピングの設定方法について説明します。

- 「MLD スヌーピングのデフォルト設定」 (P.40-6)
- 「MLD スヌーピング設定時の注意事項」 (P.40-6)
- 「MLD スヌーピングのイネーブル化またはディセーブル化」 (P.40-7)
- 「スタティックなマルチキャスト グループの設定」 (P.40-8)
- 「マルチキャスト ルータ ポートの設定」 (P.40-8)
- 「MLD 即時脱退のイネーブル化」 (P.40-9)
- 「MLD スヌーピング クエリーの設定」 (P.40-10)
- 「MLD リスナー メッセージ抑制のディセーブル化」 (P.40-11)

MLD スヌーピングのデフォルト設定

表 40-1 に、MLD スヌーピングのデフォルト設定を示します。

表 40-1 MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング (グローバル)	ディセーブル
MLD スヌーピング (VLAN 単位)	イネーブル。VLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル : 2、VLAN 単位 : 0。 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル : 2、VLAN 単位 : 0。 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル : 1000 (1 秒)、VLAN : 0。 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2
MLD リスナー抑制	イネーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が使用されている場合、Catalyst 6500 スイッチの拡張 VLAN で IPv6 MLD スヌーピングをイネーブルにして、Catalyst 3750 スイッチが VLAN のクエリーを受信できるようにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックで保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチ スタックで保持可能なアドレス エントリの最大数は 1000 です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでだけイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping</code>	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 5	<code>reload</code>	OS (オペレーティング システム) をリロードします。

スイッチで MLD スヌーピングをグローバルにディセーブルにするには、`no ipv6 mld snooping` グローバル コンフィギュレーション コマンドを使用します。

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。



(注) IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が使用されている場合、Catalyst 6500 スイッチの拡張 VLAN で IPv6 MLD スヌーピングをイネーブルにして、Catalyst 3750 スイッチが VLAN のクエリーを受信できるようにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要はありません。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping</code>	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	<code>ipv6 mld snooping vlan <i>vlan-id</i></code>	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定の VLAN 番号に対して `no ipv6 mld snooping vlan vlan-id` グローバル コンフィギュレーション コマンドを使用します。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよび メンバー ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping vlan <i>vlan-id</i> static <i>ipv6_multicast_address</i> interface <i>interface-id</i>	マルチキャスト グループのメンバーとしてレイヤ 2 ポートにマルチキャスト グループをスタティックに設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> は、マルチキャスト グループの VLAN ID です。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 <i>ipv6_multicast_address</i> は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 <i>interface-id</i> は、メンバー ポートです。物理インターフェイスまたはポート チャネル (1 ~ 48) に設定できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping multicast-address user または show ipv6 mld snooping multicast-address vlan <i>vlan-id</i> user	スタティックなメンバー ポートおよび IPv6 アドレスを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ipv6 mld snooping vlan *vlan-id* static *mac-address* interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。グループからすべてのメンバー ポートが削除された場合、このグループは削除されます。

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/0/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定

MLD スヌーピングでは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習しますが、CLI (コマンドライン インターフェイス) を使用しても VLAN にマルチキャスト ルータ ポートを追加できます。マルチキャスト ルータ ポートを追加する (マルチキャスト ルータにスタティック接続を追加する) には、スイッチで **ipv6 mld snooping vlan *mrouter*** グローバル コンフィギュレーション コマンドを使用します。



(注)

マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></code>	マルチキャスト ルータの VLAN ID、およびマルチキャスト ルータにインターフェイスを指定します。 <ul style="list-style-type: none"> VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 インターフェイスは物理インターフェイスにすることもポート チャネルにすることもできます。指定できるポート チャネルの範囲は 1 ～ 48 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>]</code>	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ipv6 mld snooping vlan *vlan-id* mrouter interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにはなりません。

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave</code>	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ipv6 mld snooping vlan <i>vlan-id</i></code>	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN で MLD 即時脱退をディセーブルにするには、**no ipv6 mld snooping vlan *vlan-id* immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピング クエリーの設定

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 mld snooping robustness-variable value</code>	(任意) スイッチが一般クエリーに応答しないリスナー (ポート) を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ~ 3 です。デフォルトは 2 です。
ステップ 3	<code>ipv6 mld snooping vlan vlan-id robustness-variable value</code>	(任意) VLAN 単位で堅牢性変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージングアウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ~ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	<code>ipv6 mld snooping last-listener-query-count count</code>	(任意) MLD クライアントがエージングアウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ~ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。
ステップ 5	<code>ipv6 mld snooping vlan vlan-id last-listener-query-count count</code>	(任意) VLAN 単位で最後のリスナー クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ~ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1 秒後に送信されます。
ステップ 6	<code>ipv6 mld snooping last-listener-query-interval interval</code>	(任意) スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ~ 32,768 ミリ秒です。デフォルト値は 1000 (1 秒) です。
ステップ 7	<code>ipv6 mld snooping vlan vlan-id last-listener-query-interval interval</code>	(任意) VLAN 単位で最後のリスナー クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ~ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	<code>ipv6 mld snooping tcn query solicit</code>	(任意) TCN 送信請求をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してだけ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	<code>ipv6 mld snooping tcn flood query count count</code>	(任意) TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ~ 10 で、デフォルトは 2 です。
ステップ 10	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>show ipv6 mld snooping querier [vlan vlan-id]</code>	(任意) スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。
ステップ 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートだけを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no ipv6 mld snooping listener-message-suppression	MLD メッセージ抑制をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD メッセージ抑制を再びイネーブルにするには、**ipv6 mld snooping listener-message-suppression** グローバル コンフィギュレーション コマンドを使用します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには、表 40-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 40-2 MLD スヌーピング情報表示用のコマンド

コマンド	目的
<code>show ipv6 mld snooping [vlan <i>vlan-id</i>]</code>	<p>スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>]</code>	<p>動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping querier [vlan <i>vlan-id</i>]</code>	<p>VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレス および着信ポートに関する情報を表示します。</p> <p>(任意) vlan <i>vlan-id</i> を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping multicast-address [vlan <i>vlan-id</i>] [count dynamic user]</code>	<p>スイッチまたは VLAN のすべてあるいは特定の IPv6 マルチキャスト アドレス情報を表示します。</p> <ul style="list-style-type: none"> • count を入力して、スイッチまたは VLAN のグループ数を表示します。 • dynamic を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • user を入力して、スイッチまたは VLAN の MLD スヌーピングユーザ設定グループ情報を表示します。
<code>show ipv6 mld snooping multicast-address vlan <i>vlan-id</i> [<i>ipv6-multicast-address</i>]</code>	<p>指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。</p>



CHAPTER 41

IPv6 ACL の設定

この章では、Catalyst 3750 スイッチに IPv6 ACL を設定する方法について説明します。IP バージョン 6 (IPv6) Access Control List (ACL; アクセス コントロール リスト) を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP バージョン 4 (IPv4) の名前付き ACL を作成し、適用する方法と同じです。入力ルータ ACL を作成して適用し、レイヤ 3 管理トラフィックをフィルタリングすることもできます。

特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチスタックを意味します。



(注) IPv6 を使用するには、デュアル IPv4 および IPv6 Switch Database Management (SDM; スイッチ データベース管理) テンプレートが設定されている必要があります。テンプレートの選択は、**sdm prefer {default | dual-ipv4-and-ipv6}** グローバル コンフィギュレーション コマンドで行います。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、[第 8 章「SDM テンプレートの設定」](#)を参照してください。
- スイッチの IPv6 については、[第 5 章「スイッチスタックの管理」](#)を参照してください。
- スイッチの ACL については、[第 41 章「IPv6 ACL の設定」](#)を参照してください。



(注) この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「IPv6 ACL の概要」(P.41-2)
- 「IPv6 ACL の設定」(P.41-4)
- 「IPv6 ACL の表示」(P.41-9)

IPv6 ACL の概要

スイッチ スタック イメージは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL
 - ルーテッド ポート、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、またはレイヤ 3 EtherChannel などのレイヤ 3 インターフェイスの発信トラフィックまたは着信トラフィックでサポートされます。
 - 経路選択済みの IPv6 パケットだけに適用されます。
- IPv6 ポート ACL
 - レイヤ 2 インターフェイスのインバウンドトラフィックだけサポートされます。
 - インターフェイスに届くすべての IPv6 パケットに適用されます。

IP ベース イメージが稼動するスイッチ スタックは、入力ルータ IPv6 ACL だけをサポートします。ポート ACL や出力 IPv6 ルータ ACL をサポートしません。



(注) 未サポートの IPv6 ACL を設定すると、エラーメッセージが表示されて設定が有効になりません。

スイッチは、IPv6 トラフィックの VLAN (仮想 LAN) ACL (VLAN マップ) をサポートしません。



(注) スイッチでの ACL サポートの詳細については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。

IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。その他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされません。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。その他のパケットはフィルタリングされません。



(注) インターフェイスに任意のポート ACL (IPv4、IPv6、または MAC) が適用される場合、このポート ACL はパケットのフィルタリングで使用され、ポート VLAN の SVI に付加されたルータ ACL はすべて無視されます。

ここでは、スイッチの IPv6 ACL の特性の一部について説明します。

- 「サポートされる ACL 機能」(P.41-3)
- 「IPv6 ACL の制限事項」(P.41-3)
- 「IPv6 ACL とスイッチ スタック」(P.41-4)

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム (IPv4 では **fragments** キーワード) がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スwitchの Ternary CAM (TCAM) スペースが不足している場合、ACL ラベルに対応付けられたパケットは CPU に転送され、ACL はソフトウェアで適用されます。
- ホップバイホップ オプションがあるルーテッドパケットまたはブリッジドパケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

IPv6 ACL の制限事項

IPv4 では、番号付きの標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- IPv6 送信元および宛先アドレス：ACL 照合は、Extended Universal Identifier (EUI) -64 形式の /0 ~ /64 のプレフィクスおよびホストアドレス (/128) だけサポートされます。スイッチは、情報損失のない次のホストアドレスだけをサポートします。
 - 集約可能なグローバルユニキャストアドレス
 - リンクに対してローカルなアドレス
- スwitchは、**flowlabel**、**routing header**、および **undetermined-transport** の各キーワードの照合をサポートしません。
- スwitchは再起 ACL (**reflect** キーワード) をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL (VLAN マップ) はサポートしていません。
- スwitchは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- スwitchは出力 ポート ACL をサポートしません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、スイッチ スタックだけでサポートされます。スイッチは、コントロールプレーン (着信) IPv6 ACL だけをサポートします。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかに関わらず、制限事項はありません。ハードウェア転送が必要なインターフェイス (物理ポートまたは SVI) に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つ Access Control Entry (ACE; アクセス コントロール エントリ) を追加しようとする場合、スイッチは現在インターフェイスに接続されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。



(注)

スイッチ スタック内で IPv6 を機能させるには、すべてのスタック メンバーで拡張 IP サービス イメージを実行している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。メンバー スイッチは、新しいスタック マスターによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 ACL を設定する場合は、事前にデュアル IPv4/IPv6 SDM テンプレートのいずれかを選択する必要があります。

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

- ステップ 1** IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
- ステップ 2** IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。
- ステップ 3** インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

ここでは、IPv6 ACL の設定および適用方法について説明します。

- 「IPv6 ACL のデフォルト設定」(P.41-4)
- 「他の機能との相互作用」(P.41-5)
- 「IPv6 ACL の作成」(P.41-5)
- 「インターフェイスへの IPv6 ACL の適用」(P.41-8)

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能との相互作用

IPv6 ACL の設定には、他の機能またはスイッチ特性と次の相互作用があります。

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットは廃棄されます。パケットのコピーが **Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル)** キューに送信され、フレームに **ICMP 到達不能メッセージ** が生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスタックに作成したり、同一インターフェイスに適用したりできます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとする、エラー メッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（たとえば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- TCAM が満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ipv6 access-list <i>access-list-name</i></code>	IPv6 アクセス リスト名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3a <code>deny permit protocol</code> <code>{source-ipv6-prefix/prefix-length </code> <code>any host source-ipv6-address}</code> <code>[operator [port-number]]</code> <code>{destination-ipv6-prefix/</code> <code>prefix-length any </code> <code>host destination-ipv6-address}</code> <code>[operator [port-number]]</code> <code>[dscp value] [fragments] [log]</code> <code>[log-input] [sequence value]</code> <code>[time-range name]</code>	<p>deny または permit を入力し、条件と一致した場合にパケットを拒否するか、または許可するかを指定します。次に、条件について説明します。</p> <ul style="list-style-type: none"> <code>protocol</code> には、インターネットプロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp または IPv6 プロトコル番号を表す 0 ~ 255 の整数を使用できます。ICMP、TCP、および UDP の具体的なパラメータについては、ステップ 3b ~ 3d を参照してください。 <code>source-ipv6-prefix/prefix-length</code> または <code>destination-ipv6-prefix/prefix-length</code> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、16 ビット値を使用したコロン区切りの 16 進形式で指定されます (RFC 2373 を参照)。 <p>(注) CLI (コマンドライン インターフェイス) ヘルプでは、/0 ~ /128 の範囲のプレフィクス長が表示されますが、スイッチは、集約可能なグローバルユニキャストアドレスとリンクに対してローカルなホストアドレスの /0 ~ /64 の範囲のプレフィクス、および EUI ベースの /128 プレフィクスに対する IPv6 アドレス照合だけをサポートします。</p> <ul style="list-style-type: none"> IPv6 プレフィクス <code>::/0</code> の短縮形として、any を入力します。 <code>host source-ipv6-address</code> または <code>destination-ipv6-address</code> には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスは 16 ビット値を使用したコロン区切りの 16 進形式で指定されます。 (任意) <code>operator</code> には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドは、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、range (包含範囲) などです。 <p><code>source-ipv6-prefix/prefix-length</code> 引数のあとのオペレータは、送信元ポートに一致する必要があります。<code>destination-ipv6-prefix/prefix-length</code> 引数のあとのオペレータは、宛先ポートに一致する必要があります。</p> <ul style="list-style-type: none"> (任意) <code>port-number</code> は、TCP または UDP のフィルタリングで、それぞれ 0 ~ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 (任意) <code>dscp value</code> を入力して、各 IPv6 パケットヘッダーの Traffic Class フィールド内のトラフィッククラス値と DiffServ コードポイント値を照合します。指定できる範囲は 0 ~ 63 です。 (任意) <code>fragments</code> を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 (任意) <code>log</code> を指定すると、エントリと一致するパケットに関するロギングメッセージがコンソールに送信されます。<code>log-input</code> を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 (任意) <code>sequence value</code> を入力して、アクセスリストステートメントのシーケンス番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 (任意) <code>time-range name</code> を入力して、ステートメントの時間の範囲を指定します。

コマンド	目的
ステップ 3b deny permit tcp <code>{source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port protocol}] [psh] [range {port protocol}] [rst] [sequence value] [syn] [time-range name] [urg]</code>	(任意) TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 <ul style="list-style-type: none"> • ack : 確認応答ビット セット • established : 確立された接続。TCP データグラムに ACK または RST ビット セットが含まれる場合は、照合が行われます。 • fin : 終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port protocol} : 所定のポート番号上にないパケットだけを照合します。 • psh : プッシュ機能ビット セット • range {port protocol} : ポート番号の範囲内のパケットだけを照合します。 • rst : リセット ビット セット • syn : 同期ビット セット • urg : 緊急ポインタ ビット セット
ステップ 3c deny permit udp <code>{source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port protocol}] [range {port protocol}] [sequence value] [time-range name]</code>	(任意) UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、 udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、 <code>[operator [port]]</code> のポート番号またはポート名は、UDP ポートの番号または名前であればなりません。UDP の場合、 established パラメータは無効です。
ステップ 3d deny permit icmp <code>{source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [operator [port-number]] [icmp-type [icmp-code] icmp-message] [dscp value] [log] [log-input] [sequence value] [time-range name]</code>	(任意) ICMP アクセス リストおよびアクセス条件を定義します。 ICMP の場合は、 icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • icmp-type : ICMP メッセージタイプを基準にしてフィルタリングします。0 ~ 255 の値を使用できます。 • icmp-code : ICMP メッセージコードタイプを基準にしてフィルタリングします。0 ~ 255 の値を使用できます。 • icmp-message : ICMP メッセージタイプ名または ICMP メッセージのタイプ名およびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定のアクセス リストから拒否または許可条件を削除するには、キーワードを指定して **no deny** | **permit IPv6** アクセスリスト コンフィギュレーション コマンドを使用します。

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番目の拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、2 番目の拒否エントリは、コンソールにすべて的一致結果を記録します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番目の許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番目の許可エントリは必要です。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。ACL をレイヤ 3 インターフェイスの発信または着信トラフィック、あるいはレイヤ 2 インターフェイスの着信トラフィックに適用することができます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	アクセス リストを適用するレイヤ 2 インターフェイス (ポート ACL 用) またはレイヤ 3 インターフェイス (ルータ ACL 用) を特定して、インターフェイス コンフィギュレーション モードを開始します。 (注) IP ベース イメージを稼働中のスイッチは、ポート ACL をサポートしていません。
ステップ 3	no switchport	ルータ ACL を適用する場合は、インターフェイスをレイヤ 2 モード (デフォルト) からレイヤ 3 モードに変更します。
ステップ 4	ipv6 address ipv6-address	レイヤ 3 インターフェイス (ルータ ACL 用) で IPv6 アドレスを設定します。 このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。
ステップ 5	ipv6 traffic-filter access-list-name {in out}	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。 out キーワードはレイヤ 2 インターフェイス (ポート ACL) ではサポートされません。stack で IP ベース イメージを稼働している場合、 out キーワードはレイヤ 3 インターフェイスではサポートされません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	アクセス リストの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスからアクセス リストを削除するには、**no ipv6 traffic-filter access-list-name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト *Cisco* を適用する例を示します。

```
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示するには、表 41-1 に示された 1 つまたは複数の特権 EXEC コマンドを使用します。

表 41-1 IPv6 アクセス リスト情報を表示するコマンド

コマンド	目的
show access-lists	スイッチに設定されたすべてのアクセス リストを表示します。
show ipv6 access-list [<i>access-list-name</i>]	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
  10 permit ip any any
IPv6 access list ipv6
  permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30

IPv6 access list outbound
  deny udp any any sequence 10
  deny tcp any any eq telnet sequence 20
```




CHAPTER 42

HSRP の設定

この章では、Catalyst 3750 スイッチで Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) を使用する方法について説明します。HSRP は、Internet Protocol (IP) トラフィック ルーティングに冗長性を提供し、1 台のルータの可用性に依存しないルーティングを実現します。IPv4 の HSRP は、IP ベース イメージまたは IP サービス イメージが実行されているスイッチ上でだけサポートされます。IPv6 HSRP を使用するには、第 39 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンド スイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンド スイッチを設定することもできます。クラスタリングの詳細については、第 6 章「スイッチのクラスタ化」、および Cisco.com で利用できる『*Getting Started with Cisco Network Assistant*』を参照してください。

この章で使用するコマンドの構文および使用方法の詳細については、次のマニュアルを参照してください。

- このリリースのスイッチ コマンド リファレンス
- 『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*』 Release 12.2。次の URL にアクセスしてください。
http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
- 『*Hot Standby Router Protocol Version 2*』 フィーチャ モジュール。次の URL にアクセスしてください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthsrpv2.html

この章で説明する内容は、次のとおりです。

- 「HSRP の概要」 (P.42-2)
- 「HSRP の設定」 (P.42-5)
- 「HSRP 設定の表示」 (P.42-14)

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE (米国電気電子学会) 802 LAN 上の IP ホストファースト ホップに冗長性を確保しネットワークの可用性を高めるシスコの標準方式です。HSRP を使用すると、特定のルータの可用性に依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC (メディア アクセス制御) アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになります。HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。相互にバックアップ機能を提供するように設定されている複数のルータに、共通のターゲットを表すルータです。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。



(注)

HSRP グループ内のルータには、Catalyst 3750 ルーテッド ポート、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRP は、ネットワーク上のホストからの IP トラフィックに冗長性を提供することで、ネットワークの可用性を高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または設定条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

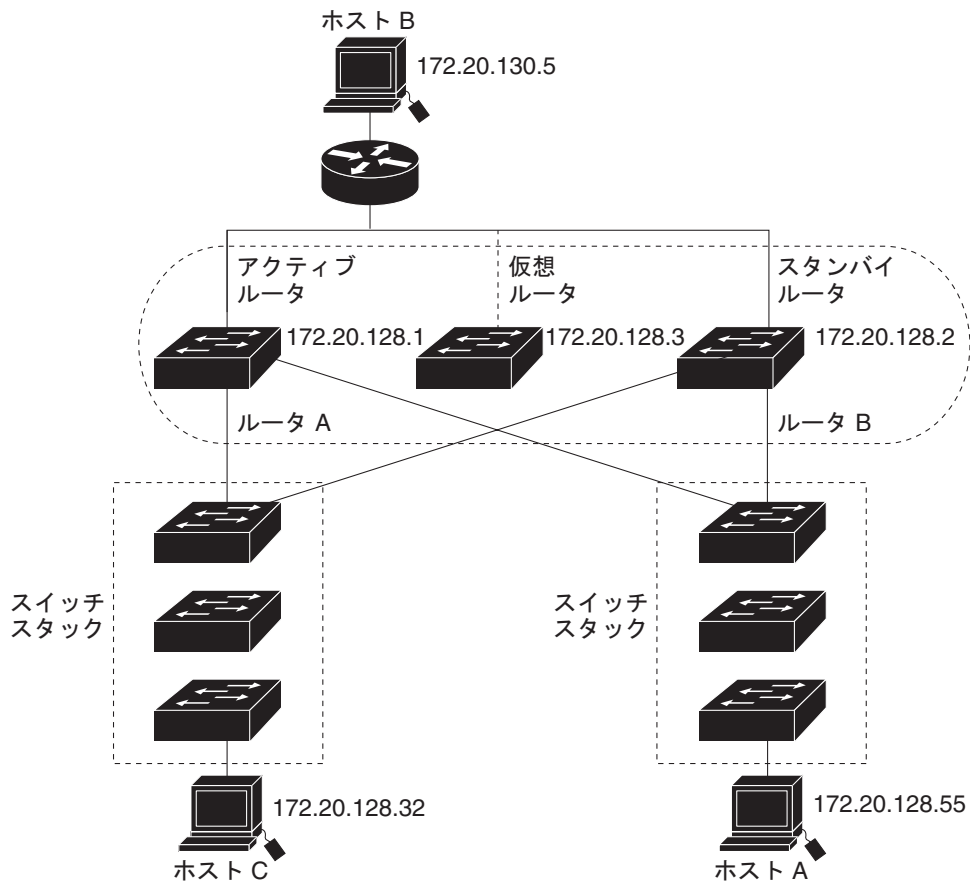
HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRP が動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛のパケットを受信し、ルーティングします。 n 台のルータで HSRP が稼働している場合、 $n + 1$ 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRP が稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスでは Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) のリダイレクト メッセージがデフォルトでディセーブルとなっています。

レイヤ 3 で動作する Catalyst 3750 スイッチおよびスイッチ スタック間で複数のホットスタンバイ グループを設定すると、冗長ルータをさらに活用できます。そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ 1 のインターフェイスをアクティブ ルータ、スイッチ 2 のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ 2 の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

図 42-1 に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルト ルータである仮想ルータの IP アドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの伝送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに回答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザと通信する必要があるホスト C のセグメント上のユーザに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 42-1 HSRP の一般的な構成



204346

HSRP バージョン

スイッチは次の Hot Standby Redundancy Protocol (HSRP) バージョンをサポートします。

- HSRPv1 (HSRP のバージョン 1)。HSRP のデフォルトバージョンです。次の機能があります。
 - 指定できる HSRP グループ番号の範囲は 0 ~ 255 です。
 - HSRPv1 はマルチキャスト アドレス 224.0.0.2 を使用して hello パケットを送信します。この処理は CGMP の脱退処理と競合することがあります。HSRPv1 と CGMP を同時にイネーブルにすることはできません。両者は相互に排他的です。
- HSRPv2 (HSRP のバージョン 2) には、次の機能があります。
 - HSRP グループ番号とサブインターフェイスの VLAN ID を対応させるため、HSRPv2 では 0 ~ 4095 の範囲のグループ番号と 0000.0C9F.F000 ~ 0000.0C9F.FFFF の範囲の MAC アドレスを使用できます。
 - HSRPv2 はマルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。HSRPv2 と CGMP の脱退処理は相互に排他的ではありません。両者を同時にイネーブルにできます。
 - HSRPv2 と HSRPv1 のパケット フォーマットは異なっています。

HSRPv1 が稼動するスイッチは hello パケットを送信した物理ルータを識別できません。これはルータの発信元 MAC アドレスが仮想 MAC アドレスだからです。

HSRPv2 と HSRPv1 のパケット フォーマットは異なっています。HSRPv2 パケットは Type-Length-Value (TLV) フォーマットを使用し、パケットを送信した物理ルータの MAC アドレスが含まれている 6 バイトの識別情報フィールドがあります。

HSRPv1 を実行するインターフェイスが HSRPv2 パケットを受信した場合、このタイプフィールドは無視されます。

Multiple HSRP

スイッチは Multiple HSRP (MHSRP) をサポートします。これは HSRP の拡張版で、複数の HSRP グループ間でロードシェアリングが可能です。ホストネットワークからサーバネットワークまで、ロードバランシングを実現して複数のスタンバイグループ（およびパス）を使用するために、MHSRP を設定できます。図 42-2 では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立しています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブルータになり、ルータ B がスタンバイルータとなります。グループ 2 では、ルータ B に最高のプライオリティが割り当てられているので、ルータ B がデフォルトのアクティブルータになり、ルータ A がスタンバイルータとなります。通常の運用では、2 つのルータが IP トラフィック負荷を共有します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

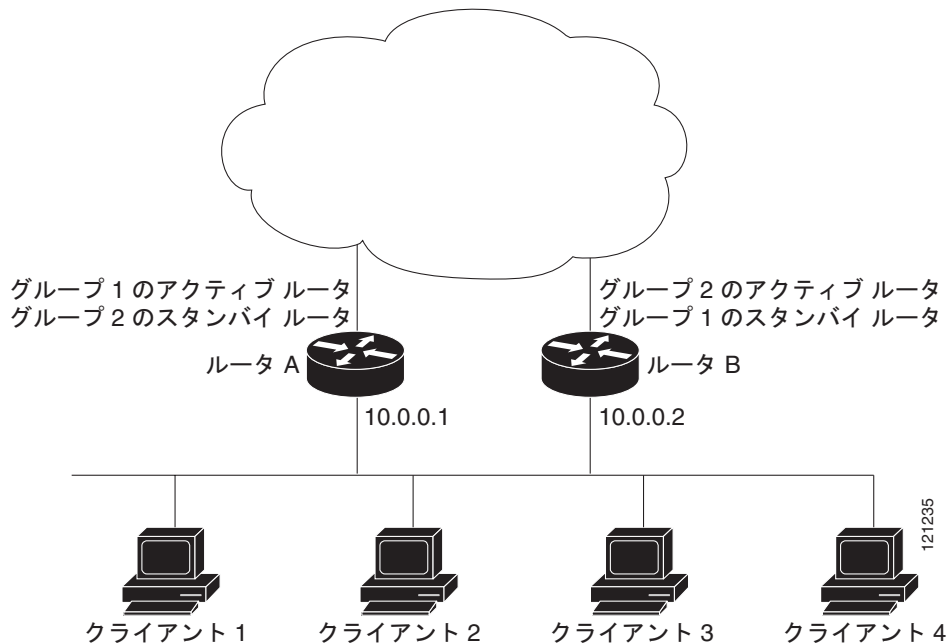
設定手順の例については、「[MHSRP の設定](#)」(P.42-11) を参照してください。



(注)

MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプトによりロードシェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 42-2 MHSRP ロードシェアリング



HSRP およびスイッチ スタック

HSRP の hello メッセージは、スタック マスターで生成されます。HSRP がアクティブであるスタック マスターに障害が発生すると、HSRP アクティブ ステートのフラッピングが生じることがあります。これは、新規スタック マスターが選択および初期化されている間に HSRP hello メッセージが生成されず、スタック マスターが故障したあとでないとスタンバイ ルータがアクティブにならない可能性があるためです。

HSRP の設定

ここでは、次の設定情報について説明します。

- 「[HSRP のデフォルト設定](#)」 (P.42-6)
- 「[HSRP 設定時の注意事項](#)」 (P.42-6)
- 「[HSRP のイネーブル化](#)」 (P.42-7)
- 「[HSRP のプライオリティの設定](#)」 (P.42-8)
- 「[MHSRP の設定](#)」 (P.42-11)
- 「[HSRP 認証およびタイマーの設定](#)」 (P.42-11)
- 「[ICMP リダイレクト メッセージの HSRP サポートのイネーブル化](#)」 (P.42-13)
- 「[HSRP グループおよびクラスタリングの設定](#)」 (P.42-13)
- 「[HSRP のトラブルシューティング](#)」 (P.42-13)

HSRP のデフォルト設定

表 42-1 に HSRP のデフォルト設定を示します。

表 42-1 HSRP のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	システムへの割り当て : 0000.0c07.acXX (XX は HSRP グループ番号)
スタンバイ プライオリティ	100
スタンバイ遅延	0 (遅延なし)
スタンバイでのインターフェイス プライオリティのトラッキング	10
スタンバイ hello タイム	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

HSRP を設定する場合は、次の注意事項に従ってください。

- IPv4 HSRP と IPv6 HSRP は相互に排他的です。両者を同時にイネーブルにすることはできません。
- HSRPv2 と HSRPv1 は相互に排他的です。インターフェイス上で HSRPv2 は HSRPv1 と相互運用ができません。またその逆も同様です。
- HSRP グループ インスタンスは 32 まで設定できます。

複数のインターフェイス上に同じ HSRP グループ番号を設定した場合、スイッチはそれぞれのインターフェイスを 1 つのインスタンスとして数えます。

たとえば、VLAN 1 とポート 1 上に HSRP グループ 0 を設定すると、スイッチはこれを 2 つのインスタンスとして数えます。

- 設定手順では、次に示すレイヤ 3 インターフェイスを指定する必要があります。
 - ルーテッド ポート : **no switchport** インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。
 - SVI : **interface vlan vlan_id** グローバル コンフィギュレーション コマンドによって作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
 - レイヤ 3 モードの EtherChannel ポート チャンネル : **interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用し、イーサネット インターフェイスをチャンネル グループにバインドして作成されたポート チャンネル論理インターフェイスです。詳細については、「レイヤ 3 EtherChannel の設定」を参照してください。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。「レイヤ 3 インターフェイスの設定」(P.12-28) を参照してください。
- 1 つの HSRP インスタンスのみ設定してください。スイッチは HSRPv1、HSRPv2、および IPv6 HSRP をサポートします。

- HSRP グループのバージョンは、グループ番号が 256 未満である場合にだけ HSRPv2 から HSRPv1 に変更できます。
- HSRPv2 と IPv6 HSRP のグループ番号を設定する際は、256 の倍数の範囲に含まれるグループ番号を使用する必要があります。たとえば、0 ～ 255、256 ～ 511、512 ～ 767、3840 ～ 4095 などが有効な範囲です。

有効なグループ番号と無効なグループ番号の例を次に示します。

- グループ番号に 2、150、および 225 を設定した場合、別のグループに番号 3850 を設定することはできません。この番号は 0 ～ 255 の範囲ではありません。
- グループ番号に 520、600、および 700 を設定した場合、別のグループに番号 900 を設定することはできません。この番号は 512 ～ 767 の範囲ではありません。
- インターフェイス上で HSRP バージョンを変更すると、新しい仮想 MAC アドレスを持ったことにより各 HSRP グループはリセットされます。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドを実行すると、設定されたインターフェイスで HSRP がアクティブになります。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によって学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上でイネーブルに設定され、プロキシ Address Resolution Protocol (ARP; アドレス解決プロトコル) がイネーブルの場合、インターフェイスのホットスタンバイ ステートがアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイ グループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

レイヤ 3 インターフェイス上で HSRP を作成する場合、またはイネーブルにする場合は、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	インターフェイス コンフィギュレーション モードを開始し、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3 standby version {1 2}	(任意) インターフェイスに HSRP バージョンを設定します。 <ul style="list-style-type: none"> • 1 : HSRPv1 を選択します。 • 2 : HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョン (HSRPv1) を実行します。

コマンド	目的
ステップ 4 standby [<i>group-number</i>] ip [<i>ip-address</i>] [<i>secondary</i>]]	<p>HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。</p> <ul style="list-style-type: none"> （任意） <i>group-number</i> : HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 255 で、デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 （1 つのインターフェイスで必須、それ以外は任意） <i>ip-address</i> : ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 （任意） <i>secondary</i> : IP アドレスはセカンダリ ホットスタンバイ ルータ インターフェイスです。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show standby [<i>interface-id</i> [<i>group</i>]]	設定を確認します。
ステップ 7 copy running-config startup-config	（任意） コンフィギュレーション ファイルに設定を保存します。

HSRP をディセーブルにするには、**no standby** [*group-number*] **ip** [*ip-address*] インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスのグループ 1 に対して HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。



(注) これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

HSRP のプライオリティの設定

standby priority、**standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドは、いずれも、アクティブ ルータとスタンバイ ルータの特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を検索するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てることにより、アクティブ ルータとスタンバイ ルータの選択ができません。プリエンプトがイネーブルの場合、プライオリティが最高のルータがアクティブ ルータになります。プライオリティが同じ場合、現在のアクティブ ルータは変わりません。
- 最大の値 (1 ~ 255) が、最高のプライオリティ (アクティブ ルータになる確率が最も高い) を表します。

- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード (**priority**、**preempt**、または両方) を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスをトラッキングする場合に有効です。トラッキング対象のインターフェイスが故障すると、トラッキングが設定されていたデバイスのホットスタンバイ プライオリティが 10 減少します。トラッキング対象でないインターフェイスの場合は、そのステータスが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、トラッキングするインターフェイスのリストを個別に設定できます。
- **standby track interface-priority** インターフェイス コンフィギュレーション コマンドを実行すると、トラッキング対象のインターフェイスがダウンした場合のホットスタンバイ プライオリティの減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- **interface-priority** 値が設定されている場合に、複数のトラッキング対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていないトラッキング対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティングテーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティングテーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	インターフェイス コンフィギュレーション モードを開始し、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3 standby [group-number] priority priority [preempt [delay delay]]	<p>アクティブ ルータを選択するときに使用される priority 値を設定します。指定できる範囲は 1 ~ 255 です。デフォルトのプライオリティは 100 です。最大の値が、最高のプライオリティを表します。</p> <ul style="list-style-type: none"> • (任意) group-number : コマンドが適用されるグループ番号です。 • (任意) preempt : ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、アクティブ ルータとして制御を行います。 • (任意) delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 (1 時間) で、デフォルトは 0 です (引き継ぐ前の遅延はありません)。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>

コマンド	目的
ステップ 4 standby [<i>group-number</i>] [priority <i>priority</i>] preempt [<i>delay delay</i>]	<p>ルータを preempt に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとして制御を行います。</p> <ul style="list-style-type: none"> （任意） <i>group-number</i> : コマンドが適用されるグループ番号です。 （任意） priority : グループ プライオリティを設定または変更します。指定できる範囲は 1 ~ 255 です。デフォルトは 100 です。 （任意） delay : ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ~ 3600 (1 時間) で、デフォルトは 0 です (引き継ぐ前の遅延はありません)。 <p>デフォルト値に戻すには、このコマンドの no 形式を使用します。</p>
ステップ 5 standby [<i>group-number</i>] track <i>type number</i> [<i>interface-priority</i>]	<p>他のインターフェイスをトラッキングするようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。</p> <ul style="list-style-type: none"> （任意） <i>group-number</i> : コマンドが適用されるグループ番号です。 <i>type</i> : トラッキング対象のインターフェイス タイプを (インターフェイス番号とともに) 入力します。 <i>number</i> : トラッキング対象のインターフェイス番号を (インターフェイスタイプとともに) 入力します。 （任意） <i>interface-priority</i> : インターフェイスがダウンした場合、または稼動状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show running-config	スタンバイ グループの設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのプライオリティ、プリエンプト、遅延値に戻すには、**no standby** [*group-number*] **priority** *priority* [**preempt** [*delay delay*]] および **no standby** [*group-number*] [**priority** *priority*] **preempt** [*delay delay*] インターフェイス コンフィギュレーション コマンドを使用します。

トラッキングを解除するには、**no standby** [*group-number*] **track** *type number* [*interface-priority*] インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートがアクティブになり、IP アドレスおよびプライオリティ 120 (デフォルト値よりも高いプライオリティ) が設定されます。アクティブ ルータになるまでの待機時間は 300 秒 (5 分間) です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、グループのアクティブ ルータとして 2 つのルータを設定し、仮想ルータをスタンバイ ルータとして設定します。以下は、図 42-2 の MHSRP 設定をイネーブルにする例です。ルータに障害が発生して正常に戻った場合、プリエンプトを発生させてロード バランシングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 スタンバイ プライオリティは 110 (デフォルトは 100) です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 スタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定

HSRP 認証ストリングを設定したり、hello タイム インターバルやホールドタイムを変更することもできます。

これらのアトリビュートを設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべての HSRP メッセージに暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を取得することができません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を取得できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常の場合、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスに HSRP の認証とタイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、認証を設定する HSRP インターフェイスを入力します。
ステップ 3	<code>standby [group-number] authentication string</code>	(任意) authentication string : すべての HSRP メッセージで伝達されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトストリングは cisco です。 (任意) group-number : コマンドが適用されるグループ番号です。
ステップ 4	<code>standby [group-number] timers hellotime holdtime</code>	(任意) hello パケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 <ul style="list-style-type: none"> • group-number : コマンドが適用されるグループ番号です。 • hellotime : hello インターバル (秒) です。指定できる範囲は 1 ~ 255 秒で、デフォルトは 3 秒です。 • holdtime : アクティブまたはスタンバイ ルータのダウンが宣言されるまでの時間 (秒) です。指定できる範囲は 1 ~ 255 秒で、デフォルトは 10 秒です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	スタンバイ グループの設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

認証ストリングを削除するには、`no standby [group-number] authentication string` インターフェイス コンフィギュレーション コマンドを使用します。タイマーをデフォルト値に戻すには、`no standby [group-number] timers hellotime holdtime` インターフェイス コンフィギュレーション コマンドを使用します。

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、`word` を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、`hello` パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

インターネット制御メッセージプロトコル (ICMP) は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク レイヤ インターネット プロトコルです。ICMP には、ホストへのエラー パケットの方向付けや送信などの診断機能があります。

スイッチで HSRP が動作している場合、ホストが HSRP グループ内のルータのインターフェイス (または実際の) MAC アドレスを検出できないことに注意してください。ICMP によってホストがルータの実際の MAC アドレスへリダイレクトされて、そのルータに障害が発生した場合、ホストからのパケットは消失します。

HSRP が設定されたインターフェイスで ICMP リダイレクト メッセージは自動的にイネーブルになります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。ここでは、ネクスト ホップ IP アドレスが HSRP 仮想 IP アドレスに変更されます。詳細については、『Cisco IOS IP Configuration Guide』 Release 12.2 を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンド スイッチおよびルーティングの冗長性を確保するには、**cluster standby-group HSRP-group-name [routing-redundancy]** グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

次に、スタンバイ グループ `my_hsrp` をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンド スイッチおよびルータの冗長性を確保する例を示します。このコマンドを実行できるのは、コマンド スイッチに対してのみです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバーである場合は、エラー メッセージが表示されます。

```
Switch# configure terminal
Switch(config)# cluster standby-group my_hsrp routing-redundancy
Switch(config)# end
```

HSRP のトラブルシューティング

表 42-2 に示すいずれかの状況が発生すると、次のメッセージが表示されます。

```
%FHRP group not consistent with already configured groups on the switch stack -
virtual MAC reservation failed
```

表 42-2 HSRP のトラブルシューティング

状況	対処
設定する HSRP グループ インスタンスの数が 32 を超えています。	グループ インスタンスの数が最大 32 になるように HSRP グループを削除します。
IPv4 HSRP と IPv6 HSRP を同時に設定しています。	スイッチには IPv4 HSRP または IPv6 HSRP のいずれかを設定します。
設定するグループ番号が 256 の有効範囲内にありません。	有効な範囲内のグループ番号を設定します。

HSRP 設定の表示

HSRP 設定を表示するには、次の特権 EXEC コマンドを使用します。

```
show standby [interface-id [group]] [brief] [detail]
```

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルト表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

次に、**show standby** 特権 EXEC コマンドを実行し、2 つのスタンバイ グループ（グループ 1 およびグループ 100）の HSRP 情報を表示する例を示します。

```
Switch# show standby
VLAN1 - Group 1
  Local state is Standby, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.182
  Hot standby IP address is 172.20.128.3 configured
  Active router is 172.20.128.1 expires in 00:00:09
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac01
  Name is bbb
VLAN1 - Group 100
  Local state is Active, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.262
  Hot standby IP address is 172.20.138.51 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac64
  Name is test
```




CHAPTER 43

Cisco IOS IP SLA 動作の設定

この章では、Catalyst 3750 スイッチで Cisco IOS IP Service Level Agreement (SLA; サービス レベル 契約) を使用する方法について説明します。Cisco IP SLA は Cisco IOS ソフトウェアの一部であり、シスコのお客様は連続的で信頼性の高い確実な方法でトラフィックを生成するアクティブ トラフィック モニタリングを行って IP アプリケーションとサービスの IP サービス レベルを分析し、ネットワーク パフォーマンスを測定することができます。Cisco IOS SLA を使用すると、サービス プロバイダーのお客様はサービス レベル契約の検討と提供、企業のお客様はサービス レベルの検証、外部委託しているサービス レベル契約の検証、およびネットワーク パフォーマンスを把握することができます。Cisco IOS IP SLA は、ネットワーク アセスメントを実行することで QoS (Quality Of Service) の検証、新しいサービス導入の簡易化、ネットワーク トラブルシューティングの補助を可能にします。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

IP ベース イメージが稼動するスイッチは IP SLA 応答側の機能だけをサポートしており、IP SLA 機能をすべてサポートする別のデバイス (たとえば、IP サービス イメージが稼動する Catalyst 3750 スイッチ) とともに構成する必要があります。

IP SLA の詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』Release 12.4T を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

コマンドの構文については、次の URL にあるコマンドリファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

この章で説明する内容は、次のとおりです。

- 「Cisco IOS IP SLA の概要」 (P.43-1)
- 「IP SLA 動作の設定」 (P.43-6)
- 「IP SLA 動作のモニタリング」 (P.43-13)

Cisco IOS IP SLA の概要

Cisco IOS IP SLA はネットワークにデータを送信し、複数のネットワーク間または複数のネットワークパス内のパフォーマンスを測定します。ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアルタイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバなどのリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用されます。

Cisco IOS IP SLA 動作に応じて Cisco デバイスのネットワーク パフォーマンス統計情報が監視され、CLI (コマンドライン インターフェイス) MIB および SNMP (簡易ネットワーク管理プロトコル) MIB に格納されます。IP SLA パケットには設定可能な IP レイヤおよびアプリケーション レイヤのオプションがあります。たとえば、宛先 IP アドレス、User Datagram Protocol (UDP; ユーザ データグラム プロトコル) /TCP ポート番号、Type of Service (ToS; サービス タイプ) バイト (Differentiated Services Code Point [DSCP; DiffServ コード ポイント] および IP プレフィクス ビット)、VPN Routing/Forwarding Instance (VRF; VPN ルーティング/転送インスタンス)、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンドユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のような一意のパフォーマンス メトリックのサブセットを収集します。

- 遅延 (往復および一方向)
- ジッタ (方向性あり)
- パケット損失 (方向性あり)
- パケット シーケンス (パケット順序)
- パス (ホップ単位)
- 接続 (方向性あり)
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Works Internetwork Performance Monitor (IPM) やサードパーティ製パフォーマンス管理製品などの Performance Monitoring (PM; パフォーマンス モニタリング) アプリケーションでも使用できます。Cisco IOS IP SLA を使用するネットワーク管理製品については、次の URL を参照してください。

<http://www.cisco.com/go/ipsla>

IP SLA を使用すると次のような利点があります。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
 - ネットワーク内のジッタ、遅延、パケット損失が測定できる。
 - 連続的で信頼性のある確実な評価が提供される。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる (たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる)。
- 信頼性の高い評価を連続的に行ってネットワーク動作のトラブルシューティングを行うので、問題をすぐに特定しトラブルシューティングにかかる時間を短縮できる。
- Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) パフォーマンス モニタリングとネットワークの検証を行う (MPLS をサポートするスイッチの場合)。

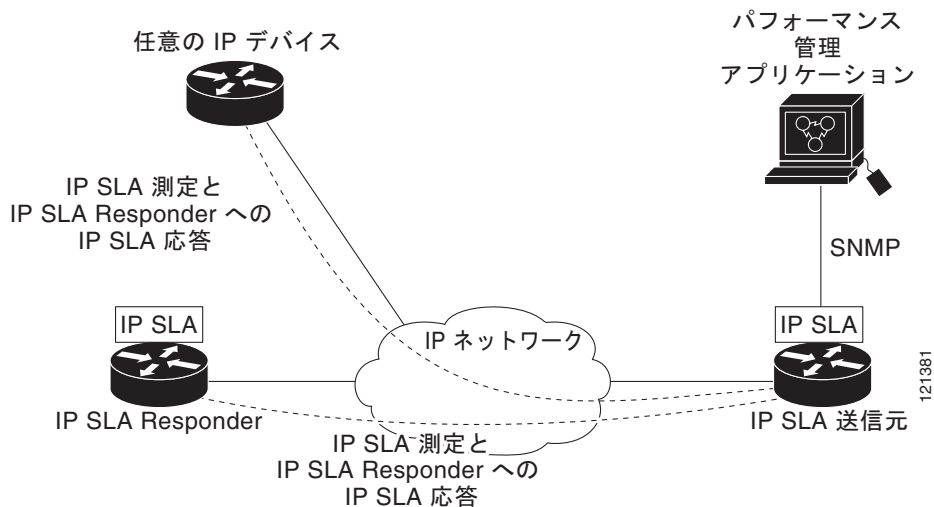
ここでは、IP SLA 機能について説明します。

- 「Cisco IOS IP SLA によるネットワーク パフォーマンスの測定」(P.43-3)
- 「IP SLA 応答側と IP SLA コントロール プロトコル」(P.43-4)
- 「IP SLA の応答時間の計算」(P.43-4)
- 「IP SLA 動作のスケジューリング」(P.43-5)
- 「IP SLA 動作しきい値モニタリング」(P.43-5)

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスを監視することができます。2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。図 43-1 に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。IP SLA 動作は、特定のプロトコル (UDP など) を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 43-1 Cisco IOS IP SLA 動作



IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

1. 必要であれば、IP SLA 応答側をイネーブルにします。
2. 必要な IP SLA 動作タイプを設定します。
3. 指定された動作タイプのオプションを設定します。
4. 必要であれば、しきい値条件を設定します。
5. 動作の実行スケジュールを指定し、しばらく動作を実行して統計情報を収集します。
6. Cisco IOS CLI を使用するか NMS (Network Management System; ネットワーク管理システム) と SNMP を併用して、動作の結果を表示し確認します。

IP SLA 動作の詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』の動作についての章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html



(注)

スイッチは、ゲートキーパー登録遅延動作測定を使用する VoIP サービス レベルをサポートしません。IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。

IP SLA 応答側と IP SLA コントロール プロトコル

IP SLA 応答側は宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。応答側は専用プローブなしで正確な測定を行います。応答側は、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて提供します。Cisco IOS デバイスだけが宛先 IP SLA 応答側の送信元になります。



(注)

IP SLA 応答側には Cisco IOS レイヤ 2 応答側設定可能スイッチが使用できます。たとえば、LAN ベース イメージが稼動する Catalyst 2960 または IE 3000 スイッチ、あるいは IP ベース イメージが稼動する Catalyst 3560 または 3750 スイッチです。応答側は、IP SLA 機能を全面的にサポートする必要はありません。

図 43-1 に、IP ネットワーク内での Cisco IOS IP SLA 応答側の配置場所を示しています。応答側は、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。この間に、応答側は要求を受け付け、応答します。応答側は、IP SLA パケットに応答したあとまたは指定の時間が経過したら ポートをディセーブルにします。セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

すべての IP SLA 動作に対して宛先デバイスの応答側をイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス (Telnet や HTTP など) は応答側では必要ありません。他社製デバイスに IP SLA 応答側を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

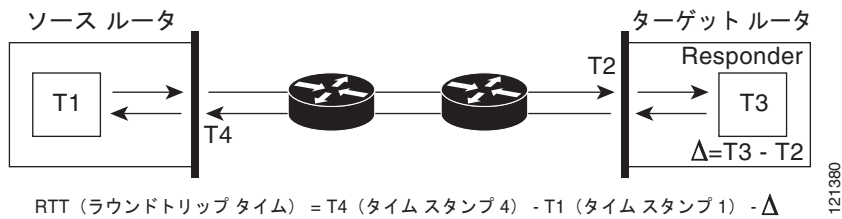
IP SLA の応答時間の計算

スイッチとルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映しません。IP SLA はソース デバイスとターゲット デバイス (応答側が使用されている場合) の処理遅延を最小化し、正しい Round-Trip Time (RTT; ラウンドトリップ時間) を識別します。IP SLA テストパケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA 応答側がイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

図 43-2 に、応答側の動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。ターゲット ルータで応答側機能がイネーブルの場合、タイム スタンプ 3 (TS3) からタイム スタンプ 2 (TS2) を引いてテスト パケットの処理にかかった時間を求め、デルタ (Δ) で表します。次に全体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース ルータにも適用されます。その場合、着信タイム スタンプ 4 (TS4) が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 43-2 Cisco IOS IP SLA 応答側タイムスタンプ



この他にも、ターゲット デバイスに 2 つのタイムスタンプがあれば一方向遅延、ジッタ、方向性を持つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方に Network Time Protocol (NTP) を設定し、両方のルータを同じくロックソースに同期させる必要があります。一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作のスケジューリングをします。すぐに動作を開始する、または特定の月、日、時刻に開始するようにスケジューリングできます。pending オプションを使用して、あとで動作を開始するように設定することもできます。pending オプションは動作の内部状態であり、SNMP で表示できます。トリガを待つ反応(しきい値)動作の場合も pending オプションを使用します。1 度に 1 つの IP SLA 動作をさせることも、グループの動作をさせることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、IP サービス イメージが稼動しているスイッチ上で複数の IP SLA 動作をスケジューリングできます。等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。IP SLA 動作をこのように分散させると Central Processing Unit (CPU; 中央処理装置) 利用率を最小限にとどめ、ネットワーク スケーラビリティを向上させることができます。

IP SLA の複数動作のスケジューリング機能に関する詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』の「IP SLAs - Multiple Operation Scheduling」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作しきい値モニタリング

SLA モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。IP SLA は SNMP トラップを送信して、次のような場合にイベントをトリガします。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッタしきい値
- 一方向パケット損失
- 一方向ジッタ
- 一方向平均オピニオン評点
- 一方向遅延

IP SLA しきい値違反があった場合も、あとで分析するために別の IP SLA 動作がトリガされます。たとえば、回数を増やしたり、ICMP パス エコーや ICMP パス ジッタ動作を開始してトラブルシューティングを行うことができます。

しきい値の種類とレベル設定を決めるのは複雑であり、ネットワークで使用する IP サービスの種類によって異なります。Cisco IOS の IP SLA 動作のしきい値の使用方法に関する詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』の「IP SLAs - Proactive Threshold Monitoring」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA 動作の設定

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『Cisco IOS IP SLAs Configuration Guide』を参照してください。ここでは、応答側の設定、UDP ジッタ動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。



(注)

IP ベース イメージが稼動するスイッチは、IP SLA 応答側機能だけをサポートします。完全な IP SLA 機能を使用するには、スイッチで IP サービス イメージが稼動している必要があります。

他の動作の設定に関する詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

ここでは、次の情報について説明します。

- 「デフォルト設定」(P.43-6)
- 「設定時の注意事項」(P.43-6)
- 「IP SLA 応答側の設定」(P.43-8)
- 「UDP ジッタ動作を使用した IP サービス レベルの分析」(P.43-8)
- 「ICMP エコー動作を使用した IP サービス レベルの分析」(P.43-11)

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA のコマンドについては、次の URL にある『Cisco IOS IP SLAs Command Reference』 Release 12.4T を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

説明と設定手順の詳細については、次の URL にある『Cisco IOS IP SLAs Configuration Guide』 Release 12.4T を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

スイッチでは、このガイドで説明する IP SLA コマンドや動作がすべてサポートされているわけではありません。スイッチでは、UDP ジッタ、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッタ、FTP、DNS、DHCP を使用する IP サービス レベル分析をサポートします。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートします。ゲートキーパー登録遅延動作測定を使用する VoIP サービス レベルはサポートされません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。コマンドの出力例は次のとおりです。

```
Switch# show ip sla application
      IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured      : 0
Number of active Entries         : 0
Number of pending Entries        : 0
Number of inactive Entries       : 0

      Supported Operation Types
Type of Operation to Perform: 802.lagEcho
Type of Operation to Perform: 802.lagJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

IP SLA 応答側の設定

IP SLA 応答側は、LAN ベースのイメージが稼動している Catalyst 2960 や Cisco ME 2400 または IE 3000 スイッチなど、レイヤ 2 スイッチを含む Cisco IOS ソフトウェアベース デバイスに限り利用可能です。レイヤ 2 スイッチは IP SLA 機能をすべてサポートしているわけではありません。ターゲット デバイス（動作ターゲット）に IP SLA 応答側を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip sla responder {tcp-connect udp-echo} ipaddress ip-address port port-number</code>	<p>スイッチを IP SLA 応答側に設定します。</p> <p>オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> tcp-connect : 応答側の TCP 接続動作をイネーブルにします。 udp-echo : 応答側の UDP エコー動作またはジッタ動作をイネーブルにします。 ipaddress ip-address : 宛先 IP アドレスを入力します。 port port-number : 宛先ポート番号を入力します。 <p>(注) IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip sla responder</code>	デバイスの IP SLA 応答側設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA 応答側をディセーブルにするには、`no ip sla responder` グローバル コンフィギュレーション コマンドを入力します。次に、デバイスを UDP ジッタ IP SLA 動作の応答側に設定する例を示します。UDP ジッタ IP SLA 動作については次のセクションで説明します。

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```



(注) IP SLA 応答側が機能するには、IP サービス イメージが稼動する Catalyst 3750 または Catalyst 3560 スイッチなどの、IP SLA を完全にサポートする送信元デバイスを設定する必要があります。設定方法については、送信元デバイスのマニュアルを参照してください。

UDP ジッタ動作を使用した IP サービス レベルの分析

ジッタはパケット間の遅延のばらつきです。発信元から宛先に向かって複数のパケットを 10 ミリ秒遅れで送信したとき、ネットワークが正常に動作していれば宛先でも 10 ミリ秒遅れで受信します。しかしネットワーク内に遅延がある場合（キューの発生や別のルータ経由で到着するなど）、パケットの到着遅延が 10 ミリ秒よりも大きくなったり小さくなったりします。正のジッタ値は、パケットの到着が 10 ミリ秒を超えていることを示します。パケットの到着が 12 ミリ秒の場合のジッタ値は +2 ミリ秒（正の値）です。8 ミリ秒で到着する場合は -2 ミリ秒（負の値）です。遅延による影響を受けやすいネットワークの場合、正のジッタ値は望ましくありません。ジッタ値 0 が理想的です。

ジッタのモニタリング以外にも、IP SLA UDP ジッタ動作を多目的データ収集動作に使用できます。パケット IP SLA は搬送パケットを生成し、ソース ターゲットと動作ターゲット間でシーケンス情報の送受信とタイム スタンプの送受信を行います。前述の点に基づき、UDP ジッタ動作は次のデータを測定します。

- 方向別ジッタ（発信元から宛先へ、宛先から発信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- 往復遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳やエラーの場所を簡単に突き止めることができます。

UDP ジッタ動作では合成（シミュレーション）UDP トラフィックを生成し、発信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際、各パケットのサイズ、パケット同士の間隔、発信間隔は決められています。デフォルトでは、10 バイトのペイロードサイズのパケットフレームを 10 ミリ秒で 10 個生成し、60 秒間隔で発信します。これらのパラメータは、提供する IP サービスを最もよくシミュレートするように設定できます。

一方向遅延を正確に測定する場合、NTP などによるソース デバイスとターゲット デバイス間のクロック同期が必要です。一方向ジッタおよびパケット損失を測定する場合は、クロック同期は不要です。ソース デバイスとターゲット デバイスのクロックが同期されていない場合、一方向ジッタおよびパケット損失データは戻されますが、UDP ジッタ動作による一方向遅延測定値は 0 で戻ります。



(注)

ソース デバイスに UDP ジッタ動作を設定する前に、ターゲット デバイス（動作デバイス）の IP SLA 応答側をイネーブルにしておく必要があります。

ソース デバイス上で UDP ジッタ動作を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip sla operation-number</code>	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3 <code>udp-jitter</code> <i>{destination-ip-address destination-hostname}</i> <i>destination-port</i> [<code>source-ip</code> <i>{ip-address hostname}</i>] <code>[source-port port-number]</code> <code>[control {enable disable}]</code> <code>[num-packets number-of-packets]</code> <code>[interval interpacket-interval]</code>	IP SLA 動作に UDP ジッタ動作を設定し、UDP ジッタ コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> • <i>destination-ip-address destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • <i>destination-port</i> : 宛先ポート番号を 1 ~ 65535 の範囲で指定します。 • (任意) <code>source-ip</code> <i>{ip-address hostname}</i> : 発信元 IP アドレスまたはホスト名を指定します。発信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • (任意) <code>source-port</code> <i>port-number</i> : 発信元ポート番号を 1 ~ 65535 の範囲で指定します。ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • (任意) <code>control</code> : IP SLA 応答側への IP SLA コントロール メッセージの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA コントロール メッセージは宛先デバイスに送信され、IP SLA 応答側との接続を確立します。 • (任意) <code>num-packets</code> <i>number-of-packets</i> : 生成するパケット数を入力します。指定できる範囲は 1 ~ 6000 です。デフォルトは 10 です。 • (任意) <code>interval</code> <i>inter-packet-interval</i> : パケットの送信間隔をミリ秒で指定します。指定できる範囲は 1 ~ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 4 <code>frequency</code> <i>seconds</i>	(任意) 指定した IP SLA 動作の反復間隔を設定します。指定できる範囲は 1 ~ 604800 秒で、デフォルトは 60 秒です。
ステップ 5 <code>exit</code>	UDP ジッタ コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 6 <code>ip sla monitor schedule</code> <i>operation-number</i> [<code>life {forever seconds}</code>] [<code>start-time {hh:mm [:ss] month day day month}</code>] <code>pending now after hh:mm:ss</code>] [<code>ageout seconds</code>] [<code>recurring</code>]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 <ul style="list-style-type: none"> • <i>operation-number</i> : RTR エントリ番号を入力します。 • (任意) <code>life</code> : 動作の実行を無期限 (<code>forever</code>) に指定するか、<i>秒数</i>を指定します。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 3600 秒 (1 時間) です。 • (任意) <code>start-time</code> : 情報の収集を開始する時刻を入力します。 <ul style="list-style-type: none"> – 特定の時刻に開始する場合は、時、分、秒 (24 時間表記)、月日を入力します。月を入力しない場合、デフォルトは当月です。 – <code>pending</code> と入力すれば、開始時刻を指定するまでは情報を収集しません。 – <code>now</code> と入力すれば、すぐに動作を開始します。 – <code>after hh:mm:ss</code> と入力すれば、指定した時刻を経過後に動作を開始します。 • (任意) <code>ageout</code> <i>seconds</i> : 情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ~ 2073600 秒です。デフォルトは 0 秒 (いつまでも保存する) です。 • (任意) <code>recurring</code> : 毎日、動作を自動的に実行します。
ステップ 7 <code>end</code>	特権 EXEC モードに戻ります。

コマンド	目的
ステップ 8 show ip sla configuration [<i>operation-number</i>]	(任意) 設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する場合と、指定した動作だけを表示する場合があります。
ステップ 9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作をディセーブルにするには、**no ip sla operation-number** グローバル コンフィギュレーション コマンドを入力します。次に、UDP ジッタ IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.
```

```
Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 30
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
```

ICMP エコー動作を使用した IP サービス レベルの分析

ICMP エコー動作は、Cisco デバイスと IP を使用する任意のデバイスとのエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセージを宛先に送信して ICMP エコー応答を受信するまでの時間を測定して算出します。多くのお客様が IP SLA ICMP ベース動作、社内 ping テスト、ping ベース専用プローブを使用して、発信元 IP SLA デバイスと宛先 IP デバイス間の応答時間を測定しています。IP SLA ICMP エコー動作は ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答時間が得られます。



(注) この動作では、IP SLA 応答側をイネーブルにしておく必要はありません。

ソース デバイス上で ICMP エコー動作を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip sla operation-number	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3 icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-id</i>]	IP SLA 動作に ICMP エコー動作を設定し、ICMP エコー コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • <i>destination-ip-address</i> <i>destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • (任意) source-ip {<i>ip-address</i> <i>hostname</i>} : 発信元 IP アドレスまたはホスト名を指定します。発信元 IP アドレスまたはホスト名を指定しない場合、IP SLA は宛先に最も近い IP アドレスを選択します。 • (任意) source-interface <i>interface-id</i> : 動作に対するソース インターフェイスを指定します。
ステップ 4 frequency seconds	(任意) 指定した IP SLA 動作の反復間隔を設定します。指定できる範囲は 1 ~ 604800 秒で、デフォルトは 60 秒です。
ステップ 5 exit	UDP ジッタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6 ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm</i> [: <i>ss</i>] [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i> }] [ageout <i>seconds</i>] [recurring]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 <ul style="list-style-type: none"> • <i>operation-number</i> : RTR エントリ番号を入力します。 • (任意) life : 動作の実行を無期限 (forever) に指定するか、<i>秒数</i>を指定します。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 3600 秒 (1 時間) です。 • (任意) start-time : 情報の収集を開始する時刻を入力します。 <ul style="list-style-type: none"> – 特定の時刻に開始する場合は、時、分、秒 (24 時間表記)、月日を入力します。月を入力しない場合、デフォルトは当月です。 – pending と入力すれば、開始時刻を指定するまでは情報を収集しません。 – now と入力すれば、すぐに動作を開始します。 – after <i>hh:mm:ss</i> と入力すれば、指定した時刻を経過したら動作を開始します。 • (任意) ageout <i>seconds</i> : 情報を収集していないとき、メモリの動作を保存する秒数を指定します。指定できる範囲は 0 ~ 2073600 秒です。デフォルトは 0 秒 (いつまでも保存する) です。 • (任意) recurring : 毎日、動作を自動的に実行します。
ステップ 7 end	特権 EXEC モードに戻ります。
ステップ 8 show ip sla configuration [<i>operation-number</i>]	(任意) 設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する場合と、指定した動作だけを表示する場合があります。
ステップ 9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA 動作をディセーブルにするには、**no ip sla operation-number** グローバル コンフィギュレーション コマンドを入力します。次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 60
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 15
  History Filter Type: None
Enhanced History:
```

IP SLA 動作のモニタリング

表 43-1 に示すユーザ EXEC コマンドまたは特権 EXEC コマンドを使用して、IP SLA 動作の設定と結果を表示します。

表 43-1 IP SLA 動作のモニタリング

コマンド	目的
show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [<i>entry-number</i>]	設定値を表示します。すべての IP SLA 動作のすべてのデフォルト値を表示する場合と、指定した動作だけを表示する場合があります。

表 43-1 IP SLA 動作のモニタリング

コマンド	目的
show ip sla enhanced-history { collection-statistics distribution statistics } [<i>entry-number</i>]	収集した履歴バケットの拡張履歴統計情報を表示します。あるいは、すべての IP SLA 動作または特定の動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [<i>entry-number</i>]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [<i>schedule-entry-number</i>]	IP SLA グループ スケジューリング設定と個別情報を表示します。
show ip sla history [<i>entry-number</i> full tabular]	すべての IP SLA 動作に関して収集した履歴を表示します。
show ip sla mpls-lsp-monitor { collection-statistics configuration ldp operational-state scan-queue summary } [<i>entry-number</i>] neighbors }	MPLS Label Switched Path (LSP; ラベル スイッチドパス) ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [<i>entry-number</i>]	すべての IP SLA 動作または特定の動作について、事前に設定したしきい値のモニタリングを表示します。
show ip sla reaction-trigger [<i>entry-number</i>]	すべての IP SLA 動作または特定の動作に関する反応トリガ情報を表示します。
show ip sla responder	IP SLA 応答側の情報を表示します。
show ip sla statistics [<i>entry-number</i> aggregated details]	現在のまたは集約した動作ステータスと統計情報を表示します。



CHAPTER 44

拡張オブジェクト トラッキングの設定

この章では、Catalyst 3750 スイッチに拡張オブジェクト トラッキングを設定する方法について説明します。この機能により Hot Standby Routing Protocol (HSRP; ホットスタンバイ ルーティング プロトコル) トラッキング メカニズムが拡張され、インターフェイスのライン プロトコル ステートがトラッキングできるようになります。インターフェイスのライン プロトコル ステートがダウンすると、そのインターフェイスの HSRP プライオリティが低下し、より高いプライオリティを持つ別の HSRP デバイスがアクティブになります。拡張オブジェクト トラッキング機能は HSRP とトラッキング メカニズムを分離し、HSRP 以外のプロセスで使用可能な個別のスタンドアロン型トラッキング プロセスを作成します。その結果、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトのトラッキングが可能になります。HSRP などのクライアント プロセスでは、トラッキングするオブジェクトを登録して、オブジェクトがステートを変更した時に通知を要求することができます。この機能は、ルーティング システムの可用性を高め、復旧のスピードを速めるとともに、停止および停止期間を削減します。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

拡張オブジェクト トラッキングおよびこれを設定するためのコマンドの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

この章で説明する内容は、次のとおりです。

- 「拡張オブジェクト トラッキングの概要」(P.44-1)
- 「拡張オブジェクト トラッキング機能の設定」(P.44-2)
- 「拡張オブジェクト トラッキングのモニタリング」(P.44-13)

拡張オブジェクト トラッキングの概要

各トラッキング オブジェクトには、トラッキング CLI (コマンドライン インターフェイス) で指定される一意の番号があります。クライアント プロセスでは、この番号を使用して特定のオブジェクトをトラッキングします。トラッキング プロセスでは、値の変更 (増加または減少値) について定期的にトラッキング オブジェクトをポーリングし、即時または指定した時間後に、対象のクライアント プロセスに変更を送信します。複数のクライアントが同じオブジェクトをトラッキングすることができ、オブジェクトのステート変更時に個別のアクションを実行することができます。

また、リストのステータスを測定するためにウェイトしきい値またはパーセンテージしきい値のいずれかを使用してリスト内のオブジェクトを組み合わせることも可能です。ブール論理を使用してオブジェクトを組み合わせることが可能です。ブール AND 機能のあるトラッキング リストでは、アップになっているトラッキング オブジェクトに対して、リスト内の各オブジェクトがアップ ステータスになっている必要があります。ブール OR 機能のあるトラッキング リストでは、アップになっているトラッキング オブジェクトに対して、リスト内の 1 つのオブジェクトだけがアップ ステータスになっている必要があります。

拡張オブジェクト トラッキング機能の設定

ここでは、次のような拡張オブジェクト トラッキングの設定について説明します。

- 「デフォルト設定」(P.44-2)
- 「インターフェイスのラインプロトコルまたは IP ルーティング ステータスのトラッキング」(P.44-2)
- 「トラッキング リストの設定」(P.44-4)
- 「HSRP オブジェクト トラッキングの設定」(P.44-7)
- 「他のトラッキング特性の設定」(P.44-8)
- 「IP SLA オブジェクト トラッキングの設定」(P.44-9)
- 「スタティック ルーティング サポートの設定」(P.44-10)

デフォルト設定

オブジェクト トラッキングの種類は設定されていません。

インターフェイスのラインプロトコルまたは IP ルーティング ステータスのトラッキング

ライン プロトコル ステータスまたはインターフェイス IP ルーティング ステータスをトラッキングすることができます。IP ルーティング ステータスをトラッキングする場合、アップになっているオブジェクトは次の 3 つの条件を満たす必要があります。

- インターフェイス上の IP ルーティングがイネーブルでありアクティブである。
- インターフェイス ラインプロトコル ステータスがアップである。
- インターフェイス IP アドレスが既知である。

これら 3 つの条件がすべて満たされない場合、IP ルーティング ステータスはダウンとなります。

インターフェイスのラインプロトコル ステートまたは IP ルーティング ステートを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 track object-number interface interface-id line-protocol	(任意) インターフェイスのラインプロトコル ステートをトラッキングするためにトラッキング リストを作成し、トラッキング コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> object-number は、トラッキング オブジェクトを識別するもので、1 ~ 500 を使用できます。 interface interface-id は、トラッキングされるインターフェイスです。
ステップ 3 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステートの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 4 exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5 track object-number interface interface-id ip routing	(任意) インターフェイスの IP ルーティング ステートをトラッキングするためにトラッキング リストを登録し、トラッキング コンフィギュレーション モードを開始します。IP ルートトラッキングは、ルーティング テーブル内の IP ルートと、IP パケットをルーティングするインターフェイスの能力をトラッキングします。 <ul style="list-style-type: none"> object-number は、トラッキング オブジェクトを識別するもので、1 ~ 500 を使用できます。 interface interface-id は、トラッキングされるインターフェイスです。
ステップ 6 delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステートの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 7 end	特権 EXEC モードに戻ります。
ステップ 8 show track object-number	指定したオブジェクトがトラッキングされていることを確認します。
ステップ 9 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスのラインプロトコル ステートをトラッキングして、その設定を確認する例を示します。

```
Switch(config)# track 33 interface gigabitethernet 1/0/1 line-protocol
Switch(config)# track 33 interface gigabitethernet 1/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
  Interface GigabitEthernet1/0/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:18:28
```

トラッキング リストの設定

ブール論理式、ウェイトしきい値、パーセンテージしきい値を使用して、オブジェクトのトラッキング リストを設定することができます。トラッキング リストには、1 つまたは複数のオブジェクトが含まれています。トラッキング リストに追加する前に、オブジェクトが存在していなければなりません。

- ブール論理式を設定して、AND または OR 演算子を使用して計算を指定します。
- ウェイトしきい値でトラッキング リスト ステートを測定する場合、重み値をトラッキング リスト内の各オブジェクトに割り当てます。トラッキング リストのステータスは、しきい値に一致するかどうかで決定されます。各オブジェクトのステータスは、全オブジェクトの合計重みと各オブジェクトのウェイトしきい値を比較することで決定されます。
- パーセンテージしきい値でトラッキング リスト ステートを測定する場合、パーセンテージしきい値をトラッキング リスト内の各オブジェクトに割り当てます。各オブジェクトに割り当てられたパーセンテージとリストを比較して、各オブジェクトのステータスが決定されます。

ブール論理式を使用したトラッキング リストの設定

ブール論理式を使用してトラッキング リストを設定することにより、AND または OR 演算子を使用して計算することができます。たとえば、AND 演算子を使用して 2 つのインターフェイスをトラッキングする場合、*up* は両方のインターフェイスがアップで、*down* はいずれかのインターフェイスがダウンであることを意味します。

ブール論理式を使用してオブジェクトのトラッキング リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>track track-number list boolean {and or}</code>	<p>トラッキング リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。<i>track-number</i> は 1 ~ 500 です。</p> <ul style="list-style-type: none"> • boolean : ブール計算に基づいてトラッキング リストのステータスを指定します。 • and : すべてのオブジェクトがアップの場合はリストがアップ、1 つ以上のオブジェクトがダウンの場合はダウンであることを指定します。 • or : すべてのオブジェクトがアップの場合はリストがアップ、すべてのオブジェクトがダウンの場合はダウンであることを指定します。
ステップ 3	<code>object object-number [not]</code>	<p>トラッキングするオブジェクトを指定します。指定できる範囲は 1 ~ 500 です。キーワード not は、オブジェクトのステータスを否定します。つまり、オブジェクトがアップの場合、トラッキング リストはオブジェクトをダウンとして検出します。</p> <p>(注) オブジェクトが存在しないと、これをトラッキング リストに追加することができません。</p>
ステップ 4	<code>delay {up seconds [down seconds] [up seconds] down seconds}</code>	(任意) トラッキング オブジェクトの通信ステータスの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show track object-number</code>	指定したオブジェクトがトラッキングされていることを確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

トラッキング リストを削除する場合は、**no track track-number** グローバル コンフィギュレーション コマンドを使用します。

次に、2 つのオブジェクトが含まれていて、そのうちの 1 つのオブジェクトのステータスが偽のものを含む、ブール AND 論理式を使用してトラッキング リスト 4 を設定する例を示します。リストがアップの場合、リストでオブジェクト 2 がダウンであることが検出されます。

```
Switch(config)# track 4 list boolean and
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

ウェイトしきい値を使用したトラッキング リストの設定

ウェイトしきい値をトラッキングするには、オブジェクトのトラッキング リストを設定し、しきい値として使用する重みを指定し、各オブジェクトの重みを設定します。各オブジェクトのステータスは、アップ ステータスの全オブジェクトの合計重みと各オブジェクトのウェイトしきい値を比較することで決定されます。

ブール NOT 演算子をウェイトしきい値 リストに使用することができません。

ウェイトしきい値を使用してトラッキング リストを設定し、各オブジェクトの重みを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	track track-number list threshold weight	トラッキング リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。 <i>track-number</i> は 1 ~ 500 です。 <ul style="list-style-type: none"> threshold : しきい値に基づいてトラッキング リストのステータスを指定します。 weight : しきい値が重みに基づいていることを指定します。
ステップ 3	object object-number [weight weight-number]	トラッキングするオブジェクトを指定します。指定できる範囲は 1 ~ 500 です。オプションの weight weight-number には、オブジェクトのウェイトしきい値を指定します。指定できる範囲は 1 ~ 255 です。 (注) オブジェクトが存在していないと、これをトラッキング リストに追加することができません。
ステップ 4	threshold weight {up number [down number]}	ウェイトしきい値を指定します。 <ul style="list-style-type: none"> up number : 指定できる範囲は 1 ~ 255 です。 down number : (任意) up number で選択した番号によって変化します。up number を 25 に設定した場合、ダウン番号で表示される範囲は 0 ~ 24 です。
ステップ 5	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステータスの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show track object-number	指定したオブジェクトがトラッキングされていることを確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トラッキング リストを削除する場合は、**no track track-number** グローバル コンフィギュレーション コマンドを使用します。

次の例では、ウェイトしきい値でトラッキングするようにトラッキング リスト 4 を設定します。オブジェクト 1 とオブジェクト 2 がダウンの場合、オブジェクト 3 が上限しきい値（アップ 30）を満たすことから、トラッキング リスト 4 はアップになります。しかし、オブジェクト 3 がダウンの場合、オブジェクト 1 と 2 がアップでなければウェイトしきい値を満たせません。

```
Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit
```

この設定は、オブジェクト 1 とオブジェクト 2 が 2 つの小帯域幅の接続を表し、オブジェクト 3 が 1 つの大帯域幅の接続を表している場合に効果的です。設定された **down 10** 値は、トラッキング オブジェクトがアップになると、しきい値が 10 以下になるまでダウンにならないこととなりますが、この例ではすべての接続がダウンになります。

パーセンテージしきい値を使用したトラッキング リストの設定

パーセンテージしきい値をトラッキングするには、オブジェクトのトラッキング リストを設定し、しきい値として使用するパーセンテージを指定し、リスト内にある各オブジェクトのパーセンテージを指定します。各オブジェクトに割り当てられたパーセンテージとリストを比較して、リストのステータスが決定されます。

ブール NOT 演算子をパーセンテージしきい値リストに使用することができません。

パーセンテージしきい値を使用してオブジェクトのトラッキング リストを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	track track-number list threshold percentage	トラッキング リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。 <i>track-number</i> は 1 ～ 500 です。 <ul style="list-style-type: none"> • threshold : しきい値に基づいてトラッキング リストのステータスを指定します。 • percentage : しきい値がパーセンテージに基づいていることを指定します。
ステップ 3	object object-number	トラッキングするオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。 (注) オブジェクトが存在していないと、これをトラッキング リストに追加することができません。
ステップ 4	threshold percentage {up number [down number]}	しきい値パーセンテージを指定します。 <ul style="list-style-type: none"> • up number : 指定できる範囲は 1 ～ 100 です。 • down number : (任意) up number で選択した番号によって変化します。up number を 25 に設定した場合、ダウン番号で表示される範囲は 0 ～ 24 です。
ステップ 5	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステータスの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show track object-number	指定したオブジェクトがトラッキングされていることを確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トラッキング リストを削除する場合は、**no track track-number** グローバル コンフィギュレーション コマンドを使用します。

次に、3 つのオブジェクトと、リストのステータスを測定するために指定したパーセンテージがあるトラッキング リスト 4 を設定する例を示します。

```
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```

HSRP オブジェクト トラッキングの設定

スタンバイ HSRP グループを設定し、オブジェクト ステータスに基づいてオブジェクトをトラッキングして HSRP 優先度を変更するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 track object-number {interface interface-id {line-protocol ip routing} ip route ip-address/prefix-length {metric threshold reachability} list {boolean {and or}} {threshold {weight percentage}}}	<p>(任意) 設定ステータスをトラッキングするためにトラッキング リストを作成し、トラッキング コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> <i>object-number</i> の範囲は 1 ~ 500 です。 interface interface-id を入力して、トラッキングするインターフェイスを選択します。 line-protocol を入力して、インターフェイス ラインプロトコル ステータスをトラッキングします。または ip routing を入力して、インターフェイス IP ルーティング ステータスをトラッキングします。 ip route ip-address/prefix-length を入力して、IP ルートのステータスをトラッキングします。 metric threshold を入力して、しきい値メトリックをトラッキングします。または reachability を入力して、ルートが到達可能かどうかをトラッキングします。 <p>デフォルトの上限しきい値は 254 で、デフォルトの下限しきい値は 255 です。</p> <ul style="list-style-type: none"> list を入力して、リストにグループ化されているオブジェクトをトラッキングします。前のページで説明したリストを設定します。 <ul style="list-style-type: none"> Boolean については、「ブール論理式を使用したトラッキング リストの設定」(P.44-4) を参照してください。 threshold weight については、「ウェイトしきい値を使用したトラッキング リストの設定」(P.44-5) を参照してください。 threshold percentage については、「パーセンテージしきい値を使用したトラッキング リストの設定」(P.44-6) を参照してください。 <p>(注) トラッキングする各インターフェイスについて、これを繰り返します。</p>
ステップ 3 exit	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 4	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<code>standby [group-number] ip [ip-address [secondary]]</code>	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 <ul style="list-style-type: none"> （任意） <i>group-number</i> : HSRP がイネーブルであるインターフェイスのグループ番号を指定します。指定できる範囲は 0 ~ 255 で、デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 （1 つのインターフェイスで必須、それ以外は任意） <i>ip-address</i> : ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 （任意） <i>secondary</i> : IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。このキーワードを省略した場合、設定されるアドレスはプライマリ IP アドレスです。
ステップ 6	<code>standby [group-number] track object-number [decrement [priority-decrement]]</code>	HSRP を設定して、オブジェクトをトラッキングし、オブジェクトのステートに基づいてホットスタンバイ プライオリティを変更します。 <ul style="list-style-type: none"> （任意） <i>group-number</i> : トラッキングが適用されるグループ番号を入力します。 <i>object-number</i> : トラッキングするオブジェクトを表す番号を入力します。指定できる範囲は 1 ~ 500 で、デフォルトは 1 です。 （任意） <i>decrement priority-decrement</i> : トラッキング オブジェクトがダウンした（または稼動状態に戻った）際の、ルータのホットスタンバイ プライオリティを減少（または増加）させる幅を指定します。指定できる範囲は 1 ~ 255 で、デフォルトは 10 です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show standby</code>	スタンバイ ルータ IP アドレスとトラッキング ステートを確認します。
ステップ 9	<code>copy running-config startup-config</code>	（任意） コンフィギュレーション ファイルに設定を保存します。

他のトラッキング特性の設定

拡張オブジェクト トラッキングを他の特性のトラッキングにも使用することができます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用して IP ルートの到達可能性をトラッキングすることができます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用して、ルートがしきい値を超えるのか下回るのかを判別することができます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用して、ルーティングプロトコルのメトリック分解能のデフォルト値を変更することができます。
- **track timer** トラッキング コンフィギュレーション コマンドを使用して、定期的にトラッキング オブジェクトをポーリングするためのトラッキング プロセスを設定することができます。

拡張オブジェクト トラッキング設定を確認するには、**show track** 特権 EXEC コマンドを使用します。

拡張オブジェクト トラッキングおよびこれを設定するためのコマンドの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541be.html

IP SLA オブジェクト トラッキングの設定

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) (IP SLA) はネットワーク パフォーマンスを測定および診断するツールです。トラフィックを生成してネットワーク パフォーマンスを測定するアクティブ モニタリングを使用します。Cisco IP SLA の動作は、ネットワークのトラブルシューティング、設計、分析に使用できるリアルタイム メトリックを収集します。

スイッチの Cisco IP SLA について詳しくは、第 43 章「Cisco IOS IP SLA 動作の設定」を参照してください。IP SLA コマンドについては、次の URL の『Cisco IOS IP SLAs Command Reference』Release 12.4T を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a008049739b.html

IP SLA 動作のオブジェクト トラッキングにより、クライアントは IP SLA オブジェクトの出力をトラッキングし、この情報を使ってアクションを開始できます。それぞれの IP SLA 動作は、トラッキングプロセスによって解釈される *OK* や *OverThreshold* などの SNMP 動作リターン コード値を維持します。IP SLA 動作の 2 つの側面であるステートと到達可能性をトラッキングできます。ステートに関しては、リターン コードが *OK* であればトラック ステートはアップであり、*OK* でなければトラック ステートはダウンです。到達可能性のリターン コードが *OK* または *OverThreshold* であれば到達可能性はアップであり、*OK* でなければ到達可能性はダウンです。

特権 EXEC モードで次の手順を実行し、IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性をトラッキングします。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	track object-number rtr operation-number state	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートをトラッキングします。 <ul style="list-style-type: none"> <i>object-number</i> の範囲は 1 ~ 500 です。 <i>operation-number</i> の範囲は 1 ~ 2147483647 です。
ステップ 3	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステートの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	track object-number rtr operation-number reachability	トラッキング コンフィギュレーション モードを開始し、IP SLA IP ホストの到達可能性をトラッキングします。 <ul style="list-style-type: none"> <i>object-number</i> の範囲は 1 ~ 500 です。 <i>operation-number</i> の範囲は 1 ~ 2147483647 です。
ステップ 6	delay {up seconds [down seconds] [up seconds] down seconds}	(任意) トラッキング オブジェクトの通信ステートの変更を遅延させるための時間を秒数で指定します。指定できる範囲は 1 ~ 180 秒です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show track object-number	トラッキング情報を表示して設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、IP SLA ステート トラッキングを設定して表示する例を示します。

```
Switch(config)# track 2 200 state
Switch(config)# end
Switch# show track 2
Track 2
  Response Time Reporter 1 state
  State is Down
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (milliseconds) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

次に、ルートの到達可能性に関する出力結果の例を示します。

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
  Response Time Reporter 1 reachability
  Reachability is Up
    1 change, last change 00:00:47
  Latest operation return code: over threshold
  Latest RTT (milliseconds) 4
  Tracked by:
    HSRP Ethernet0/1 3
```

スタティック ルーティング サポートの設定

Cisco IOS release 12.2(46)SE 以降の IP サービス稼働しているスイッチは、拡張オブジェクト トラッキングのスタティック ルーティングをサポートしています。拡張オブジェクト トラッキングを使用するスタティック ルーティングのサポートにより、スイッチは ICMP ping を使用して、事前に設定されたスタティック ルートまたは DHCP ルートがダウンしたことを識別できます。トラッキングがイネーブルの場合、システムはルートの状態をトラッキングし、ルートの状態が変化するとクライアントに通知します。スタティック ルート オブジェクト トラッキングでは、Cisco IP SLA を使用して ICMP ping を生成し、プライマリ ゲートウェイへの接続の状態をモニタします。

- スイッチでの Cisco IP SLA サポートの詳細については、第 43 章「Cisco IOS IP SLA 動作の設定」を参照してください。
- スタティック ルートのオブジェクト トラッキングに関する詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

スタティック ルートのオブジェクト トラッキングを設定するには、次の手順を実行します。

-
- ステップ 1** プライマリ インターフェイスにスタティック ルーティングまたは DHCP を設定します。
 - ステップ 2** プライマリ インターフェイスとトラッキング オブジェクトの IP アドレスに ping を実行してエージェントの状態をモニタするように、IP SLA エージェントを設定します。
 - ステップ 3** セカンダリ インターフェイスを使用するデフォルトのスタティック デフォルト ルートを設定します。このルートはプライマリ ルートが削除された場合にのみ使用されます。
-

プライマリ インターフェイスの設定

プライマリ インターフェイスにスタティック ルーティングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに記述を追加します。
ステップ 4	ip address ip-address mask [secondary]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。

プライマリ インターフェイスに DHCP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	プライマリまたはセカンダリ インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに記述を追加します。
ステップ 4	ip dhcp client route track number	追加されるすべてのルートに指定したトラッキング番号に関連付けるよう、DHCP クライアントを設定します。有効な番号は、1 ~ 500 です。
ステップ 5	ip address dhcp	イーサネット インターフェイスの IP アドレスを DHCP から取得します。
ステップ 6	exit	グローバル コンフィギュレーション モードに戻ります。

Cisco IP SLA のモニタリング エージェントおよびトラッキング オブジェクトの設定

Cisco IP SLA によるネットワーク モニタリングを設定するには、特権 EXEC モードで次の手順を実行します。

ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip sla operation-number	Cisco IP SLA の動作設定を開始し、IP SLA コンフィギュレーション モードを開始します。
ステップ 3	icmp-echo {destination-ip-address destination hostname [source- ipaddr {ip-address hostname source-interface interface-id]}	Cisco IP SLA のエンドツーエンドの ICMP エコー応答時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。
ステップ 4	timeout milliseconds	要求パケットの応答に対する待機時間を設定します。
ステップ 5	frequency seconds	ネットワークに送信するレートを設定します。
ステップ 6	threshold milliseconds	反応イベントを生成して処理の履歴情報を保存する上昇しきい値 (ヒステリシス) を設定します。

ステップ 7	exit	IP SLA ICMP エコー コンフィギュレーション モードを終了します。
ステップ 8	ip sla schedule <i>operation-number</i> [life { forever <i>seconds</i> }] start-time <i>time</i> pending now after <i>time</i>] [ageout <i>seconds</i>] [recurring]	IP SLA の単一動作のスケジューリング パラメータを設定します。
ステップ 9	track <i>object-number</i> rtr <i>operation-number</i> { state reachability }	Cisco IOS IP SLA の動作状態をトラッキングし、トラッキング コンフィギュレーション モードを開始します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show track <i>object-number</i>	トラッキング情報を表示して設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してバックアップ スタティック ルーティングのルーティング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。この手順のコマンドに関する詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list <i>access-list-number</i>	拡張 IP アクセス リストを定義します。任意のオプション特性を設定します。
ステップ 3	route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>]	ルートマップ コンフィギュレーション モードを開始し、ルートルーティング プロトコル間で再配信する条件を定義します。
ステップ 4	match ip address { <i>access-list number</i> <i>access-list name</i> }	標準または拡張アクセス リストで許可されている宛先ネットワーク番号アドレス、またはパケットでポリシー ルーティングを実行する宛先ネットワーク番号アドレスを持つルートをすべて配信します。番号または名前を複数入力できます。
ステップ 5	set ip next-hop dynamic dhcp	DHCP ネットワーク専用です。DHCP クライアントが最後に学習したゲートウェイへのネクスト ホップを設定します。
ステップ 6	set interface <i>interface-id</i>	スタティック ルーティング ネットワーク専用です。ポリシー ルーティングのルート マップの match コマンドに合格した出力パケットの送信先を指定します。
ステップ 7	exit	ルートマップ コンフィギュレーション モードを終了します。
ステップ 8	ip local policy route-map <i>map-tag</i>	ローカル ポリシー ルーティングに使用するルート マップを指定します。
ステップ 9	ip route <i>prefix mask</i> { <i>ip-address</i> <i>interface-id</i> [<i>ip-address</i>]} [<i>distance</i>] [<i>name</i>] [permanent track <i>track-number</i>] [<i>tag tag</i>]	スタティック ルーティング ネットワーク専用です。スタティック ルートを確立します。 track track-number を入力すると、スタティック ルートは設定されたトラッキング オブジェクトがアップの場合にだけインストールされます。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show ip route track table	IP ルートトラック テーブルに関する情報を表示します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定例については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

拡張オブジェクト トラッキングのモニタリング

表 44-1 に示す特権 EXEC コマンドまたはユーザ EXEC コマンドを使用して、拡張オブジェクト トラッキング情報を表示します。

表 44-1 トラッキング情報を表示するためのコマンド

コマンド	目的
show ip route track table	IP ルート トラック テーブルに関する情報を表示します。
show track [<i>object-number</i>]	すべてのトラッキング リストまたは指定したリストの情報を表示します。
show track brief	トラッキング情報出力を 1 行表示します。
show track interface [brief]	トラッキングするインターフェイス オブジェクトの情報を表示します。
show track ip [<i>object-number</i>] [brief] route	トラッキングする IP ルート オブジェクトの情報を表示します。
show track resolution	トラッキングするパラメータの分解能を表示します。
show track timers	トラッキングするポーリング インターバル タイマーを表示します。



CHAPTER 45

WCCP による Web キャッシュ サービスの設定

この章では、Web Cache Communication Protocol (WCCP) を使用し、トラフィックを広域アプリケーション エンジン (Cisco Cache Engine 550 など) にリダイレクトするように Catalyst 3750 スイッチを設定する方法について説明します。このソフトウェア リリースでは、WCCP バージョン 2 (WCCPv2) だけをサポートします。

WCCP はシスコが開発したコンテンツ ルーティング テクノロジーです。WCCP を使用すると広域アプリケーション エンジン (以降、アプリケーション エンジンと呼ぶ) をネットワーク インフラストラクチャに統合できます。アプリケーション エンジンは、頻繁にアクセスされるコンテンツを透過的に格納して、同じコンテンツに対する連続する要求に応えます。これにより Web サーバは同じコンテンツを繰り返し送信する必要がなくなります。アプリケーション エンジンを使用することでコンテンツの配信が高速化され、コンテンツのスケーラビリティとアベイラビリティが最大限に確保されます。サービス プロバイダー ネットワークでは、WCCP とアプリケーション エンジンによるソリューションを Point of Presence (POP; アクセス ポイント) に展開できます。企業ネットワークでは、WCCP とアプリケーション エンジンによるソリューションを地方のサイトや小規模の支店に展開できます。

この機能を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。特に明記しないかぎり、スイッチという用語はスタンドアロンスイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 の「*System Management Commands*」の「*WCCP Router Configuration Commands*」のセクションを参照してください。このマニュアルには、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] からアクセスできます。

この章で説明する内容は、次のとおりです。

- 「[WCCP の概要](#)」 (P.45-1)
- 「[WCCP の設定](#)」 (P.45-5)
- 「[WCCP のモニタおよびメンテナンス](#)」 (P.45-10)

WCCP の概要

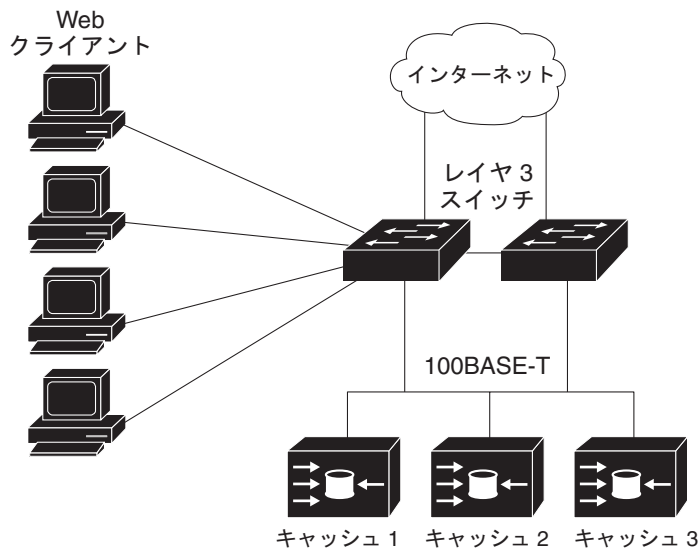
WCCP および Cisco Cache Engine (または WCCP が稼動する他のアプリケーション エンジン) は、ネットワークのトラフィック パターンをローカライズすることにより、コンテンツ要求をローカルで対応できます。

WCCP をサポートするシスコ製ルータおよびスイッチは、WCCP を使用してコンテンツ要求を透過的にリダイレクトできます。リダイレクションは透過的に行われるので、ブラウザを設定して Web プロキシを使用する必要がありません。ユーザはプロキシではなく、目的とする URL を使用してコンテンツを要求することができます。要求は自動的にアプリケーション エンジンにリダイレクトされます。透過的とは、要求したファイル（Web ページなど）が本来の指定したサーバからでなくアプリケーション エンジンから送信されている事実エンド ユーザは気づかないことを意味します。

アプリケーション エンジンは要求を受信すると、アプリケーション自身のローカル キャッシュを参照して要求を処理しようとします。要求された情報が存在しない場合は、独自に要求をエンドサーバに送信して要求された情報を取得します。要求された情報を受信すると要求元のクライアントに転送し、その後の同じ要求に応えられるようにキャッシュにも格納します。

アプリケーション エンジン クラスタ（アプリケーション エンジンの集合）は、WCCP を使用することで複数のルータやスイッチの要求を処理できます（図 45-1 を参照）。

図 45-1 Cisco Cache Engine と WCCP のネットワーク設定



WCCP メッセージ交換

WCCP メッセージ交換の一連の流れは、次のとおりです。

1. アプリケーション エンジンは、WCCP を使用して WCCP 対応スイッチに自己の IP アドレスを送信するとともに、*Here I am* メッセージで存在を伝えます。スイッチとアプリケーション エンジンは、UDP ポート 2048 に基づく制御チャネルを介して相互に通信します。
2. WCCP 対応スイッチは、アプリケーション エンジンの IP 情報を使用して、クラスタ ビュー（クラスタ内のアプリケーション エンジンの一覧）を作成します。このビューは *I see you* メッセージでクラスタ内の各アプリケーション エンジンに送信され、すべてのアプリケーション エンジンがお互いの存在を認識することになります。クラスタのメンバシップが一定時間を経過しても変わらなければ、安定したビューが確立されます。
3. 安定したビューが確立されると、クラスタ内で最も低い IP アドレスを持つアプリケーション エンジンが代表アプリケーション エンジンに選出されます。

WCCP ネゴシエーション

代表アプリケーション エンジンと WCCP 対応スイッチは、WCCP プロトコル メッセージを交換して次の項目のネゴシエーションを行います。

- 転送方法 (スイッチがアプリケーション エンジンにパケットを転送する方法)。スイッチは、パケットの宛先 MAC アドレスをターゲット アプリケーション エンジンの MAC アドレスに置き換えることで、レイヤ 2 ヘッダーを書き換えます。次に、そのパケットをアプリケーション エンジンに転送します。この転送方法を行うには、ターゲット アプリケーション エンジンとスイッチがレイヤ 2 レベルで直接接続されている必要があります。
- 割り当て方法 (クラスタ内のアプリケーション エンジン間にパケットを配信する方法)。スイッチは、宛先 IP アドレス、送信元 IP アドレス、宛先レイヤ 4 ポート、および送信元レイヤ 4 ポートの一部のビットを使用して、リダイレクトされたパケットを受信するアプリケーション エンジンを決めます。
- パケットリターン方法 (パケットをアプリケーション エンジンからスイッチに戻して通常転送を行う方法)。アプリケーション エンジンがパケットを拒否し、パケットリターン機能を実行する主な理由は、次のとおりです。
 - アプリケーション エンジンが過負荷になり、パケットを処理する余裕がなくなった場合
 - アプリケーション エンジンが Web サーバからエラー メッセージ (プロトコル エラーや認証エラーなど) を受信し、ダイナミック クライアント バイパス機能を使用する場合。この機能により、クライアントはアプリケーション エンジンを經由せず Web サーバに直接接続することができます。

アプリケーション エンジンがパケットを WCCP 対応スイッチに戻し、スイッチはアプリケーション エンジンが存在しないかのように Web サーバに転送します。アプリケーション エンジンは、再接続試行を代行受信しません。これにより、アプリケーション エンジンはアプリケーション エンジンへのパケットのリダイレクトを実質的に取り消し、バイパス フローを作成します。このリターン方法が **Generic-Route Encapsulation (GRE; 総称ルーティング カプセル化)** の場合、スイッチはアプリケーション エンジンに設定されている GRE トンネルを介して戻されたパケットを受信します。スイッチの CPU は、**Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング)** を使用して、これらのパケットを目的とする Web サーバに送信します。リターン方法がレイヤ 2 ヘッダーの書き換えの場合、パケットはハードウェアで目的とする Web サーバに転送されます。要求された情報がサーバから返されると、スイッチは通常のレイヤ 3 転送を使用して要求元のクライアントに情報を戻します。

MD5 セキュリティ

WCCP の各プロトコル メッセージにはセキュリティ コンポーネントがオプションとして用意されているので、スイッチはアプリケーション エンジンとのメッセージ交換に MD5 認証を使用できます。MD5 で認証されないメッセージ (スイッチの認証機能がイネーブルの場合) は、スイッチにより廃棄されます。パスワードストリングは MD5 値と組み合わせられ、スイッチとアプリケーション エンジンとの接続にセキュリティが確保されます。各アプリケーション エンジンには、同じパスワードを設定する必要があります。

パケット リダイレクションおよびサービス グループ

WCCP を設定することで、トラフィックを FTP、プロキシ Web キャッシュ処理、音声アプリケーション、およびビデオ アプリケーションなどに分類してリダイレクトすることができます。この分類は、サービス グループと呼ばれ、プロトコル タイプ (TCP または UDP) およびレイヤ 4 の送信元/宛先ポート番号に基づいて行われます。サービス グループは、Web キャッシュ (TCP ポート 80) などの well-known 名、またはサービス番号 (0 ~ 99) で識別されます。サービス グループは、プロトコルとレイヤ 4 ポート番号にマッピングされ、個別に確立され管理されます。WCCP ではダイナミック サービス グループを使用できます。このグループでは参加するアプリケーション エンジンによって分類基準がダイナミックに提供されます。

スイッチまたはスイッチ スタック上には、最大 8 つのサービス グループと、サービス グループあたり最大 32 のキャッシュ エンジンを設定できます。WCCP は、グループ定義内にサービス グループのプライオリティを管理しています。プライオリティは、スイッチ ハードウェア内のサービス グループの設定に使用されます。たとえば、プライオリティ 100 のサービス グループ 1 が宛先ポート 80 を待ち受け、プライオリティ 50 のサービス グループ 2 が送信元ポート 80 を待ち受けている場合、送信元および宛先ポート 80 の着信パケットは、プライオリティの高いサービス グループ 1 を使用して転送されます。

WCCP は、サービス グループごとにアプリケーション エンジンのクラスタをサポートします。リダイレクトするトラフィックを、クラスタ内の任意のアプリケーション エンジンに送信できます。スイッチは、サービス グループのクラスタ内のアプリケーション エンジン間でトラフィックのロード バランシングを行うマスク割り当て方式をサポートしています。

スイッチに WCCP が設定されると、スイッチはクライアントから受信したすべてのサービス グループのパケットを、アプリケーション エンジンに転送します。ただし、次のパケットはリダイレクトされません。

- アプリケーション エンジンから発信されて、Web サーバを宛先とするパケット
- アプリケーション エンジンから発信されて、クライアントを宛先とするパケット
- アプリケーション エンジンにより戻されたか、拒否されたパケット。これらのパケットは、Web サーバに送信されます。

プロトコル メッセージの送受信に、サービス グループあたり 1 つのマルチキャスト アドレスを設定できます。マルチキャスト アドレスが 1 つ設定されていると、アプリケーション エンジンは 1 つのアドレス (例: 225.0.0.0) 宛に通知を送信します。このアドレスは、サービス グループ内のすべてのルータを受信対象に含みます。1 つのマルチキャストアドレスを使用すると、ルータをダイナミックに追加したり取り外したりする場合に、WCCP ネットワーク内のすべてのデバイスのアドレスを個別に入力する手間が省けるので設定が容易になります。

アプリケーション エンジンから受信したプロトコル パケットの検証には、ルータ グループ リストを使用できます。グループ リスト内のアドレスに一致するパケットが処理され、一致しないパケットは破棄されます。

特定のクライアント、サーバ、またはクライアント/サーバ ペアのキャッシュをディセーブルにする場合は、WCCP リダイレクト ACL を使用できます。リダイレクト ACL に一致しないパケットは、キャッシュをバイパスし正常に転送されます。

WCCP パケットをリダイレクトする前に、スイッチはインターフェイス上に設定されているインバウンド方向のすべての機能に関連した ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。



(注) WCCP リダイレクト リストでは、許可 ACL エントリだけがサポートされます。

パケットがリダイレクトされる場合は、リダイレクトされるインターフェイスに関連付けられた出力 ACL がパケットに適用されます。元のポートに関連付けられた ACL は、リダイレクトされるインターフェイスに必要な出力 ACL を具体的に設定しないかぎり、適用されません。

WCCP とスイッチ スタック

スイッチ スタックの WCCP サポート機能は、スタンドアロン スイッチの場合と同じです。WCCP の設定情報は、スタック内のすべてのスイッチに伝播されます。スタック マスターを含むスタック内のすべてのスイッチは、情報を処理し、ハードウェアをプログラミングします。スイッチ スタックの詳細については、第 5 章「[スイッチ スタックの管理](#)」を参照してください。

スタック マスターは、次に示す WCCP 機能を実行します。

- WCCP 対応インターフェイスからプロトコル パケットを受信し、スタック内のすべての WCCP 対応インターフェイスに送信します。
- WCCP 設定を処理し、情報をすべてのスタック メンバーに伝播します。
- WCCP 情報をスタックに加入するすべてのスイッチに配信します。
- 処理する WCCP 情報を使用して、ハードウェアをプログラミングします。

スタック メンバーはマスター スイッチから WCCP 情報を受信し、ハードウェアをプログラミングします。

サポートされない WCCP 機能

次の WCCP 機能は、このソフトウェア リリースではサポートされません。

- **ip wccp redirect out** インターフェイス コンフィギュレーション コマンドを使用して設定する、アウトバウンド インターフェイスでのパケット リダイレクション。このコマンドはサポートされません。
- パケット リダイレクションに GRE フォワーディング方式は使用できません。
- ロード バランシングにハッシュ割り当て方式は使用できません。
- WCCP で SNMP はサポートされません。

WCCP の設定

ここでは、スイッチに WCCP を設定する手順について説明します。

- 「[WCCP のデフォルト設定](#)」(P.45-6)
- 「[WCCP 設定時の注意事項](#)」(P.45-6)
- 「[Web キャッシュ サービスのイネーブル化](#)」(P.45-7) (必須)

WCCP のデフォルト設定

表 45-1 に、WCCP のデフォルト設定を示します。

表 45-1 WCCP のデフォルト設定

機能	デフォルト設定
WCCP イネーブル ステート	WCCP サービスはディセーブル
プロトコル バージョン	WCCPv2
インターフェイスで受信したトラフィックのリダイレクト	ディセーブル

WCCP 設定時の注意事項

スイッチに WCCP を設定する前に、次に示す設定時の注意事項に従ってください。

- 同じサービス グループ内のアプリケーション エンジンとスイッチは、WCCP をイネーブルにしたスイッチが直接接続される同じサブネットワーク内にある必要があります。
- Web クライアント、アプリケーション エンジン、および Web サーバに接続されるスイッチ インターフェイスは、レイヤ 3 インターフェイス（ルーテッド ポートおよび Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)）として設定します。WCCP パケット リダイレクションが動作するには、サーバ、アプリケーション エンジン、およびクライアントは異なるサブネット上にある必要があります。
- 各アプリケーション エンジンに単一のマルチキャスト アドレスを設定する場合は、予約されていないマルチキャスト アドレスだけを使用してください。
- WCCP エントリと PBR エントリは、同じ TCAM リージョンを使用します。WCCP は、PBR をサポートするアクセス テンプレート、ルーティング テンプレート、およびデュアル IPv4/v6 ルーティング テンプレート上に限りサポートされます。
- WCCP エントリを追加する際に TCAM エントリが使用できない場合、パケットはリダイレクトされずに標準のルーティング テーブルを使用して転送されます。
- WCCP 入力リダイレクションをイネーブルにしたインターフェイスの数が増えると、使用可能な PBR ラベルの数は減ります。ラベルは、サービス グループをサポートするインターフェイスごとに 1 つ消費されます。WCCP ラベルは PBR ラベルから取得されます。PBR と WCCP の間で使用可能なラベルの数をモニタし、管理するようにしてください。ラベルが使用できないと、スイッチはサービス グループを追加できません。ただし、同じ順番のサービス グループを持つインターフェイスが別にある場合は、新しいラベルがなくてもインターフェイスにグループを追加できます。
- スタック メンバー スイッチに設定するルーティング最大伝送ユニット (Maximum Transmission Unit; MTU) サイズは、クライアントの MTU サイズより大きい必要があります。アプリケーション エンジンに接続されるポートに設定する MAC レイヤの MTU サイズには、GRE トンネル ヘッダーのバイト数を含める必要があります。
- WCCP と VPN Routing/Forwarding (VRF; VPN ルーティング/転送) は、同じスイッチ インターフェイスに設定できません。
- WCCP と PBR は、同じスイッチ インターフェイスに設定できません。
- WCCP とプライベート VLAN (PVLAN) は、同じスイッチ インターフェイスに設定できません。

Web キャッシュ サービスのイネーブル化

WCCP パケット リダイレクションが動作するには、クライアントに接続されたスイッチ インターフェイスが、インバウンド パケットをリダイレクトするように設定されている必要があります。

次に、ルーテッド ポートにこれらの機能を設定する方法を示します。これらの機能を SVI に設定する場合は、この手順のあとの設定例を参照してください。



(注) WCCP コマンドを設定する前に、SDM テンプレートを設定し、スイッチを再起動します。詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

Web キャッシュ サービスをイネーブルにする場合、マルチキャスト グループ アドレスまたはグループ リストを設定する場合、ルーテッド インターフェイスを設定する場合、クライアントから受信したインバウンド パケットをアプリケーション エンジンにリダイレクトする場合、マルチキャスト アドレスを待ち受けるようにインターフェイスをイネーブルにする場合、およびパスワードを設定する場合は、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip wccp {web-cache service-number} [group-address groupaddress] [group-list access-list] [redirect-list access-list] [password encryption-number password]</code>	<p>Web キャッシュ サービスをイネーブルにし、アプリケーション エンジンで定義されているダイナミック サービスに対応するサービス番号を指定します。デフォルトでは、この機能はディセーブルです。</p> <p>(任意) <code>group-address groupaddress</code> には、サービス グループに参加するスイッチおよびアプリケーション エンジンが使用するマルチキャスト グループ アドレスを指定します。</p> <p>(任意) マルチキャスト グループ アドレスを使用しない場合、<code>group-list access-list</code> には、サービス グループに参加するアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。</p> <p>(任意) <code>redirect-list access-list</code> には、特定のホストまたはホストからの特定の packets に対するリダイレクト サービスを指定します。</p> <p>(任意) <code>password encryption-number password</code> には、暗号化番号を指定します。指定できる範囲は 0 ~ 7 です。暗号化しない場合は 0 を、独自の暗号化方式の場合は 7 を使用します。パスワード名には最大 7 文字を指定します。スイッチは、パスワードと MD5 認証値を組み合わせて、スイッチとアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトではパスワードは設定されません。認証も行われません。</p> <p>各アプリケーション エンジンには、同じパスワードを設定する必要があります。</p> <p>認証をイネーブルにした場合、認証されなかったメッセージは廃棄されます。</p>
ステップ 3	<code>interface interface-id</code>	アプリケーション エンジンまたは Web サーバに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>no switchport</code>	レイヤ 3 モードを開始します。
ステップ 5	<code>ip address ip-address subnet-mask</code>	IP アドレスおよびサブネット マスクを設定します。
ステップ 6	<code>no shutdown</code>	インターフェイスをイネーブルにします。

	コマンド	目的
ステップ 7	exit	グローバル コンフィギュレーション モードに戻ります。アプリケーション エンジンおよび Web サーバごとに、ステップ 3 ~ 7 を繰り返します。
ステップ 8	interface interface-id	クライアントに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	no switchport	レイヤ 3 モードを開始します。
ステップ 10	ip address ip-address subnet-mask	IP アドレスおよびサブネット マスクを設定します。
ステップ 11	no shutdown	インターフェイスをイネーブルにします。
ステップ 12	ip wccp {web-cache service-number} redirect in	クライアントから受信したパケットを、アプリケーション エンジンにリダイレクトします。クライアントに接続するインターフェイスで、これをイネーブルにします。
ステップ 13	ip wccp {web-cache service-number} group-listen	(任意) マルチキャスト グループ アドレスを使用する場合、 group-listen によりインターフェイスでマルチキャスト アドレスの待ち受けが可能になります。アプリケーション エンジンに接続するインターフェイスで、これをイネーブルにします。
ステップ 14	exit	グローバル コンフィギュレーション モードに戻ります。各クライアントで、ステップ 8 ~ 13 を繰り返します。
ステップ 15	end	特権 EXEC モードに戻ります。
ステップ 16	show ip wccp web-cache および show running-config	設定を確認します。
ステップ 17	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Web キャッシュ サービスをディセーブルにするには、**no ip wccp web-cache** グローバル コンフィギュレーション コマンドを使用します。インバウンド パケット リダイレクションをディセーブルにするには、**no ip wccp web-cache redirect in** インターフェイス コンフィギュレーション コマンドを使用します。この手順が完了したら、ネットワークのアプリケーション エンジンを設定してください。

次に、ルーテッド インターフェイスを設定する例、およびマルチキャスト グループ アドレスとリダイレクト アクセス リストを使用して Web キャッシュ サービスをイネーブルにする例を示します。ギガビットイーサネットのポート 1 をアプリケーション エンジンに接続し、IP アドレス 172.20.10.30 のルーテッド ポートとして設定してから、再度イネーブルにします。ギガビットイーサネットのポート 2 をインターネット経由で Web サーバに接続し、IP アドレス 175.20.20.10 のルーテッド ポートとして設定してから、再度イネーブルにします。ギガビットイーサネットのポート 3 ~ 6 をクライアントに接続し、IP アドレス 175.20.30.20、175.20.40.30、175.20.50.40、および 175.20.60.50 のルーテッド ポートとして設定します。スイッチはマルチキャスト トラフィックを待ち受け、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
```

```

Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.40.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.50.40 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/6
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.60.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit

```

次に、SVI を設定し、マルチキャスト グループ リストを使用して Web キャッシュ サービスをイネーブ
ルにする例を示します。VLAN 299 を作成し、IP アドレス 175.20.20.10 に設定します。ギガビット
イーサネットのポート 1 をインターネット経由で Web サーバに接続し、VLAN 299 のアクセス ポート
として設定します。VLAN 300 を作成し、IP アドレス 172.20.10.30 に設定します。ギガビットイーサ
ネットのポート 2 をアプリケーション エンジンに接続し、VLAN 300 のアクセス ポートとして設定し
ます。VLAN 301 を作成し、IP アドレス 175.20.30.50 に設定します。ファストイーサネットのポート
3～6 をクライアントに接続し、VLAN 301 のアクセス ポートとして設定します。スイッチはクライ
アント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。



(注) リダイレクトリストには許可 ACL エントリだけを使用します。拒否エントリはサポートされていませ
ん。

```

Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-list 15
Switch(config)# access-list 15 permit host 171.69.198.102
Switch(config)# access-list 15 permit host 171.69.198.104
Switch(config)# access-list 15 permit host 171.69.198.106
Switch(config)# vlan 299
Switch(config-vlan)# exit
Switch(config)# interface vlan 299
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 299
Switch(config)# vlan 300
Switch(config-vlan)# exit
Switch(config)# interface vlan 300
Switch(config-if)# ip address 171.69.198.100 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 300

```

```

Switch(config-if)# exit
Switch(config)# vlan 301
Switch(config-vlan)# exit
Switch(config)# interface vlan 301
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 301
Switch(config-if-range)# exit

```

WCCP のモニタおよびメンテナンス

WCCP をモニタしてメンテナンスするには、表 45-2 に記載された特権 EXEC コマンドを 1 つまたは複数使用します。

表 45-2 WCCP のモニタリングおよびメンテナンスのためのコマンド

コマンド	目的
<code>clear ip wccp web-cache</code>	Web キャッシュ サービスの統計情報を削除します。
<code>show ip wccp web-cache</code>	WCCP に関連するグローバル情報を表示します。
<code>show ip wccp web-cache detail</code>	スイッチおよび WCCP クラスタ内のすべてのアプリケーション エンジンを表示します。
<code>show ip interface</code>	インターフェイスに設定されたすべての IP WCCP リダイレクション コマンドのステータスを表示します (Web Cache Redirect is enabled / disabled のように表示)。
<code>show ip wccp web-cache view</code>	他の検出されたメンバーまたは検出されなかったメンバーを表示します。



CHAPTER 46

IP マルチキャスト ルーティングの設定

この章では、Catalyst 3750 スイッチに IP マルチキャスト ルーティングを設定する方法について説明します。IP マルチキャストは、ネットワークのリソースをより効率的に使用する方法です。特に、音声やビデオなど、帯域幅を消費するサービスに効果があります。IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP 「マルチキャスト グループ アドレス」と呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバー）のグループにパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレスフィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャストグループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーのみです。

IP マルチキャスト ルーティング機能を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。PIM スタブルーティング機能を使用する場合は、スタック マスター上で IP ベース イメージを稼動することができます。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』Release 12.2 を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- 「IP マルチキャスト ルーティングの実装の概要」 (P.46-2)
- 「マルチキャスト ルーティングおよびスイッチ スタック」 (P.46-11)
- 「IP マルチキャスト ルーティングの設定」 (P.46-11)
- 「高度な PIM 機能の設定」 (P.46-38)
- 「オプションの IGMP 機能の設定」 (P.46-41)
- 「オプションのマルチキャスト ルーティング機能の設定」 (P.46-47)
- 「基本的な DVMRP 相互運用性機能の設定」 (P.46-52)
- 「高度な DVMRP 相互運用性機能の設定」 (P.46-57)
- 「IP マルチキャスト ルーティングのモニタおよびメンテナンス」 (P.46-65)

Multicast Source Discovery Protocol (MSDP) の設定の詳細については、第 47 章「MSDP の設定」を参照してください。

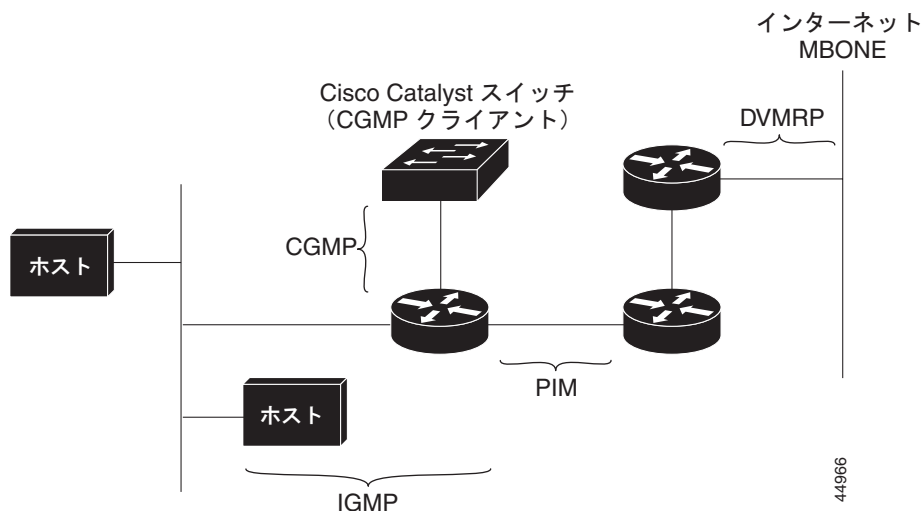
IP マルチキャスト ルーティングの実装の概要

Cisco IOS ソフトウェアは IP マルチキャスト ルーティングを実装するため、次のプロトコルをサポートしています。

- **Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)** : LAN のホストおよび LAN のルータ (およびマルチレイヤ スイッチ) 間で使用され、ホストがメンバーとして属するマルチキャスト グループをトラッキングします。
- **Protocol-Independent Multicast (PIM)** : ルータおよびマルチレイヤ スイッチ間で使用され、相互に転送されるマルチキャスト パケット、および直接接続された LAN に転送されるマルチキャスト パケットをトラッキングします。
- **Distance Vector Multicast Routing Protocol (DVMRP; ディスタンスベクトル マルチキャスト ルーティング プロトコル)** : インターネットの **Multicast Backbone (MBONE; マルチキャスト バックボーン)** に使用されます。ソフトウェアは PIM と DVMRP の相互作用をサポートします。
- **Cisco Group Management Protocol (CGMP)** : レイヤ 2 Catalyst スイッチに接続されたシスコ ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。

図 46-1 に、これらのプロトコルが動作する IP マルチキャスト環境内の位置を示します。

図 46-1 IP マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト規格に従って、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの最後の 23 ビットが付加されます。Catalyst 3750 スイッチでは、マルチキャスト パケットがスイッチのマルチキャスト アドレスと一致しない場合、パケットは次のように取り扱われます。

- パケットにマルチキャスト IP アドレスとユニキャスト MAC アドレスがある場合、パケットはソフトウェアで転送されます。これは、従来型デバイスのプロトコルの中に、マルチキャスト IP アドレスとともにユニキャスト MAC アドレスを使用するものがあるために発生します。
- パケットにマルチキャスト IP アドレスと不一致のマルチキャスト MAC アドレスがある場合、パケットはドロップします。

ここでは、次の内容について説明します。

- 「[IGMP の概要](#)」 (P.46-3)
- 「[PIM の概要](#)」 (P.46-4)
- 「[DVMRP の概要](#)」 (P.46-10)

- 「CGMP の概要」(P.46-10)

IGMP の概要

IP マルチキャストリングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。このプロトコルは、クエリアおよびホストの役割を定義します。

- クエリアは、指定されたマルチキャスト グループに属するネットワーク デバイスを検出するためのクエリー メッセージを送信するネットワーク デバイスです。
- ホストは、クエリアにホスト メンバシップを通知するためのレポート メッセージ (クエリー メッセージに応答するメッセージ) を送信するレシーバーです。

同じ送信元からマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは IGMP メッセージを使用して、マルチキャスト グループに加入したり、脱退したりします。

グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーのみです。マルチキャスト グループのメンバシップはダイナミックです。ホストはいつでもグループに加入し、また脱退できます。マルチキャスト グループの場所またはメンバー数に制限はありません。ホストは一度に複数のマルチキャストのメンバーになることができます。マルチキャスト グループのアクティブ状態および所属メンバーは、グループや時間によって変化し、マルチキャスト グループを長時間または短時間アクティブにすることもできます。グループのメンバシップはいつでも変更可能です。メンバーを含むグループにアクティブでない場合もあります。

IP マルチキャスト トラフィックには、グループ アドレス (クラス D アドレス) が使用されます。クラス D アドレスの上位ビットは 1110 です。したがって、ホスト グループ アドレスは 224.0.0.0 ~ 239.255.255.255 の範囲を取ります。224.0.0.0 ~ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために確保されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは、次に示す IP マルチキャスト グループ アドレスを使用して送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1 (サブネット上のすべてのシステム) を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象グループの IP アドレスを宛先とします。
- IGMP グループ メンバシップ レポートは、レポート対象グループの IP アドレスを宛先とします。
- IGMPv2 (IGMP バージョン 2) Leave メッセージは、アドレス 224.0.0.2 (サブネット上のすべてのマルチキャスト ルータ) を宛先とします。古いホスト IP スタックの中には、Leave メッセージの宛先がすべてのルータのアドレスでなく、グループの IP アドレスであるものがあります。

IGMP バージョン 1

IGMPv1 (IGMP バージョン 1) にはクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ スイッチは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか (マルチキャスト グループに関係するホストが 1 台または複数存在するか) を判別できません。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMPv2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

PIM の概要

PIM は「プロトコルに依存しない」マルチキャストと呼ばれます。ユニキャスト ルーティング テーブルを読み込むために使用されるユニキャスト ルーティング プロトコルに関係なく、PIM はこのテーブルの情報を使用してマルチキャスト転送を実行します。マルチキャスト ルーティング テーブルは個別に維持されません。

PIM は、RFC 2362 『*Protocol-Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification*』で定義されています。次に示す Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) インターネット ドラフトを参照してください。

- 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』
- 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』
- 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』
- 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』
- 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ Rendezvous Point (RP; ランデブー ポイント) を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- Bootstrap Router (BSR; ブートストラップ ルータ) はフォールトトレラントな、自動化された RP ディスカバリ メカニズム、および配信メカニズムを提供します。これらのメカニズムにより、ルータおよびマルチレイヤ スイッチはグループ/RP マッピングをダイナミックに取得できます。
- 希薄モード (SM) および dense (稠密) モード (DM) は、インターフェイスではなく、グループに関するプロパティです。SM または DM のいずれか一方のみでなく、SM-DM (sparse-dense モード) を使用してください。
- PIM の Join メッセージおよび Prune メッセージを使用すると、複数のアドレス ファミリーを柔軟に符号化できます。
- 現在は以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RP への登録メッセージが境界ルータによって送信されるか、あるいは代表ルータによって送信されるかは、メッセージ自身によって指定されます。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

PIM のモード

PIM は DM、SM、または PIM SM-DM のいずれかのモードで動作します。PIM DM-SM では、希薄グループと dense（稠密）グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元ベースのマルチキャスト配信ツリーが構築されます。DM の場合、PIM DM のルータまたはマルチレイヤ スイッチは、他のすべてのルータまたはマルチレイヤ スイッチで常にグループ宛のマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバーが存在しない場合、PIM DM デバイスがマルチキャスト パケットを受信すると、Prune メッセージが送信元に送信され、不要なマルチキャスト トラフィックが停止されます。このプルニング済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラッディングしません。レシーバーを含まないブランチが配信ツリーからプルニングされ、レシーバーを含むブランチのみが存続するためです。

プルニング済みのツリー内ブランチのレシーバーがマルチキャスト グループに新規に加入すると、PIM DM デバイスは新しいレシーバーを検出し、配信ツリーの送信元方向にすぐに接合メッセージを送信します。アップストリームの PIM DM デバイスが接合メッセージを受信すると、受信したデバイスは接合メッセージが着信したインターフェイスをすぐにフォワーディング ステートにし、マルチキャスト トラフィックのレシーバーへの転送を開始します。

PIM SM

PIM SM は共有ツリーおよび Shortest-Path-Trees (SPT) を使用し、マルチキャスト トラフィックをネットワーク内のマルチキャスト レシーバーに配信します。PIM SM の場合、ルータまたはマルチレイヤ スイッチは、トラフィックに関する明示的な要求 (Join メッセージ) がないかぎり、他のルータまたはスイッチではグループ宛のパケットが転送されないと想定します。IGMP を使用してホストがマルチキャスト グループに加入すると、直接接続された PIM SM デバイスは、RP と呼ばれるルートに向けて PIM Join メッセージを送信します。この Join メッセージはルートに向かってルータを順次移動しながら、共有ツリーのブランチを作成します。

RP はマルチキャスト レシーバーをトラッキングします。また、送信元の先頭ホップ ルータ (Designated Router (DR; 代表ルータ)) から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバーへの共有ツリー パスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信し、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルニングする場合は、Prune メッセージが配信ツリーの上方向に送信されます。この結果、明示的な Join メッセージによって作成された共有ツリーまたは SPT のブランチが不要になった場合、これらを解除することが可能となります。

PIM スタブルーティング

PIM スタブルーティング機能は、すべてのソフトウェア イメージで使用することができ、エンドユーザの近くにルーテッド トラフィックを移動することでリソースの利用率が軽減されます。



(注)

IP ベース イメージには PIM スタブルーティングのみが含まれています。IP サービス イメージには、完全なマルチキャスト ルーティングが含まれています。IP ベース イメージが稼動するスイッチで、VLAN インターフェイスを PIM DM、SM、または SM-DM に設定しようとしても、設定は許可されません。

PIM スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートのみが PIM スタブ ルーティングを設定しているスイッチを通過します。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメインに接続されるか、他のレイヤ 2 デバイスを接続先とするインターフェイスに接続されます。直接接続されるマルチキャスト (IGMP) 受信者と送信元のみが、レイヤ 2 アクセス ドメイン内に許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットの送信や処理を行いません。

PIM スタブ ルーティングを使用する場合、分散ルータとリモートルータで IP マルチキャスト ルーティングを使用するように設定し、スイッチのみを PIM スタブ ルータとして設定するようにしてください。スイッチは、分散ルータ間で中継トラフィックをルーティングしません。また、スイッチにルーテッドアップリンク ポートを設定する必要があります。スイッチのアップリンク ポートは SVI と併用できません。SVI アップリンク ポートに PIM が必要な場合は、IP サービス フィーチャ セットにアップグレードする必要があります。

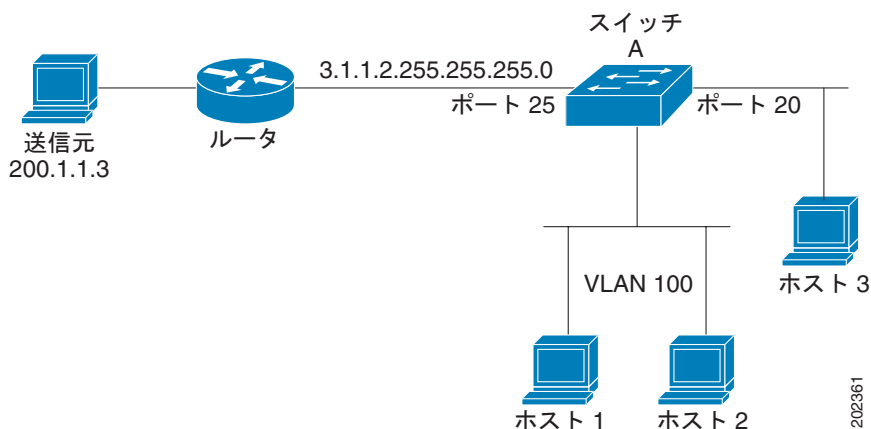
スイッチに PIM スタブ ルーティングを設定する場合は、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「[EIGRP スタブ ルーティングの設定](#)」(P.38-45) を参照してください。

冗長 PIM スタブ ルータ トポロジはサポートされません。マルチキャスト トラフィックをシングル アクセス ドメインにフォワーディングする PIM ルータが複数存在すると、冗長 トポロジになります。PIM メッセージはブロックされ、PIM アセットおよび代表ルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能は、非冗長アクセスルータ トポロジのみをサポートします。非冗長 トポロジを使用することで、PIM 受動インターフェイスは自己がアクセス ドメイン上の唯一のインターフェイスで代表ルータであると想定します。

PIM スタブ機能は、IP ベース イメージに実装されています。上位のソフトウェア バージョンにアップグレードした場合、インターフェイスを再設定するまで PIM スタブ設定は残ります。

図 46-2 で、スイッチ A のルーテッドアップリンク ポート 25 はルータに接続されており、VLAN 100 インターフェイスおよびホスト 3 で PIM スタブ ルーティングがイネーブルになっています。この設定により、直接接続されているホストはマルチキャスト送信元 200.1.1.3 からのトラフィックを受信できます。詳細については、「[PIM スタブ ルーティングの設定](#)」(P.46-25) を参照してください。

図 46-2 PIM スタブ ルータ設定



IGMP ヘルパー

PIM スタブ ルーティングはルーティングされたトラフィックをエンド ユーザの近くに移動させ、ネットワーク トラフィックを軽減します。また、スタブ ルータ（スイッチ）に IGMP ヘルパー機能を設定してトラフィックを軽減させることもできます。

igmp helper help-address インターフェイス コンフィギュレーション コマンドを使用してスタブ ルータ（スイッチ）を設定し、スイッチからネクスト ホップ インターフェイスにレポートを送信できます。このようにすると、ダウンストリーム ルータに直接接続していないホストはアップストリーム ネットワークからのマルチキャスト グループに参加できます。この機能を設定すると、マルチキャスト ストリームへの参加を待機しているホストの IGMP パケットがアップストリームのネクスト ホップ デバイスに転送されます。アップストリーム中央ルータがヘルパー IGMP レポートを受信した場合や脱退した場合、ルータはそのグループの発信インターフェイス リストにインターフェイスを追加または削除します。

ip igmp helper-address コマンドの詳しい構文と使い方については、『Cisco IOS IP and IP Routing Command Reference』 Release 12.1 を参照してください。

自動 RP

この独自の機能により、ネットワーク内のルータまたはマルチレイヤ スイッチごとに RP 情報を手動で設定する必要がなくなります。自動 RP を機能させるには、シスコのルータまたはマルチレイヤ スイッチをマッピング エージェントとして設定します。マッピング エージェントは IP マルチキャストを使用して、候補 RP アナウンスメントを受信する候補 RP として設定可能なネットワーク内のルータまたはスイッチを取得します。候補 RP はマルチキャスト RP アナウンス メッセージを特定のグループまたはグループ範囲に定期的に送信し、それらが使用可能であることをアナウンスします。

マッピング エージェントはこれらの候補 RP アナウンスメントをリスニングし、この情報を使用して、グループ/RP マッピング キャッシュにエントリを作成します。受信されたグループ/RP 範囲に対して複数の候補 RP が RP アナウンスメントを送信した場合でも、この範囲には 1 つのマッピング キャッシュ エントリのみが作成されます。RP アナウンス メッセージ着信時に、マッピング エージェントは IP が最大であるルータまたはスイッチをアクティブ RP として選択し、この RP アドレスをグループ/RP マッピング キャッシュ内に保存します。

マッピング エージェントは、グループ/RP マッピング キャッシュの内容を定期的にマルチキャストします。このため、すべてのルータおよびスイッチで、サポート対象のグループに使用される RP が自動的に検出されます。ルータまたはスイッチが RP ディスカバリ メッセージの受信に失敗し、グループ/RP マッピング情報が期限切れになると、ルータまたはスイッチは、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって定義された、スタティックに設定された RP に切り替わります。スタティックに設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を DM に変更します。

複数の RP がさまざまなグループ範囲として、または互いのホット バックアップとして機能します。

BSR

PIMv2 BSR は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤ スイッチに配信する別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップバイホップでフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由してホップバイホップで送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージのみを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR によって、Time to Live (TTL; 存続可能時間) 値が 1 である BSR メッセージが送信されます。近接する PIMv2 ルータまたはマルチレイヤ スイッチは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス (BSR メッセージの着信インターフェイスを除く) にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップバイホップで移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディングメカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズメントを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップバイホップで移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送およびリバース パス チェック

ユニキャスト ルーティングの場合、ルータおよびマルチレイヤ スイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが格納されている宛先ホストへ、ネットワーク内の単一のパスに沿ってトラフィックを送信します。パス上の各ルータおよびスイッチはユニキャスト ルーティング テーブル内の宛先アドレスを参照し、指定されたインターフェイスを経由して、宛先方向のネクストホップへパケットを転送します。そのあと、パケット内の宛先 IP アドレスを使用して、ユニキャスト転送判断を行います。

マルチキャストルーティングの場合、送信元は IP パケットの宛先アドレス フィールドに格納された、マルチキャスト グループ アドレスで表されるホストの任意のグループにトラフィックを送信します。着信マルチキャスト パケットを転送するかドロップするかを決定するため、ルータまたはマルチレイヤ スイッチで、パケットに対する RPF チェックを実行します (図 46-3 を参照)。

1. ルータまたはマルチレイヤ スイッチは着信したマルチキャスト パケットの送信元アドレスを調べ、リバース パス上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。
2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス (ルータのすべてのインターフェイスとは限りません) にパケットが転送されます。
3. RPF チェックに失敗した場合、パケットは廃棄されます。

DVMRP など一部のマルチキャスト ルーティング プロトコルでは、マルチキャスト ルーティング テーブルは個別に維持され、RPF チェックに使用されます。ただし、PIM では RPF チェックを実行するためにユニキャスト ルーティング テーブルが使用されます。

図 46-3 に、送信元 151.10.3.21 からのマルチキャスト パケットを受信するポート 2 を示します。表 46-1 により、送信元へのリバース パス上にあるポートはポート 2 ではなく、ポート 1 であることがわかります。RPF チェックに失敗したため、マルチレイヤ スイッチはパケットを廃棄します。送信元 151.10.3.21 からの別のマルチキャスト パケットは、ポート 1 に着信します。ルーティング テーブルにより、このポートは送信元へのリバース パス上にあることがわかります。RPF チェックに合格したため、パケットは発信ポート リスト内のすべてのポートに転送されます。

図 46-3 RPF チェック

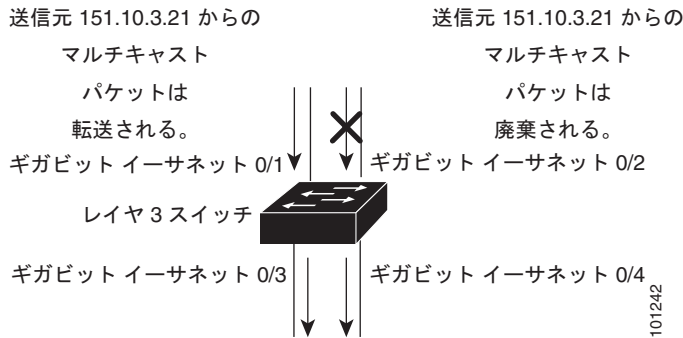


表 46-1 RPF チェックのルーティング テーブル例

ネットワーク	ポート
151.10.0.0/16	ギガビット イーサネット 1/0/1
198.14.32.0/32	ギガビット イーサネット 1/0/3
204.1.16.0/24	ギガビット イーサネット 1/0/4

PIM は送信元ツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します (「PIM DM」 (P.46-5) および 「PIM SM」 (P.46-5) を参照)。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤ スイッチが送信元ツリー ステートである場合 (つまり [S,G] エントリがマルチキャスト ルーティング テーブル内にある場合)、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ スイッチが共有ツリー ステートである場合 (および送信元ツリー ステートが明示されていない場合)、(メンバーがグループに加入している場合は既知である) RP アドレスについて RPF チェックが実行されます。

PIM SM は RPF 参照機能を使用し、加入および Prune メッセージを送信する必要があるかどうかを決定します。

- (S,G) Join メッセージ (送信元ツリー ステート) は送信元に向け送信されます。
- (*,G) Join メッセージ (共有ツリー ステート) は RP に向け送信されます。

DVMRP および PIM DM では送信元ツリーのみが使用され、上記のように RPF が使用されます。

DVMRP の概要

DVMRP は多くのベンダーのデバイスに実装されており、パブリック ドメインでマルチキャスト ルーティング (mroute) されたプログラムに基づいて動作します。このプロトコルは MBONE、およびその他のドメイン内マルチキャスト ネットワークに採用されています。

シスコ ルータおよびマルチレイヤ スイッチでは PIM が動作し、マルチキャスト パケットの DVMRP ネイバーへの転送および、DVMRP ネイバーからの受信を可能にします。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。ソフトウェアは DVMRP ルートを伝播し、ルータやマルチレイヤ スイッチごとにこれらのルートのデータベースを個別に構築します。ただし、PIM はこのルーティング情報をパケット転送判断に使用します。ソフトウェアに完全な DVMRP は実装されていません。ただし、DVMRP ルータのダイナミック ディスカバリをサポートし、従来のメディア (イーサネットや Fiber Distributed Data Interface (FDDI; ファイバ分散データ インターフェイス) など) または DVMRP 固有のトンネルを通して、これらを相互運用します。

DVMRP ネイバーは、送信元ネットワーク ルーティング情報をルートレポート メッセージに格納して定期的に交換し、ルート テーブルを構築します。DVMRP ルーティング テーブルに格納されているルーティング情報は、ユニキャスト ルーティング テーブルから独立し、送信元配信ツリーの構築および、RPF によるマルチキャスト転送の実行に使用されます。

DVMRP は DM プロトコルです。抑制されたマルチキャスト モデルを使用して親子データベースを構築し、マルチキャスト パケットの送信元でルーティングされた転送ツリーを構築します。マルチキャスト パケットはまず、この送信元ツリーの下方向にフラッディングされます。冗長パスが送信元ツリー上にある場合、パケットはこれらのパスに沿って転送されません。これらの親子リンクで Prune メッセージが受信されるまで転送が行われ、これによってマルチキャスト パケットのブロードキャストが抑制されます。

CGMP の概要

このソフトウェア リリースは、スイッチ上で CGMP サーバ サポート機能を提供します。クライアント側の機能は提供されません。スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれているデバイス用の CGMP サーバとして機能します。

CGMP はレイヤ 2 Catalyst スイッチに接続されたシスコ ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。CGMP を使用すると、レイヤ 2 グループ メンバシップ情報を CGMP サーバからスイッチに通信できます。これにより、スイッチはすべてのスイッチ インターフェイスにマルチキャストトラフィックをフラッディングしないで、マルチキャストメンバーが存在するインターフェイスを取得できるようになります (IGMP スヌーピングは、マルチキャスト パケットのフラッディングを抑制するためのもう 1 つの方法です。詳細は、[第 25 章「IGMP スヌーピングおよび MVR の設定」](#)を参照してください)。

CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポートメッセージを区別できないためです。これらはともに MAC レベルで、同じグループアドレスにアドレッシングされます。

CGMP は HSRPv1 と相互に排他的です。CGMP 脱退処理と HSRPv1 を同時にイネーブルにすることはできません。ただし、CGMP と HSRPv2 は同時にイネーブルにできます。詳細については、「[HSRP バージョン」\(P.42-4\)](#)を参照してください。

マルチキャスト ルーティングおよびスイッチ スタック

すべてのマルチキャスト ルーティング プロトコルでは、スタック全体が単一ルータとしてネットワークに認識され、単一のマルチキャスト ルータとして動作します。

Catalyst 3750 スイッチ スタックでは、ルーティング マスター (スタック マスター) は次の機能を実行します。

- スタックの IP マルチキャスト ルーティング機能を実行します。IP マルチキャスト ルーティング プロトコルを完全に初期化して、実行します。
- スタック全体のマルチキャスト ルーティング テーブルを構築して、保持します。
- マルチキャスト ルーティング テーブルをすべてのスタック メンバーに配信します。

スタック メンバーは、次に示す機能を実行します。

- マルチキャスト ルーティング スタンバイ デバイスとして機能し、スタック マスターに障害が発生した場合に処理を引き継ぎます。スタック マスターに障害が発生すると、すべてのスタック メンバーは自身のマルチキャスト ルーティング テーブルを削除します。新規に選択されたスタック マスターはルーティング テーブルの構築を開始して、スタック メンバーに配信します。



(注) IP サービス イメージを実行しているスタック マスターで障害が発生し、新しく選択されたスタック マスターで IP ベース イメージ (以前の標準マルチレイヤ イメージ [SMI]) が稼動している場合、そのスイッチ スタックのマルチキャスト ルーティング機能は失われます。

スタック マスターの選択プロセスについては、[第 5 章「スイッチ スタックの管理」](#)を参照してください。

- マルチキャスト ルーティング テーブルを構築しないで、スタック マスターから配信されたマルチキャスト ルーティング テーブルを使用します。

IP マルチキャスト ルーティングの設定

ここでは、次の設定情報について説明します。

- 「[マルチキャスト ルーティングのデフォルト設定](#)」 (P.46-12)
- 「[マルチキャスト ルーティング設定時の注意事項](#)」 (P.46-12)
- 「[基本的なマルチキャスト ルーティングの設定](#)」 (P.46-14) (必須)
- 「[SSM の設定](#)」 (P.46-15)
- 「[SSM マッピングの設定](#)」 (P.46-19)
- 「[PIM スタブ ルーティングの設定](#)」 (P.46-25) (任意)
- 「[RP の設定](#)」 (P.46-26) (インターフェイスが SM モードで、グループを希薄グループとして扱う場合に必須)
- 「[自動 RP および BSR の使用](#)」 (P.46-37) (他社製の PIMv2 デバイスをシスコ製 PIMv1 デバイスと相互運用する場合に必須)
- 「[RP マッピング情報のモニタ](#)」 (P.46-38) (任意)
- 「[PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング](#)」 (P.46-38) (任意)

マルチキャスト ルーティングのデフォルト設定

表 46-2 に、マルチキャスト ルーティングのデフォルト設定を示します。

表 46-2 マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kbps
PIM ルータ クエリー メッセージ インターバル	30 秒

マルチキャスト ルーティング設定時の注意事項

スイッチ上でのマルチキャスト ルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

- 「[PIMv1 および PIMv2 の相互運用性](#)」(P.46-12)
- 「[自動 RP および BSR 設定時の注意事項](#)」(P.46-13)

PIMv1 および PIMv2 の相互運用性

シスコの PIMv2 実装機能を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合があります。

PIMv2 に付加的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準のトラッキング プロトコルです。したがって、PIMv2 の使用を推奨します。BSR メカニズムは、シスコのルータおよびマルチレイヤ スイッチ上の自動 RP と相互運用します。詳細については、「[自動 RP および BSR 設定時の注意事項](#)」(P.46-13) を参照してください。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への変換を簡単に行うための推奨事項は次のとおりです。

- 領域全体で自動 RP を使用します。
- 領域全体で SM-DM を設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。詳細については、「[自動 RP の設定](#)」(P.46-28) を参照してください。

自動 RP および BSR 設定時の注意事項

PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- 使用しているネットワークがすべてシスコ ルータおよびマルチレイヤ スイッチである場合は、自動 RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- シスコの PIMv1 および PIMv2 ルータとマルチレイヤ スイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- ブートストラップ メッセージはホップバイホップで送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤ スイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、シスコ ルータおよびマルチレイヤ スイッチのみが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、シスコ PIMv2 ルータまたはマルチレイヤ スイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。詳細については、「[自動 RP および BSR の使用](#)」(P.46-37) を参照してください。

基本的なマルチキャスト ルーティングの設定

IP マルチキャスト ルーティングをイネーブルにし、PIM バージョンおよび PIM モードを設定する必要があります。これにより、ソフトウェアはマルチキャスト パケットを転送し、スイッチがそのマルチキャスト ルーティング テーブルを読み込むことができます。

インターフェイスは PIM DM、SM、または SM-DM のいずれかに設定できます。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。IP マルチキャスト ルーティングを実行するには、インターフェイスに対して、これらの PIM モードのいずれかをイネーブルにする必要があります。インターフェイスで PIM をイネーブルにすると、同じインターフェイス上で IGMP 処理もイネーブルになります。



(注)

複数のインターフェイスで PIM をイネーブルにした場合、そのほとんどのインターフェイスが発信インターフェイス リストになく、IGMP スヌーピングがディセーブルであると、余分なレプリケーションのために発信インターフェイスでマルチキャスト トラフィックのラインレートを維持することができません。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。特定の送信元からのマルチキャスト トラフィックが十分であれば、レシーバーの先頭ホップ ルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

デフォルトでは、マルチキャスト ルーティングはディセーブルとなっており、モードは設定されていません。この手順は必須です。

IP マルチキャストをイネーブルにし、PIM バージョンおよび PIM モードを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip multicast-routing distributed</code>	IP マルチキャストによる分散スイッチングをイネーブルにします。
ステップ 3	<code>interface interface-id</code>	<p>マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッド ポート : <code>no switchport</code> インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI : <code>interface vlan vlan-id</code> グローバル コンフィギュレーション コマンドを使用して作成された VLAN (仮想 LAN) インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。詳細については、「レイヤ 3 インターフェイスの設定」(P.12-28)を参照してください。</p>

コマンド	目的
ステップ 4 <code>ip pim version [1 2]</code>	<p>インターフェイスに PIM バージョンを設定します。</p> <p>デフォルトでは、バージョン 2 がイネーブルです（推奨設定）。</p> <p>PIMv2 モードのインターフェイスに PIMv1 ネイバーが存在する場合、インターフェイスは自動的に PIMv1 モードにダウングレードされます。バージョン 1 のすべてのネイバーがシャットダウンするかアップグレードされると、インターフェイスはバージョン 2 モードに戻ります。</p> <p>詳細については、「PIMv1 および PIMv2 の相互運用性」(P.46-12) を参照してください。</p>
ステップ 5 <code>ip pim {dense-mode sparse-mode sparse-dense-mode}</code>	<p>インターフェイスで PIM モードをイネーブルにします。</p> <p>デフォルトで、モードは設定されていません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • dense-mode : DM 動作をイネーブルにします。 • sparse-mode : SM 動作をイネーブルにします。SM を設定する場合は、RP も設定する必要があります。詳細については、「RP の設定」(P.46-26) を参照してください。 • sparse-dense-mode : グループが属するモードでインターフェイスが処理されます。DM-SM 設定を推奨します。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャストをディセーブルにするには、**no ip multicast-routing distributed** グローバル コンフィギュレーション コマンドを使用します。デフォルトの PIM バージョンに戻すには、**no ip pim version** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで PIM をディセーブルにするには、**no ip pim** インターフェイス コンフィギュレーション コマンドを使用します。

SSM の設定

ここでは、Source-Specific Multicast (SSM) の設定方法について説明します。ここに記載されている SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」の章を参照してください。この章に記載されている他のコマンドのマニュアルについては、コマンドリファレンス マスター インデックスを使用するか、オンラインで検索してください。

SSM 機能は IP マルチキャストの拡張版で、レシーバーが明示的に加入しているマルチキャスト送信元だけからのデータグラム トラフィックをレシーバーに転送します。SSM 用に設定されるマルチキャスト グループには、SSM 配信ツリーのみ（共有ツリーなし）が作成されます。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション（ブロードキャストアプリケーション）を最適なデータグラム デリバリティ モデルです。SSM は、音声およびビデオのブロードキャストアプリケーション環境を対象にしたシスコの IP マルチキャストソリューションのコア ネットワーキング テクノロジーです。スイッチ は、SSM の導入をサポートする次のコンポーネントをサポートします。

- Protocol Independent Multicast Source-Specific Mode (PIM-SSM)

PIM-SSM は SSM の導入をサポートするルーティング プロトコルであり、PIM Sparse Mode (PIM-SM; PIM 希薄モード) から派生しています。

- IGMP バージョン 3 (IGMPv3)

SSM と IGMPv3 を稼動するには、SSM が Cisco IOS ルータ、アプリケーションの稼動するホスト、およびアプリケーション自身でサポートされている必要があります。

SSM とインターネット標準マルチキャストとの違い

インターネットおよび多くの企業イントラネットの IP マルチキャスト インフラストラクチャは、PIM-SM プロトコルおよび Multicast Source Discovery Protocol (MSDP) に基づいています。これらのプロトコルには、Internet Standard Multicast (ISM) サービス モデルの制限があります。たとえば、ISM を使用する場合、ネットワークはネットワーク内でマルチキャスト トラフィックをアクティブに送信しているホストを把握している必要があります。

ISM サービスは、任意の送信元からレシーバー グループ（マルチキャスト ホスト グループ）への IP データグラムの配信です。マルチキャスト ホスト グループに対するデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と、IP 宛先アドレスであるマルチキャスト グループ アドレス G で構成されています。システムは、ホスト グループのメンバーになることでこのトラフィックを受信します。

ホスト グループのメンバシップに必要なのは、IGMP バージョン 1、2、または 3 を使用してホスト グループにシグナリングすることだけです。SSM では、データグラムの配信は (S, G) チャネルに基づいています。SSM および ISM のどちらでも、送信元になるためにシグナリングは必要ありません。ただし SSM の場合、レシーバーは、特定の送信元からのトラフィックを受信するには (S, G) チャネルに加入し、受信しないようにするには (S, G) チャネルから脱退する必要があります。つまりレシーバーは、加入先の (S, G) チャネルからのみトラフィックを受信できます。これに対し ISM の場合、受信トラフィックの送信元 IP アドレスを知る必要はありません。チャネル加入シグナリングに関する提案標準方式では、IGMP の INCLUDE モードメンバシップ レポートを使用しますが、これは IGMP バージョン 3 でのみサポートされます。

SSM の IP アドレスの範囲

SSM は、SSM デリバリティ モデルを IP マルチキャスト グループ アドレス範囲の既定サブセットに適用することで、ISM サービスと共存できます。Cisco IOS ソフトウェアでは、224.0.0.0 ~ 239.255.255.255 の IP マルチキャスト アドレス範囲に対して SSM を設定できます。SSM 範囲が定義されると、既存の IP マルチキャスト レシーバー アプリケーションがその SSM 範囲のアドレスを使用しようとしても、トラフィックをまったく受信しません（アプリケーションが明示的な [S, G] チャネル加入を使用するように変更されている場合を除きます）。

SSM の動作

PIM-SM に基づいて IP マルチキャスト サービスを実装しているネットワークでは、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なプロトコル (MSDP、自動 RP、Bootstrap Router (BSR; ブートストラップ ルータ) など) がすべて揃っていないネットワークでも、SSM を単独で導入できます。

PIM-SM がすでに設定されているネットワークに SSM を導入する場合、SSM がサポートされるのは最終ホップ ルータだけです。レシーバーに直接接続されていないルータは、SSM をサポートする必要がありません。一般に、最終ホップを除いたこれらのルータは、SSM 範囲で PIM-SM だけを実行する必要があります。アクセス コントロールを追加設定して SSM 範囲内で MSDP シグナリング、登録動作、または PIM-SM 共有ツリー動作が起こらないようにすることが必要になる場合があります。

SSM 範囲を設定し、SSM をイネーブルにするには、`ip pim ssm` グローバル コンフィギュレーション コマンドを使用します。この設定は、次のような影響があります。

- SSM 範囲内のグループについては、(S,G) チャネル加入は IGMPv3 の INCLUDE モード メンバシップ レポートを使用して受け入れられます。
- SSM 範囲内にあるアドレスの PIM 動作は、PIM-SM から派生したモードである PIM-SSM に切り替わります。このモードでは、PIM (S,G) Join および Prune メッセージだけがルータによって生成され、(S,G) Rendezvous Point Tree (RPT) および (*, G) RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは、無視または廃棄されます。着信 PIM 登録メッセージには、登録停止メッセージがただちに返されます。ルータが最終ホップ ルータである場合を除いて、PIM-SSM は PIM-SM と下位互換性があります。したがって、最終ホップ以外のルータは SSM グループに対し PIM-SM を実行できます (ルータが SSM をまだサポートしていない場合など)。
- SSM 範囲内の MSDP Source-Active (SA) メッセージは、受け入れ、生成、転送ができません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストがマルチキャスト グループの最終ホップ ルータにメンバシップを伝えます。ホストは、送信元を基準にしたフィルタリング機能を使用してグループ メンバシップを伝えることができます。具体的には、ホストは、グループに送信するすべての送信元のうち、特定送信元からのトラフィックの受信を希望しない (EXCLUDE モード) こと、またはそのグループに送信する特定送信元だけからのトラフィックの受信を希望する (INCLUDE モード) ことを伝えることができます。

IGMPv3 は ISM および SSM の両方と連動できます。ISM では、EXCLUDE および INCLUDE モード レポートの両方を使用できます。SSM では、INCLUDE モード レポートのみが最終ホップ ルータで受け入れられます。EXCLUDE モード レポートは無視されます。

設定時の注意事項

ここでは、SSM を設定する際の注意事項について説明します。

SSM 範囲の制約事項に該当するレガシー アプリケーション

SSM より古いネットワークの既存アプリケーションは、(S,G) チャネル加入をサポートするように変更しないかぎり、SSM 範囲内では動作しません。そのため、ネットワークで SSM をイネーブルにした場合、既存アプリケーションが SSM の指定範囲内のアドレスを使用していると問題が生じます。

アドレス管理の制約事項

SSM をレイヤ 2 スイッチング メカニズムで使用すると、アドレス管理がある程度は必要になります。CGMP、IGMP スヌーピング、または Router-Port Group Management Protocol (RGMP) は、グループ別フィルタリングだけをサポートし、(S,G) チャネル別フィルタリングをサポートしていません。スイッチド ネットワーク内の異なるレシーバーが、同じグループを共有している異なる (S,G) チャネルを要求した場合、レシーバーは既存メカニズムの恩恵を受けられません。代わりに、両方のレシーバーは全 (S,G) チャネルのトラフィックを受信し、入力時に不要なトラフィックをフィルタリングします。SSM は、多くの個別アプリケーションに対し SSM 範囲のグループ アドレスを再利用できるので、この状況はスイッチド ネットワークのトラフィック フィルタリング機能の低下につながります。この理由から、SSM 範囲からランダムな IP アドレスをアプリケーションに使用するようにして、異なるアプリケーション間で SSM 範囲内の単一アドレスが再利用される可能性を最小限にすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスは、SSM を使用する場合でも、TV (S,G) チャネルごとに異なるグループを使用するようにしてください。このようにすることで、レイヤ 2 スイッチを含むネットワークにおいて、同じアプリケーション サービス内の異なるチャネルを利用する複数のレシーバーでトラフィック エイリアシングが発生しないようにできます。

IGMP スヌーピングおよび CGMP の制限事項

IGMPv3 には新しいメンバシップ レポート メッセージが採用されており、このメッセージが従来の IGMP スヌーピング スイッチで正しく認識されない場合があります。

IGMP (特に CGMP) に関連するスイッチングの問題の詳細については、「[IGMP の概要](#)」(P.46-3) を参照してください。

ステート管理の制限事項

PIM-SSM では、インターフェイス上に適切な (S,G) 加入が存在している場合、最終ホップ ルータは (S,G) Join メッセージの定期的な送信を継続します。したがって、レシーバーが (S,G) 加入を送信している限り、レシーバーから送信元への Shortest Path Tree (SPT) ステートが維持されます。これは送信元が長期間 (あるいはまったく) トラフィックを送信しない場合も同様です。

PIM-SM は、この反対の動作になります。つまり、送信元がトラフィックの送信を続けていて、レシーバーがグループに加入している場合に限り、(S,G) ステートが維持されます。PIM-SM では、送信元が 3 分間を超えて送信を停止した場合、(S,G) ステートは削除され、送信元からのパケットが再び RPT を介して到着したあとに再確立されます。PIM-SSM には送信元がアクティブであることをレシーバーに通知するメカニズムが存在しないため、ネットワークはレシーバーがそのチャネルの受信を要求している限り、PIM-SSM の (S,G) ステートを維持する必要があります。

SSM の設定

SSM を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>ip pim ssm [default range access-list]</code>	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 2	<code>interface type number</code>	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim {sparse-mode sparse-dense-mode}</code>	インターフェイス上で PIM をイネーブルにします。sparse mode または sparse-dense mode のどちらかを使用する必要があります。

コマンド	目的
ステップ 4 <code>ip igmp version 3</code>	このインターフェイス上で IGMPv3 をイネーブルにします。IGMP のデフォルト バージョンはバージョン 2 に設定されています。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM のモニタリング

SSM をモニタするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
<code>show ip igmp groups detail</code>	IGMPv3 を介した (S,G) チャンネル加入を表示します。
<code>show ip mroute</code>	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートを受信したかどうかを表示します。

SSM マッピングの設定

SSM マッピング機能は、エンド システムでの SSM のサポートが管理上または技術的な理由で不可能であるか、または望ましくない場合に SSM の変換をサポートします。SSM マッピングを使用すると、IGMPv3 がサポートされないレガシー STB にビデオを配信したり、IGMPv3 ホスト スタックを使用しないアプリケーションで、SSM を活用できます

ここで説明する内容は次のとおりです。

- 「設定時の注意事項」 (P.46-19)
- 「SSM マッピングの概要」 (P.46-20)
- 「SSM マッピングの設定」 (P.46-22)
- 「SSM マッピングのモニタリング」 (P.46-24)

設定時の注意事項

SSM マッピングの設定時の注意事項を次に示します。

- SSM マッピングを設定する前に、IP マルチキャスト ルーティングをイネーブルにし、PIM-SM をイネーブルにして、SSM を設定します。IP マルチキャスト ルーティングおよび PIM-SM をイネーブルにする方法については、「マルチキャスト ルーティングのデフォルト設定」 (P.46-12) を参照してください。
- スタティック SSM マッピングを設定する前に、Access Control List (ACL; アクセス コントロール リスト) を設定して、送信元アドレスにマッピングするグループ範囲を定義しておく必要があります。ACL の設定方法については、第 35 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- SSM マッピングを設定し DNS lookup を使用して SSM マッピングを行う前に、稼働中の DNS サーバにレコードを追加できるようになっている必要があります。DNS サーバが稼働していない場合は、インストールする必要があります。

Cisco Network Registra (CNR; Cisco ネットワーク レジストラ) などの製品が使用できます。詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml>

SSM マッピングの制約事項を次に示します。

- SSM マッピング機能では、完全な SSM の利点のすべてが提供されるわけではありません。SSM マッピングでは、ホストのグループ加入を用いて、1 つまたは複数の送信元に関連付けられたアプリケーションとそのグループを結びつけるため、グループあたり 1 つのアプリケーションしかサポートできません。完全な SSM のアプリケーションでも、SSM マッピングに見られるような同じグループを共有できます。
- 完全な SSM の変換ソリューションとして SSM マッピングに全面的に依存している場合は、注意して最終ホップルータで IGMPv3 をイネーブルにしてください。SSM マッピングおよび IGMPv3 の両方をイネーブルにするときに、各ホストがすでに IGMPv3 をサポートしている場合（ただし SSM はサポートしていない）、ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、これらの IGMPv3 グループ レポートをサポートしていません。またルータは、送信元とこれらのレポートを正しく関連付けることができません。

SSM マッピングの概要

一般的な STB 構成の場合、各 TV チャンネルは、1 つの独立した IP マルチキャスト グループを使用し、TV チャンネルを送信する 1 つのアクティブ サーバ ホストを持っています。1 つのサーバで複数の TV チャンネルを送信できますが、各チャンネルは異なるグループに送信されます。このネットワーク環境では、特定グループに対する IGMPv1 または IGMPv2 メンバシップ レポートをルータが受信する場合、レポートはマルチキャスト グループに関連付けられた TV チャンネルの well-known TV サーバに宛てられます。

SSM マッピングが設定されている場合、特定のグループに対する IGMPv1 または IGMPv2 メンバシップ レポートをルータが受信すると、ルータはこのレポートをそのグループに関連付けられている well-known 送信元の 1 つまたは複数のチャンネル メンバシップに変換します。

ルータがグループに対する IGMPv1 または IGMPv2 メンバシップ レポートを受信すると、ルータは SSM マッピングを使用して、そのグループの 1 つまたは複数の送信元 IP アドレスを特定します。SSM マッピングは次に、メンバシップ レポートを IGMPv3 レポートとして変換し、IGMPv3 レポートを受信したものとして動作を続けます。ルータは次に、PIM Join を送信し、IGMPv1 または IGMPv2 メンバシップ レポートを受信し続ける限り、グループに加入され続けます。グループの SSM マッピングも同じ状態のままです。

SSM マッピングにより、最終ホップルータは、ルータ上のスタティックに設定されたテーブルまたは DNS サーバを使用して送信元アドレスを特定することができます。スタティックに設定されたテーブルまたは DNS マッピングの変更があると、ルータは加入グループに関連付けられた現在の送信元から脱退します。

SSM マッピングの追加情報については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

スタティック SSM マッピング

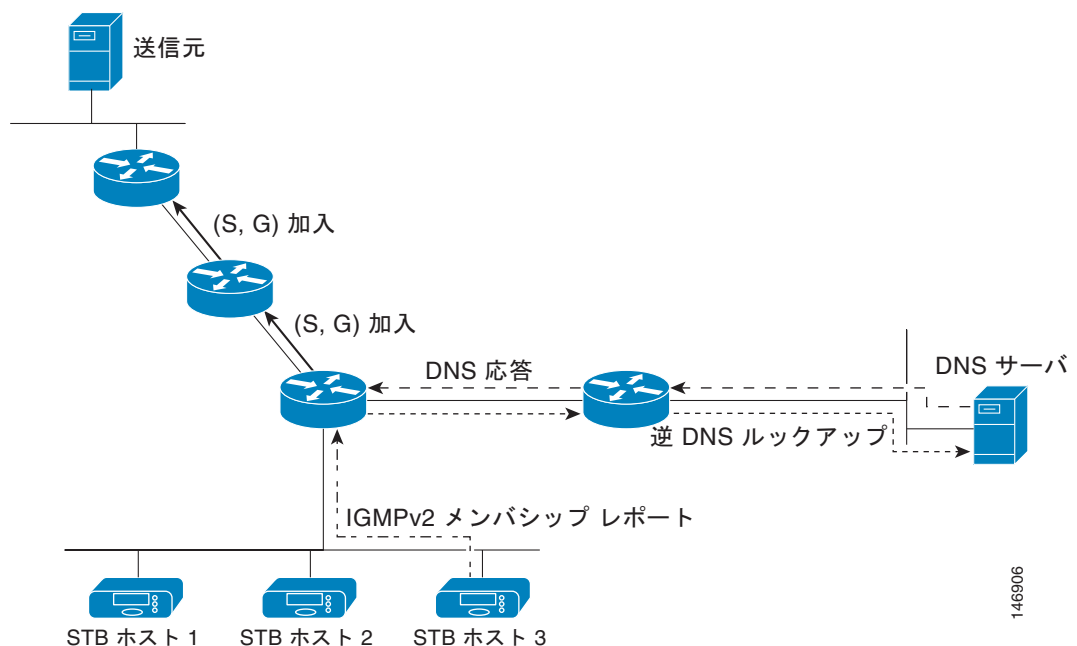
スタティック SSM マッピングを使用すると、グループに送信する送信元の特定にスタティック マップを使用するよう最終ホップルータを設定できます。スタティック SSM マッピングを使用するには、ACL を設定してグループ範囲を定義する必要があります。次に、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可したグループを送信元にマッピングします。

DNS が必要ない小規模ネットワークや、DNS マッピングをローカルで無効にする場合、スタティック SSM マッピングを設定できます。スタティック SSM マッピングが設定されると、DNS マッピングに優先します。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用すると、グループに送信する送信元の特定に逆 DNS ルックアップを実行するよう最終ホップ ルータを設定できます。DNS ベースの SSM マッピングが設定されている場合、ルータはグループ アドレスを含んだドメイン名を作成し、DNS の逆ルックアップを実行します。ルータは IP アドレス リソース レコードを検索し、それをグループに関連付けられた送信元アドレスとして使用します。SSM マッピングは、グループあたり最大 20 の送信元をサポートしています。ルータは、1 つのグループに設定されているすべての送信元に参加します (図 46-4 を参照)。

図 46-4 DNS ベースの SSM マッピング



SSM マッピングのメカニズムにより、最終ホップ ルータがグループの複数の送信元に参加できるため、TV ブロードキャストの送信元冗長性を提供できます。この状況では、最終ホップ ルータが SSM マッピングの使用により冗長性を提供して、同じ TV チャンルの 2 つのビデオ送信元に同時に加入します。ただし、最終ホップ ルータでビデオトラフィックが重複しないように、ビデオの送信元はサーバ側のスイッチオーバー メカニズムを使用する必要があります。つまり、一方のビデオ送信元をアクティブに、他方のバックアップ ビデオ送信元をパッシブにします。パッシブな送信元はアクティブな送信元の障害が検出されるのを待って、TV チャンルのビデオトラフィックを送信します。このように、サーバ側のスイッチオーバー メカニズムにより、1 台のサーバだけが TV チャンルのビデオトラフィックをアクティブに送信できるようになります。

G1、G2、G3、および G4 を含むグループの 1 つまたは複数の送信元アドレスを検索するには、DNS サーバ上に次の DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
      IN A source-address-2
      IN A source-address-n
```

DNS リソース レコードの設定に関する詳細については DNS サーバのマニュアルを参照してください。SSM マッピングの追加情報については次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」 (P.46-22) (必須)
- 「DNS ベースの SSM マッピングの設定」 (P.46-23) (必須)
- 「SSM マッピングを使用したスタティック トラフィック フォワーディングの設定」 (P.46-23) (任意)

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp ssm-map enable	設定した SSM 範囲内のグループの SSM マッピングをイネーブルにします。 (注) デフォルトでは、このコマンドは DNS ベースの SSM マッピングをイネーブルにします。
ステップ 3	no ip igmp ssm-map query dns	(任意) DNS ベースの SSM マッピングをディセーブルにします。 (注) スタティック SSM マッピングのみを使用する場合、DNS ベースの SSM マッピングをディセーブルにしてください。デフォルトでは、 ip igmp ssm-map グローバル コンフィギュレーション コマンドは DNS ベースの SSM マッピングをイネーブルにします。
ステップ 4	ip igmp ssm-map static access-list source-address	スタティック SSM マッピングを設定します。 <i>access-list</i> の ACL には、 <i>source-address</i> に入力した送信元 IP アドレスにマッピングされるグループを定義します。 (注) スタティック SSM マッピングの設定は追加できます。SSM マッピングの設定が追加されている場合、ルータが SSM 範囲内のグループの IGMPv1 または IGMPv2 メンバシップ レポートを受信すると、スイッチは設定された各 ip igmp ssm-map static コマンドを使用して、グループに関連付けられた送信元アドレスを特定します。スイッチはグループあたり 20 までの送信元を関連付けます。
ステップ 5	必要な場合は、ステップ 4 を繰り返してスタティック SSM マッピングの設定を追加します。	—
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定例を参照するには、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバゾーンを作成するか、既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用しているルータが他の目的にも DNS を使用している場合は、通常設定されている DNS サーバを使用するようにしてください。DNS ベースの SSM マッピングがルータ上で使用されている唯一の DNS の運用である場合は、空のルートゾーンを使用するか、自身を指定するルートゾーンを使用して擬似的な DNS セットアップを設定できます。

DNS ベースの SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip igmp ssm-map enable</code>	設定した SSM 範囲内のグループの SSM マッピングをイネーブルにします。
ステップ 3	<code>ip igmp ssm-map query dns</code>	(任意) DNS ベースの SSM マッピングをイネーブルにします。 デフォルトでは、 <code>ip igmp ssm-map</code> コマンドは DNS ベースの SSM マッピングをイネーブルにします。この <code>no</code> 形式のコマンドだけが実行コンフィギュレーションに保存されます。 (注) DNS ベースの SSM マッピングがディセーブルになっている場合に、DNS ベースの SSM マッピングを再度イネーブルにするためにこのコマンドを使用します。
ステップ 4	<code>ip domain multicast domain-prefix</code>	(任意) DNS ベースの SSM マッピングにスイッチが使用しているドメインプレフィクスを変更します。 デフォルトでは、スイッチは <code>ip-addr.arpa</code> ドメインプレフィクスを使用します。
ステップ 5	<code>ip name-server server-address1 [server-address2... server-address6]</code>	1 つまたは複数のネームサーバのアドレスを指定して、名前およびアドレスの解決に使用します。
ステップ 6	必要な場合は、ステップ 5 を繰り返して冗長性のための DNS サーバの設定を追加します。	—
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

SSM マッピングを使用したスタティック トラフィック フォワーディングの設定

特定のグループの SSM トラフィックをスタティックに転送するには、SSM マッピングによるスタティック トラフィック フォワーディングを使用します。

SSM マッピングを使用したスタティック トラフィック フォワーディングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface type number</code>	マルチキャスト グループのトラフィックを SSM マッピングを使用してスタティックに転送するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。 (注) SSM マッピングによるトラフィックのスタティック フォワーディングは、DNS ベースの SSM マッピングまたはスタティックに設定された SSM マッピングと連動します。
ステップ 3	<code>ip igmp static-group group-address source ssm-map</code>	インターフェイスからの (S,G) チャンネルをスタティックに転送するように SSM マッピングを設定します。 特定のグループの SSM トラフィックをスタティックに転送する場合に、このコマンドを使用します。DNS ベースの SSM マッピングは、チャンネルの送信元アドレスの特定に使用します。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングのモニタリング

SSM マッピングをモニタするには、表 46-3 に示す特権 EXEC コマンドを使用します。

表 46-3 SSM マッピングのモニタリング コマンド

コマンド	目的
<code>show ip igmp ssm-mapping</code>	SSM マッピングに関する情報を表示します。
<code>show ip igmp ssm-mapping group-address</code>	SSM マッピングが使用する、特定のグループの送信元を表示します。
<code>show ip igmp groups [group-name group-address interface-type interface-number] [detail]</code>	ルータに直接接続されているレシーバーで IGMP によって学習されたレシーバーを持ったマルチキャスト グループを表示します。
<code>show host</code>	デフォルトのドメイン名、名前検索サービスの方式、ネームサーバホストのリスト、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。
<code>debug ip igmp group-address</code>	送受信した IGMP パケットおよび IGMP ホスト関連のイベントを表示します。

SSM マッピングのモニタリング例を参照するには、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#wp1047772

PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。また、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類の PIM インターフェイスをサポートします。PIM パッシブ モードで設定されたルーテッド インターフェイスは、PIM コントロール トラフィックの通過または転送を行いません。IGMP トラフィックの通過または転送のみを行います。

PIM スタブ ルーティングの設定時の注意事項

インターフェイスで PIM スタブ ルーティングをイネーブルにするときは、次の注意事項に従ってください。

- PIM スタブ ルーティングを設定する前に、スタブ ルータおよび中央ルータの両方に IP マルチキャスト ルーティングを設定しておく必要があります。また、スタブ ルータのアップリンク インターフェイスに PIM モード (DM、SM、または DM-SM) も設定しておく必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間で中継トラフィックのルーティングを行いません。ユニキャスト (EIGRP) スタブ ルーティングではこの動作が適用されます。ユニキャスト スタブ ルーティングを設定して PIM スタブ ルータの動作を補助する必要があります。詳細については、「[EIGRP スタブ ルーティングの設定](#)」(P.38-45) を参照してください。
- 直接接続されるマルチキャスト (IGMP) 受信者と送信元のみが、レイヤ 2 アクセス ドメイン内に許可されます。PIM プロトコルは、アクセス ドメインではサポートされません。
- 冗長 PIM スタブ ルータ トポロジはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim passive</code>	インターフェイスに PIM スタブ 機能を設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip pim interface</code>	各インターフェイスでイネーブルになっている PIM スタブ を表示します。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、`no ip pim passive` インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています (`spare-dense-mode` がイネーブル)。PIM スタブ ルーティングは、[図 46-2](#) に示すように、VLAN 100 インターフェイスとギガビット イーサネット ポート 20 でイネーブルになっています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet3/0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet3/0/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet3/0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

各インターフェイスで PIM スタブがイネーブルになっていることを確認するには、**show ip pim interface** 特権 EXEC コマンドを使用してください。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2

100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

PIM スタブの設定およびステータスに関する情報を表示するには、次の特権 EXEC コマンドを使用します。

- **show ip pim interface** は、各インターフェイスでイネーブルになっている PIM スタブを表示します。
- **show ip igmp detail** は、特定のマルチキャスト送信グループに加入している対象クライアントを表示します。
- **show ip igmp mroute** は、マルチキャスト ストリームが送信元から対象クライアントに転送されていることを確認します。

RP の設定

インターフェイスが SM-DM で、グループを希薄グループとして扱う場合には、RP を設定する必要があります。ここに記載するいくつかの方法を使用できます。

- 「マルチキャスト グループへの RP の手動割り当て」(P.46-27)
- 「自動 RP の設定」(P.46-28) (PIMv1 から独立した、スタンドアロンのシスコ独自のプロトコル)
- 「PIMv2 BSR の設定」(P.46-33) (IETF 標準のトラッキング プロトコル)

動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。詳細については、「PIMv1 および PIMv2 の相互運用性」(P.46-12) および「自動 RP および BSR 設定時の注意事項」(P.46-13) を参照してください。

マルチキャスト グループへの RP の手動割り当て

ここでは、RP を手動で割り当てる方法について説明します。ダイナミック メカニズム（自動 RP や BSR など）を使用してグループの RP を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（代表ルータ）から受信して RP に転送される Register メッセージを通し、自身の存在をアナウンスします。マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「合流地点」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチは PIM DM 技術を使用し、グループを **dense**（稠密）として処理します。

RP のアドレスを手動で設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>ip pim rp-address ip-address [access-list-number] [override]</code>	<p>PIM RP のアドレスを設定します。</p> <p>デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ スイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。グループに RP が設定されていない場合、スイッチは PIM DM 技術を使用し、グループを dense（稠密）として処理します。</p> <p>1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。</p> <ul style="list-style-type: none"> • <code>ip-address</code> には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • (任意) <code>access-list-number</code> を指定する場合は、1 ~ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • (任意) <code>override</code> キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。

コマンド	目的
ステップ 3 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、RP が使用されるマルチキャスト グループのアドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RP アドレスを削除するには、`no ip pim rp-address ip-address [access-list-number] [override]` グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 225.2.2.2 の場合のみ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

自動 RP の設定

自動 RP は IP マルチキャストを使用し、グループ/RP マッピングを PIM ネットワーク内のすべてのシスコ ルータおよびマルチレイヤ スイッチに自動配信します。自動 RP には次の利点があります。

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ スイッチで矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

自動 RP を設定する場合は、次の注意事項に従ってください。

- PIM を SM または SM-DM に設定し、自動 RP を設定しない場合は、RP を手動で設定する必要があります（「マルチキャスト グループへの RP の手動割り当て」(P.46-27) を参照）。
- ルーテッド インターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッド インターフェイスが SM に設定されていて、`ip pim autorp listener` グローバル コンフィギュレーション コマンドを入力した場合は、自動 RP グループの手動 RP アドレスですべてのデバイスが設定されていない場合でも、自動 RP を使用できます。

ここでは、自動 RP を設定する方法について説明します。

- 「新規インターネットワークでの自動 RP の設定」(P.46-29) (任意)
- 「既存の SM クラウドへの自動 RP の追加」(P.46-29) (任意)
- 「問題のある RP への Join メッセージの送信禁止」(P.46-31) (任意)
- 「着信 RP アナウンスメント メッセージのフィルタリング」(P.46-31) (任意)

概要については、「自動 RP」(P.46-7) を参照してください。

新規インターネットワークでの自動 RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。「既存の SM クラウドへの自動 RP の追加」(P.46-29) に記載された手順に従ってください。ただし、PIM ルータをローカル グループの RP として設定する場合は、ステップ 3 を省略してください。

既存の SM クラウドへの自動 RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

既存の SM クラウドに自動 RP を導入するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 show running-config	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、 ip pim rp-address グローバル コンフィギュレーション コマンドによって設定済みです。 SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ (224.x.x.x やその他のグローバル グループなど) に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によってダイナミックに検出された RP は、スタティックに設定された RP よりも優先されます。ローカル グループ用に別の RP を使用することもできます。
ステップ 2 configure terminal	グローバル コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3 <code>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</code>	<p>別の PIM デバイスをローカル グループの候補 RP として設定します。</p> <ul style="list-style-type: none"> <code>interface-id</code> には、RP アドレスを識別するインターフェイス タイプ および番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 <code>scope ttl</code> には、ホップの TTL 値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。 <code>group-list access-list-number</code> には、1 ~ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 <code>interval seconds</code> には、アナウンスメント メッセージを送信する頻度を指定します。デフォルト値は 60 ミリ秒です。指定できる範囲は 1 ~ 16383 です。
ステップ 4 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 3 で指定したアクセス リスト番号を入力します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 5 <code>ip pim send-rp-discovery scope ttl</code>	<p>接続が中断される可能性がないスイッチを検索し、RP マッピング エージェントの役割を割り当てます。</p> <p><code>scope ttl</code> には、ホップの TTL 値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾 (グループ/RP 範囲の重なりなど) を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。</p>
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code> <code>show ip pim rp mapping</code> <code>show ip pim rp</code>	<p>設定を確認します。</p> <p>関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。</p> <p>ルーティング テーブルに保管されている情報を表示します。</p>
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定された PIM デバイスを解除するには、**no ip pim send-rp-announce interface-id** グローバル コンフィギュレーション コマンドを使用します。RP マッピング エージェントとして設定されたスイッチを解除するには、**no ip pim send-rp-discovery** グローバル コンフィギュレーション コマンドを使用します。

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセスリスト 5 には、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、あとでこの問題を解決できます。ルータまたはマルチレイヤ スイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。この手順は任意です。

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

着信 RP アナウンスメント メッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

着信 RP アナウンスメント メッセージをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip pim rp-announce-filter rp-list access-list-number group-list access-list-number	<p>着信 RP アナウンスメント メッセージをフィルタリングします。</p> <p>ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。</p> <p>rp-list access-list-number を指定する場合は、候補 RP アドレスのアクセスリストを設定します。アクセスリストが許可されている場合は、group-list access-list-number 変数で指定されたグループ範囲に対してアクセスリストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。</p> <p>複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピング エージェント間でフィルタを統一する必要があります。</p>

コマンド	目的
ステップ 3 access-list access-list-number {deny permit} source [source-wildcard]	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント (rp-list Access Control List (ACL; アクセス コントロール リスト)) がマッピング エージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト (グループリスト ACL) を作成します。 • <i>source</i> には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

着信 RP アナウンスメント メッセージに関するフィルタを削除するには、**no ip pim rp-announce-filter rp-list access-list-number [group-list access-list-number]** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

この例では、マッピング エージェントは 2 つのデバイス (172.16.5.1 および 172.16.2.1) からの候補 RP アナウンスのみを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ~ 239.255.255.255 であるマルチキャスト グループ宛のアナウンスメントのみを許可します。マッピング エージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ~ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

PIMv2 BSR の設定

ここでは、PIMv2 ネットワークでの BSR の設定方法について説明します。

- 「PIM ドメイン境界の定義」(P.46-33) (任意)
- 「IP マルチキャスト境界の定義」(P.46-34) (任意)
- 「候補 BSR の設定」(P.46-35) (任意)
- 「候補 RP の設定」(P.46-36) (任意)

概要については、「BSR」(P.46-7) を参照してください。

PIM ドメイン境界の定義

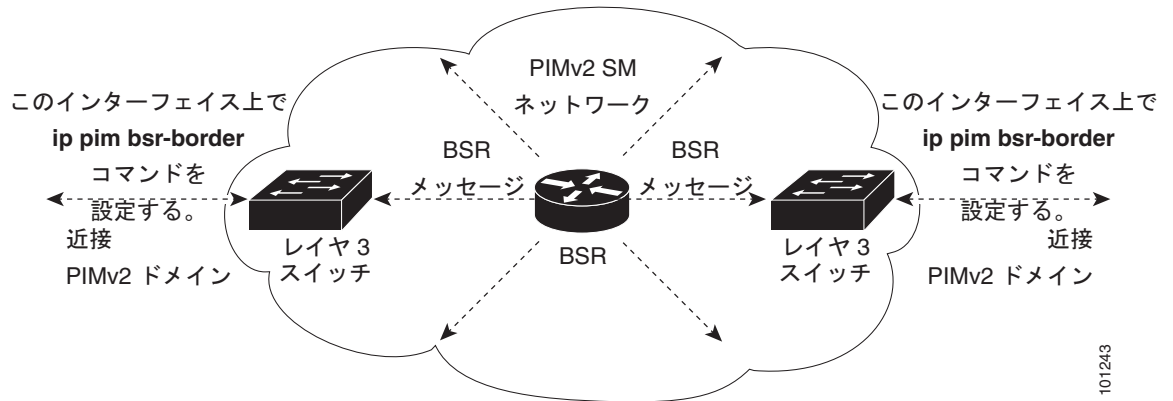
IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えてきました。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが共存し、間違ったドメイン内で RP が選択されたりすることがあります。

PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim bsr-border</code>	PIM ドメイン用の PIM プートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、スイッチは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます (図 46-5 を参照)。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM 境界を削除するには、`no ip pim bsr-border` インターフェイス コンフィギュレーション コマンドを使用します。

図 46-5 PIMv2 BSR メッセージの抑制



101243

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛の packets を拒否するアクセス リストを作成します。

マルチキャスト境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 access-list access-list-number deny source [source-wildcard]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <i>access-list-number</i> の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。 <i>source</i> には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 3 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 ip multicast boundary access-list-number	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show running-config	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。


```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1
```

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

スイッチを候補 BSR として設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim bsr-candidate interface-id hash-mask-length [priority]	候補 BSR となるようにスイッチを設定します。 <ul style="list-style-type: none"> <i>interface-id</i> には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となる、スイッチ上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポートチャンネル、VLAN などです。 <i>hash-mask-length</i> には、ハッシュ機能呼び出す前に、グループアドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットのみが使用されます。 (任意) <i>priority</i> を指定する場合は、0 ~ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

候補 BSR として設定されたデバイスを解除するには、**no ip pim bsr-candidate** グローバル コンフィギュレーション コマンドを使用します。

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
Switch(config-if)# ip pim bsr-candidate gigabitethernet0/2 30 10
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/2 30 10
```

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレススペース全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズメントを BSR に送信します。RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP のみが使用されているシスコ ルータおよびマルチレイヤ スイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダーのルータのみで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤ スイッチを RP として設定できます。

スイッチが自身を PIMv2 候補 RP として BSR にアドバタイズするよう設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip pim rp-candidate interface-id [group-list access-list-number]</code>	候補 RP となるようにスイッチを設定します。 <ul style="list-style-type: none"> • <i>interface-id</i> には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • (任意) <i>group-list access-list-number</i> には、1 ~ 99 の IP 標準アクセス リスト番号を入力します。<i>group-list</i> を指定しない場合は、スイッチがすべてのグループの候補 RP となります。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定されたデバイスを解除するには、`no ip pim rp-candidate interface-id` グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループプレフィクスが指定されます。この RP は、プレフィクスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

自動 RP および BSR の使用

ネットワーク上のルータがすべてシスコ デバイスである（他のベンダー製のルータが存在しない）場合には、BSR を設定する必要はありません。PIMv1 と PIMv2 が両方とも動作しているネットワークに、自動 RP を設定します。

シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 ルータまたはマルチレイヤ スイッチを、自動 RP マッピング エージェントと BSR の両方に設定してください。

BSR を 1 つまたは複数使用する必要がある場合は、次の推奨事項に従ってください。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。詳細については、「[自動 RP の設定](#)」(P.46-28) および「[候補 BSR の設定](#)」(P.46-35) を参照してください。
- グループプレフィクスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループプレフィクスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループプレフィクスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

グループ/RP マッピングの一貫性を確認するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>show ip pim rp [[group-name group-address] mapping]</code>	任意のシスコ デバイスに関して、使用可能な RP マッピングを表示します。 <ul style="list-style-type: none"> • (任意) <code>group-name</code> を指定する場合は、RP を表示するグループの名前を指定します。 • (任意) <code>group-address</code> を指定する場合は、RP を表示するグループのアドレスを指定します。 • (任意) シスコ デバイスによって認識されている（設定されているか、自動 RP によって取得されている）すべてのグループ/RP マッピングを表示するには、<code>mapping</code> キーワードを使用します。
ステップ 2	<code>show ip pim rp-hash group</code>	PIMv2 ルータまたはマルチレイヤ スイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 <code>group</code> には、RP 情報を表示するグループアドレスを入力します。

RP マッピング情報のモニタ

RP マッピング情報をモニタするには、特権 EXEC モードで次のコマンドを使用します。

- **show ip pim bsr** - 現在選択されている BSR の情報を表示します。
- **show ip pim rp-hash - group** 指定グループに選択されている RP を表示します。
- **show ip pim rp [group-name | group-address | mapping]** - スイッチが RP を取得する方法 (BSR 経由か、または自動 RP メカニズムによるか) を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題を解決するには、次の点を順にチェックします。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します (この場合は、登録停止に応答し、カプセル化が解除されたデータ パケットをレジスタから転送します)。

高度な PIM 機能の設定

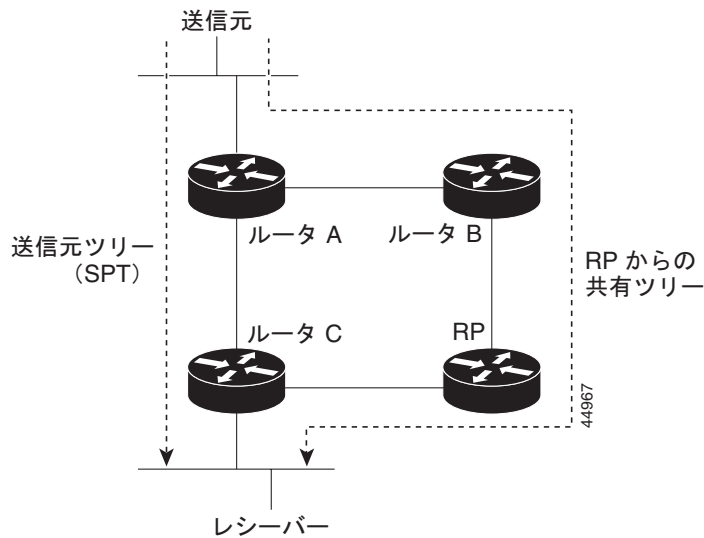
ここでは、高度なオプションの PIM 機能について説明します。

- 「[PIM 共有ツリーおよび送信元ツリーの概要](#)」 (P.46-38)
- 「[PIM SPT 使用の延期](#)」 (P.46-40) (任意)
- 「[PIM ルータクエリー メッセージ インターバルの変更](#)」 (P.46-41) (任意)

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。図 46-6 に、このタイプの共有配信ツリーを示します。送信側からのデータは、共有ツリーに加入しているグループ メンバーに配信するため、RP にアドバタイズされます。

図 46-6 共有ツリーおよび送信元ツリー (SPT)



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ (ダウンストリーム接続がないルータ) で使用できます。このタイプの配信ツリーは、**SPT** または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバーがグループに加入します。リーフ ルータ C は **Join** メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して **Register** メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて **Join** メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります (カプセル化されたデータ、およびネイティブ状態のデータ)。
5. データがネイティブ状態 (カプセル化されていない状態) で着信すると、RP は **Register 停止** メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が **Join** メッセージを送信元に送信するよう要求します。
7. (S,G) に関するデータを受信すると、ルータ C は送信元宛の **Prune** メッセージを共有ツリーの上方向に送信します。
8. RP は (S,G) の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けて **Prune** メッセージを送信します。

Join および **Prune** メッセージが送信元および RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。**Register** メッセージおよび **Register 停止** メッセージはホップバイホップで送信されません。これらのメッセージは、送信元に直接接続された代表ルータで送信され、グループの RP で受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。

共有ツリー上に存在するように、PIM デバイスを設定できます。詳細については、「[PIM SPT 使用の延期](#)」(P.46-40) を参照してください。

PIM SPT 使用の延期

最初のデータ パケットが最終ホップ ルータ (図 46-6 のルータ C) に着信すると、共有ツリーから送信元ツリーへと変更されます。この変更が生じるのは、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドによってタイミングが制御されるためです。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度 (キロビット/秒) 以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー (SPT) を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、Prune メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト (標準アクセス リスト) を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

マルチキャスト ルーティングが送信元ツリーから SPT に切り替わる上限値となるトラフィック速度のしきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成します。 <ul style="list-style-type: none"> <i>access-list-number</i> の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>source</i> には、しきい値が適用されるマルチキャスト グループを指定します。 (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 3	ip pim spt-threshold {kbps infinity} [group-list access-list-number]	SPT に移行する上限値となるしきい値を指定します。 <ul style="list-style-type: none"> <i>kbps</i> を指定する場合は、トラフィック速度をキロビット/秒で指定します。デフォルトは 0 kbps です。 (注) 有効範囲は 0 ~ 4294967 ですが、スイッチ ハードウェアの制限により、0 kbps 以外は無効です。 <ul style="list-style-type: none"> infinity を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 (任意) group-list access-list-number には、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 4	end	特権 EXEC モードに戻ります。

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

デフォルト設定に戻すには、`no ip pim spt-threshold {kpbs | infinity}` グローバル コンフィギュレーション コマンドを使用します。

PIM ルータクエリー メッセージ インターバルの変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント (サブネット) の DR になるデバイスを判別するため、PIM ルータクエリーメッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合のみ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM Register メッセージを送信し、送信元からのマルチキャストトラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

ルータクエリー メッセージ インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim query-interval seconds</code>	スイッチが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルト値は 30 秒です。指定できる範囲は 1 ~ 65535 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no ip pim query-interval [seconds]` インターフェイス コンフィギュレーション コマンドを使用します。

オプションの IGMP 機能の設定

ここでは、次の設定情報について説明します。

- 「IGMP のデフォルト設定」 (P.46-42)
- 「グループのメンバーとしてのスイッチの設定」 (P.46-42) (任意)
- 「IP マルチキャスト グループへのアクセスの制御」 (P.46-43) (任意)
- 「IGMP バージョンの変更」 (P.46-44) (任意)
- 「IGMP ホストクエリー メッセージ インターバルの変更」 (P.46-45) (任意)

- 「IGMPv2 の IGMP クエリー タイムアウトの変更」(P.46-46) (任意)
- 「IGMPv2 の最大クエリー応答時間の変更」(P.46-46) (任意)
- 「スタティックに接続されたメンバーとしてのスイッチの設定」(P.46-47) (任意)

IGMP のデフォルト設定

表 46-4 に、IGMP のデフォルト設定を示します。

表 46-4 IGMP のデフォルト設定

機能	デフォルト設定
マルチキャスト グループのメンバーとしてのマルチレイヤ スイッチ	グループ メンバシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP バージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
スタティックに接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ スイッチがマルチキャスト グループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレッシングされた ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。



注意

この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

スイッチがグループのメンバーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 <code>ip igmp join-group group-address</code>	マルチキャスト グループに加入するスイッチを設定します。 デフォルトで、グループのメンバシップは定義されていません。 <code>group-address</code> には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。

コマンド	目的
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show ip igmp interface [interface-id]	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

グループ内のメンバシップを取り消すには、**no ip igmp join-group group-address** インターフェイス コンフィギュレーション コマンドを使用します。

次に、マルチキャスト グループ 255.2.2.2 へのスイッチの加入を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、スイッチは、マルチキャスト グループにアドレッシングされたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

インターフェイスで許可されるマルチキャスト グループをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 ip igmp access-group access-list-number	インターフェイスで処理されるサブネット上のホストが加入できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 <i>access-list-number</i> には、IP 標準アドレス アクセス リスト番号を指定します。指定できる範囲は 1 ~ 99 です。
ステップ 4 exit	グローバル コンフィギュレーション モードに戻ります。

コマンド	目的
ステップ 5 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセスリストを作成します。 <ul style="list-style-type: none"> <code>access-list-number</code> には、ステップ 3 で作成したアクセスリストを指定します。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、サブネット上のホストが加入できるマルチキャストグループを指定します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

インターフェイスでグループをディセーブルにするには、`no ip igmp access-group` インターフェイスコンフィギュレーション コマンドを使用します。

次に、ポートに接続されたホストが、グループ 255.2.2.2 にのみ加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

IGMP バージョンを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

コマンド	目的
ステップ 3 ip igmp version {1 2}	スイッチで使用する IGMP バージョンを指定します。 (注) バージョン 1 に変更すると、 ip igmp query-interval または ip igmp query-max-response-time インターフェイス コンフィギュレーション コマンドを設定することができません。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show ip igmp interface [interface-id]	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no ip igmp version** インターフェイス コンフィギュレーション コマンドを使用します。

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは、IGMP ホストクエリー メッセージを定期的送信し、接続されたネットワーク上にあるマルチキャスト グループを検出します。これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ (224.0.0.1) に送信されます。スイッチはホストクエリー メッセージを送信し、ネットワーク上に存在するメンバシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、Prune メッセージが送信元のアップストリーム方向へ送信されます。

スイッチは LAN (サブネット) 用の PIM DR を選択します。DR は、IP アドレスが最大である、IGMPv2 用のルータまたはマルチレイヤ スイッチです。IGMPv1 の場合、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。

ホストクエリー インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 ip igmp query-interval seconds	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。指定できる範囲は 1 ~ 65535 です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show ip igmp interface [interface-id]	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-interval** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、スイッチがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。デフォルトでは、スイッチは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリーインターバルの 2 倍の時間だけ待機します。この時間を経過しても、スイッチがクエリーを受信しない場合は、スイッチがクエリアになります。

クエリー インターバルを設定するには、**show ip igmp interface interface-id** 特権 EXEC コマンドを入力します。

IGMP クエリー タイムアウトを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp querier-timeout seconds	IGMP クエリー タイムアウトを指定します。 デフォルトは 60 秒です (クエリー インターバルの 2 倍)。指定できる範囲は 60 ~ 300 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp querier-timeout** インターフェイス コンフィギュレーション コマンドを使用します。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。スイッチは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバーが存在しないことを短時間で検出します。値を小さくすると、グループのプルーンング速度が向上します。

最大クエリー応答時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp query-max-response-time seconds	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルト値は 10 秒です。指定できる範囲は 1 ~ 25 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを使用します。

スタティックに接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しなかったり、ホストで IGMP を使用してグループ メンバシップを報告することができないにもかかわらず、そのネットワーク セグメントにマルチキャスト トラフィックを送り込むことが必要な場合もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込む方法は次のとおりです。

- **ip igmp join-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはマルチキャスト パケットの転送だけでなく、受信も行います。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。
- **ip igmp static-group** インターフェイス コンフィギュレーション コマンドを使用します。この方法の場合、スイッチはパケットそのものを受信せず、転送のみを実行します。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに *L* (ローカル) フラグが付かないことから明らかなように、スイッチ自体はメンバーではありません。

スタティックに接続されたグループのメンバーになるように (および高速スイッチングできるように) スイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp static-group group-address	スイッチをスタティックに接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

グループのメンバーとして設定されたスイッチを解除するには、**no ip igmp static-group group-address** インターフェイス コンフィギュレーション コマンドを使用します。

オプションのマルチキャスト ルーティング機能の設定

ここでは、オプションのマルチキャスト ルーティング機能の設定方法について説明します。

- レイヤ 2 接続および MBONE マルチメディア会議セッションに関する機能と設定：
 - 「CGMP サーバ サポート機能のイネーブル化」 (P.46-48) (任意)
 - 「sdr リスナー サポート機能の設定」 (P.46-49) (任意)
- 帯域幅の利用率を制御する機能：
 - 「IP マルチキャスト境界の設定」 (P.46-50) (任意)

- VPN Routing/Forwarding Table (VRF; VPN ルーティング/転送テーブル) にマルチキャストを設定する手順：
 - 「マルチキャスト VRF の設定」(P.38-85)

CGMP サーバ サポート機能のイネーブル化

スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれているデバイス用の CGMP サーバとして機能します。CGMP はレイヤ 2 Catalyst スイッチに接続されたシスコ ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。CGMP が必要となるのは、レイヤ 2 スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループアドレスにアドレッシングされます。

スイッチ インターフェイスで CGMP サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	レイヤ 2 Catalyst スイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip cgmp [proxy]</code>	<p>インターフェイス上で CGMP をイネーブルにします。</p> <p>デフォルトでは、CGMP はすべてのインターフェイス上でディセーブルです。</p> <p>CGMP をイネーブルにすると、CGMP Join メッセージが送信されます。レイヤ 2 Catalyst スイッチに接続されたレイヤ 3 インターフェイスでのみ、CGMP をイネーブルにします。</p> <p>(任意) proxy キーワードを入力すると、CGMP プロキシ機能がイネーブルになります。プロキシ ルータは、CGMP 非対応ルータの MAC アドレス、およびグループ アドレス 0000.0000.0000 が格納された CGMP Join メッセージを送信し、CGMP 非対応ルータが存在することをアドバタイズします。</p> <p>(注) CGMP プロキシを実行するには、スイッチを IGMP クエリアに設定する必要があります。ip cgmp proxy コマンドを設定する場合は、ネットワークで動作中の IGMP のバージョンに応じて、IP アドレスが最大または最小のスイッチが IGMP クエリアになるように IP アドレスを手動で操作する必要があります。IGMP バージョン 2 クエリアは、インターフェイスの最小の IP アドレスに基づいて選択されます。IGMP バージョン 1 クエリアは、インターフェイスで使用されるマルチキャスト ルーティング プロトコルに基づいて選択されます。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 7		レイヤ 2 Catalyst スイッチ CGMP クライアントの設定を確認します。詳細については、製品に付属のマニュアルを参照してください。

インターフェイス上で CGMP をディセーブルにするには、**no ip cgmp** インターフェイス コンフィギュレーション コマンドを使用します。

複数のシスコ CGMP 対応デバイスがスイッチド ネットワークに接続されていて、**ip cgmp proxy** コマンドを使用する必要がある場合は、すべてのデバイスを同じ CGMP オプションを使用して設定し、他社製のルータよりも IGMP クエリアを優先させてください。

sdr リスナー サポート機能の設定

MBONE は、相互接続された、IP マルチキャスト トラフィックの転送が可能なインターネット ルータ およびホストの小さなサブセットです。その他のマルチメディア コンテンツも、通常は MBONE を通じてブロードキャストされます。マルチメディア セッションに加入する前に、このセッションで使用されているマルチメディア グループ アドレス、ポート、セッションがアクティブになる時期、およびワークステーションで必要となるアプリケーションの種類（音声、ビデオなど）を把握する必要があります。この情報は、MBONE Session Directory バージョン 2 (sdr) ツールによって提供されます。このフリーウェア アプリケーションは WWW 上の複数のサイト (<http://www.video.ja.net/mice/index.html> など) からダウンロードできます。

SDR は、Session Announcement Protocol (SAP) マルチキャスト パケット用の既知のマルチキャスト グループ アドレスおよびポートを、SAP クライアントからリスニングするマルチキャスト アプリケーションです (SAP クライアントは、会議セッションをアナウンスします)。これらの SAP パケットには、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループ アドレス、メディア形式、担当者、およびアドバタイズされたマルチメディア セッションに関するその他の情報が格納されます。SAP パケットの情報は、SDR Session Announcement ウィンドウに表示されます。

sdr リスナー サポート機能のイネーブル化

デフォルトでは、スイッチでセッション ディレクトリのアドバタイズメントはリスニングされません。

スイッチがインターフェイスのデフォルトのセッション ディレクトリ グループ (224.2.127.254) に加入し、セッション ディレクトリ アドバタイズメントをリスニングできるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	sdr に対してイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip sdr listen	sdr リスナー サポート機能をイネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

sdr サポート機能をディセーブルにするには、**no ip sdr listen** インターフェイス コンフィギュレーション コマンドを使用します。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュから削除されません。送信元が SAP 情報のアドバタイズを停止した場合に、古いアドバタイズメントが無駄に保持されないようにするため、エントリがアクティブである期間を制限できます。

sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip sdr cache-timeout minutes</code>	sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限します。 デフォルトでは、エントリはキャッシュから削除されません。 <code>minutes</code> に指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no ip sdr cache-timeout` グローバル コンフィギュレーション コマンドを使用します。キャッシュ全体を削除するには、`clear ip sdr` 特権 EXEC コマンドを使用します。

セッション ディレクトリ キャッシュを表示するには、`show ip sdr` 特権 EXEC コマンドを使用します。

IP マルチキャスト境界の設定

管理の有効範囲付き境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理の有効範囲付きアドレス」と呼ばれる特殊なマルチキャスト アドレス範囲が境界のメカニズムとして使用されます。管理の有効範囲付き境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りすることができません。この結果、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

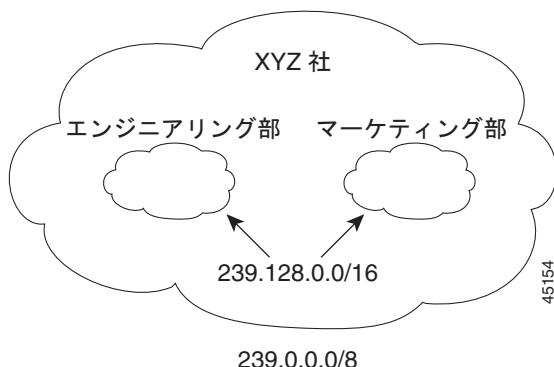


(注)

マルチキャスト境界および TTL しきい値は、マルチキャスト ドメインの有効範囲を制御しますが、TTL しきい値はこのスイッチでサポートされていません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 46-7 に、XYZ 社が自社ネットワーク周辺にあるすべてのルーテッド インターフェイス上で、管理の有効範囲付き境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ~ 239.255.255.255 の範囲のマルチキャスト トラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理の有効範囲付き境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ~ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ったり、外部に出ることができません。

図 46-7 管理の有効範囲付き境界



マルチキャストグループアドレスに対して、ルーテッドインターフェイス上に管理の有効範囲付き境界を定義できます。影響を受けるアドレス範囲は、標準アクセスリストによって定義されます。この境界が定義されている場合、マルチキャストデータパケットはいずれの方向であっても境界を通過することができません。この境界を使用すると、異なる管理ドメイン内で同じマルチキャストグループアドレスを再利用できます。

IANA は、マルチキャストアドレス範囲 239.0.0.0 ~ 239.255.255.255 を管理の有効範囲付きアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意的であると見なされます。

管理の有効範囲付き境界を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> の範囲は 1 ~ 99 です。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 3 interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 ip multicast boundary access-list-number	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show running-config	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

境界を削除するには、**no ip multicast boundary** インターフェイス コンフィギュレーション コマンドを使用します。

次に、すべての管理の有効範囲付きアドレスに対して境界を設定する例を示します。

```
Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1
```

基本的な DVMRP 相互運用性機能の設定

ここでは、次の設定情報について説明します。

- 「DVMRP 相互運用性」(P.46-52) (任意)
- 「DVMRP トンネルの設定」(P.46-54) (任意)
- 「DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ」(P.46-56) (任意)
- 「mrinfo 要求への応答」(P.46-57) (任意)

高度な DVMRP 機能の詳細については、「高度な DVMRP 相互運用性機能の設定」(P.46-57) を参照してください。

DVMRP 相互運用性

PIM を使用するシスコのマルチキャスト ルータおよびマルチレイヤ スイッチは、DVMRP を使用する他社製のマルチキャスト ルータと相互運用させることができます。

PIM デバイスは、DVMRP プロブ メッセージをリスニングし、接続されているネットワーク上にある DVMRP マルチキャスト ルータを動的に検出します。DVMRP ネイバーが検出された場合、PIM デバイスは、PIM ドメイン内の到達可能なユニキャスト送信元をアドバタイズする DVMRP レポート メッセージを定期的に送信します。デフォルトでは、直接接続されたサブネットおよびネットワークがアドバタイズされます。デバイスは DVMRP ルータによって転送されたマルチキャスト パケットを転送し、次にマルチキャスト パケットを DVMRP ルータに転送します。

DVMRP ルート レポート内でアドバタイズされるユニキャスト ルート数を制限するには、MBONE に接続された PIM ルーテッド インターフェイスにアクセス リストを設定できます。この設定を行わないと、ユニキャスト ルーティング テーブル内のすべてのルートがアドバタイズされます。



(注)

マルチキャスト ルーティングされるプロトコルは、DVMRP のパブリックドメイン実装バージョンです。シスコ ルータおよびマルチレイヤ スイッチを DVMRP ルータに直接接続する場合、または MBONE トンネルを通して DVMRP ルータと相互運用する場合は、マルチキャスト ルーティングのバージョン 3.8 を使用する必要があります (バージョン 3.8 には、DVMRP の非ブルーニングバージョンが実装されています)。Cisco IOS ソフトウェアによって作成される DVMRP アドバタイズメントを使用すると、マルチキャスト ルーティングされた古いバージョンのプロトコルによってルーティング テーブルやネイバーのルーティング テーブルが破壊されることもあります。

アドバタイズされる送信元、および使用されるメトリックを設定する場合は、**ip dvmrp metric** インターフェイス コンフィギュレーション コマンドを設定します。特定のユニキャスト ルーティング プロセスによって取得されたすべての送信元を、DVMRP にアドバタイズするように指示することもできます。

DVMRP ルートレポート メッセージが送信される時に、アドバタイズされる送信元と使用されるメトリックを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <code>access-list-number</code> の範囲は 1 ~ 99 です。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 3 <code>interface interface-id</code>	MBONE に接続されている、マルチキャスト ルーティングが可能なインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 <code>ip dvmrp metric metric [list access-list-number] [[protocol process-id] [dvmrp]]</code>	DVMRP レポートの一連の宛先に関連付けられるメトリックを設定します。 <ul style="list-style-type: none"> <code>metric</code> の範囲は 0 ~ 32 です。値が 0 の場合、ルートはアドバタイズされません。値 32 は無限大 (到達不能) を意味します。 (任意) <code>list access-list-number</code> に、ステップ 2 で作成されたアクセス リスト番号を入力します。この指定をすると、このアクセス リストに一致するマルチキャストの宛先だけが設定済みの基準に従ってレポートされます。 (任意) <code>protocol process-id</code> を指定する場合は、<code>eigrp</code>、<code>igrp</code>、<code>ospf</code>、<code>rip</code>、<code>static</code>、または <code>dvmrp</code> などのユニキャスト ルーティング プロトコルの名前、およびルーティング プロトコルのプロセス ID 番号を入力します。これらが指定されている場合は、指定されたルーティング プロトコルによって取得されたルートだけが、DVMRP レポート メッセージに格納されてアドバタイズされます。 (任意) <code>dvmrp</code> キーワードが指定されている場合は、設定された <code>metric</code> を使用して DVMRP ルーティング テーブルのルートをアドバタイズしたり、フィルタリングできます。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

メトリックまたはルート マップをディセーブルにするには、`no ip dvmrp metric metric [list access-list-number] [[protocol process-id] | [dvmrp]]` または `no ip dvmrp metric metric route-map map-name` インターフェイス コンフィギュレーション コマンドを使用します。

より詳細な方法で上記コマンドと同じ結果を得るには、アクセスリストの代わりに、ルートマップ (**ip dvmrp metric metric route-map map-name** インターフェイス コンフィギュレーション コマンド) を使用します。ユニキャスト ルートが DVMRP に入る前に、ルートマップ条件にユニキャスト ルートを適用します。

次に、PIM デバイスおよび DVMRP ルータが同じネットワーク セグメント上にある場合に、DVMRP 相互運用性を設定する例を示します。次の例では、アクセス リスト 1 はネットワーク (198.92.35.0、198.92.36.0、198.92.37.0、131.108.0.0、および 150.136.0.0) を DVMRP ルータにアドバタイズします。アクセス リスト 2 は他のすべてのネットワークのアドバタイズを禁止します (**ip dvmrp metric 0** インターフェイス コンフィギュレーション コマンド)。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.255.255
Switch(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP トンネルの設定

ソフトウェアは、MBONE への DVMRP トンネルをサポートします。一方の端で DVMRP が動作しているルータまたはマルチレイヤ スイッチには、DVMRP トンネルを設定できます。これにより、トンネルを通してマルチキャスト パケットが送受信されます。この方法で、パス上の一部のルータでマルチキャスト ルーティングがサポートされていない場合に、PIM ドメインを DVMRP ルータに接続できます。2 つのルータ間で DVMRP トンネルを設定することはできません。

シスコ ルータまたはマルチレイヤ スイッチがトンネルを通して DVMRP を実行している場合は、DVMRP レポート メッセージ内の送信元が、実際のネットワークと同様にアドバタイズされます。また、受信された DVMRP レポート メッセージはキャッシュに格納され、RPF 計算にも使用されます。この動作により、トンネルを通して受信されたマルチキャスト パケットの転送が可能になります。

次の場合は、DVMRP トンネルを設定するときに、IP アドレスをトンネルに割り当てる必要があります。

- トンネルを通して IP パケットを送信する場合
- DVMRP サマライズを実行するようにソフトウェアを設定する場合

トンネルとサブネットのネットワーク番号が異なる場合、サブネットはトンネルを通してアドバタイズされません。この場合は、ネットワーク番号のみがトンネルを通してアドバタイズされます。

DVMRP トンネルを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 access-list access-list-number {deny permit} source [source-wildcard]	<p>標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> の範囲は 1 ~ 99 です。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 3 interface tunnel number	トンネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4 tunnel source ip-address	トンネル インターフェイスの送信元アドレスを指定します。スイッチのインターフェイスの IP アドレスを入力します。
ステップ 5 tunnel destination ip-address	トンネル インターフェイスの宛先アドレスを指定します。マルチキャスト ルーティングされたルータの IP アドレスを入力します。
ステップ 6 tunnel mode dvmrp	DVMRP へのトンネルに対してカプセル化モードを設定します。
ステップ 7 ip address address mask または ip unnumbered type number	<p>インターフェイスに IP アドレスを割り当てます。</p> <p>または</p> <p>インターフェイスを非番号として設定します。</p>
ステップ 8 ip pim [dense-mode sparse-mode]	インターフェイスに PIM モードを設定します。
ステップ 9 ip dvmrp accept-filter access-list-number [distance] neighbor-list access-list-number	<p>着信 DVMRP レポートに対して許可フィルタを設定します。</p> <p>デフォルトでは、距離が 0 のすべての宛先レポートが許可されます。したがって、すべてのネイバーからのレポートが許可されます。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で作成したアクセス リスト番号を指定します。アクセス リストに一致するすべての送信元は、距離とともに DVMRP ルーティング テーブルに格納されます。 • (任意) <i>distance</i> を指定する場合は、宛先への管理上の距離を入力します。デフォルトでは、DVMRP ルートへの管理上の距離は 0 で、ユニキャスト ルーティング テーブル ルートよりも優先されます。ユニキャスト ルーティングによるパス (マルチキャスト ルーティング プロトコルとして PIM を使用) と DVMRP を使用するパスという、送信元への 2 つのパスがある場合に PIM パスを使用するときは、DVMRP ルートの管理上の距離を増加させます。指定できる範囲は 1 ~ 255 です。 • neighbor-list access-list-number には、ステップ 2 で作成したネイバー リストの番号を入力します。DVMRP レポートは、リスト内のネイバーでのみ許可されます。

	コマンド	目的
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show running-config	設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタをディセーブルにするには、**no ip dvmrp accept-filter access-list-number [distance] neighbor-list access-list-number** インターフェイス コンフィギュレーション コマンドを使用します。

次に、DVMRP トンネルを設定する例を示します。この設定では、シスコ スイッチ上のトンネルの IP アドレスに、*unnumbered* が割り当てられます。これにより、トンネルにはポート 1 と同じ IP アドレスが設定されます。これにより、トンネルにはポート 1 と同じ IP アドレスが設定されます。トンネルのエンドポイント送信元 IP アドレスは 172.16.2.1 です。トンネルの接続先であるリモート DVMRP ルータのトンネルのエンドポイント アドレスは 192.168.1.10 です。トンネルを通して送信されるパケットは、外部 IP ヘッダー内にカプセル化されます。シスコ スイッチは、198.92.37.0 から 198.92.37.255 への距離が 100 である着信 DVMRP レポートを受信するように設定されます。

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet1/0/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/0/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ

使用しているスイッチがマルチキャスト ルーティング バージョン 3.6 のデバイスと近接している場合は、ネットワーク 0.0.0.0 (デフォルト ルート) を DVMRP ネイバーにアドバタイズするように、ソフトウェアを設定できます。DVMRP デフォルト ルートでは、具体的なルートと一致しないマルチキャスト送信元の RPF 情報が計算されます。

DVMRP のデフォルト ルートを MBONE にアドバタイズしないでください。

インターフェイスの DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

コマンド	目的
ステップ 3 <code>ip dvmrp default-information {originate only}</code>	DVMRP ネイバーへのネットワーク 0.0.0.0 をアドバタイズします。 このコマンドは、スイッチがマルチキャスト ルーティング バージョン 3.6 のデバイスと近接している場合のみ使用します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • originate - 0.0.0.0 以外の具体的なルートもアドバタイズできるように指定します。 • only - 0.0.0.0 以外の DVMRP ルートはアドバタイズされません。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ルートのアドバタイズメントを禁止するには、**no ip dvmrp default-information** インターフェイス コンフィギュレーション コマンドを使用します。

mrinfo 要求への応答

ソフトウェアは、マルチキャスト ルーティングされたシステム、シスコ ルータ、およびマルチレイヤ スイッチによって送信された **mrinfo** 要求に応答します。ソフトウェアはネイバーに関する情報を、DVMRP トンネルおよびすべてのルーテッド インターフェイスを通して戻します。この情報にはメトリック (常に 1 に設定)、設定された TTL しきい値、インターフェイスのステータス、および各種フラグが含まれます。次の例のように、**mrinfo** 特権 EXEC コマンドを使用し、ルータまたはスイッチ自体をクエリーすることもできます。

```
Switch# mrinfo
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

高度な DVMRP 相互運用性機能の設定

シスコ ルータおよびマルチレイヤ スイッチは PIM を実行し、マルチキャスト パケットをレシーバーに転送したり、送信側から受信したりします。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。PIM はこの情報を使用しますが、シスコ ルータおよびマルチレイヤ スイッチでは、マルチキャスト パケットを転送するために DVMRP を実行しません。

ここでは、次の設定情報について説明します。

- 「[DVMRP ユニキャスト ルーティングのイネーブル化](#) (P.46-58) (任意)
- 「[DVMRP の非ブルーニング ネイバーの拒否](#) (P.46-59) (任意)
- 「[ルート交換の制御](#) (P.46-61) (任意)

基本的な DVMRP 機能の詳細については、「基本的な DVMRP 相互運用性機能の設定」(P.46-52) を参照してください。

DVMRP ユニキャスト ルーティングのイネーブル化

マルチキャスト ルーティングおよびユニキャスト ルーティングには個別のトポロジが必要となるため、PIM はマルチキャスト トポロジに従って、ループのない配信ツリーを構築する必要があります。シスコ ルータ、マルチレイヤ スイッチ、およびマルチキャスト ルーティング ベースのデバイスは、DVMRP ユニキャスト ルーティングを使用して、DVMRP ユニキャスト ルートを交換します。PIM はこれらのルートにリバースパスを転送します。

シスコ デバイスは DVMRP マルチキャスト ルーティングを相互に実行しませんが、DVMRP ルートを交換します。DVMRP ルートは、ユニキャスト トポロジと異なるマルチキャスト トポロジを提供します。このため、マルチキャスト トポロジを通して PIM を実行し、この結果 MBONE トポロジを通しての PIM SM が可能になります。

DVMRP ユニキャスト ルーティングがイネーブルの場合、ルータまたはスイッチは、DVMRP ルーティング テーブル内の DVMRP レポート メッセージで取得されたルートをキャッシュに格納します。PIM が動作中の場合、これらのルートはユニキャスト ルーティング テーブル内のルートよりも優先されます。したがって、MBONE トポロジがユニキャスト トポロジと異なる場合、PIM による MBONE トポロジが可能となります。

DVMRP ユニキャスト ルーティングは、すべてのインターフェイスで実行できます。DVMRP トンネルの場合は、DVMRP マルチキャスト ルーティングが使用されます。この機能を使用しても、シスコ ルータおよびマルチレイヤ スイッチ間で DVMRP マルチキャスト ルーティングはイネーブルになりません。ただし、DVMRP 対応マルチキャスト ルータがある場合は、シスコ デバイスで PIM/DVMRP マルチキャスト ルーティングを実行できます。

DVMRP ユニキャスト ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

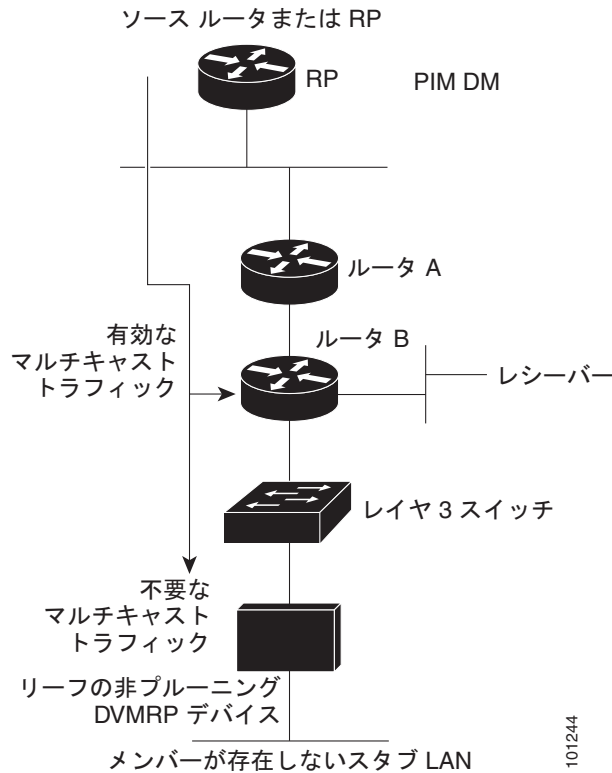
	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip dvmrp unicast-routing	DVMRP ユニキャスト ルーティングをイネーブルにします (DVMRP ルートを送受信します)。この機能は、デフォルトではディセーブルに設定されています。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip dvmrp unicast-routing** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP の非プルーニング ネイバーの拒否

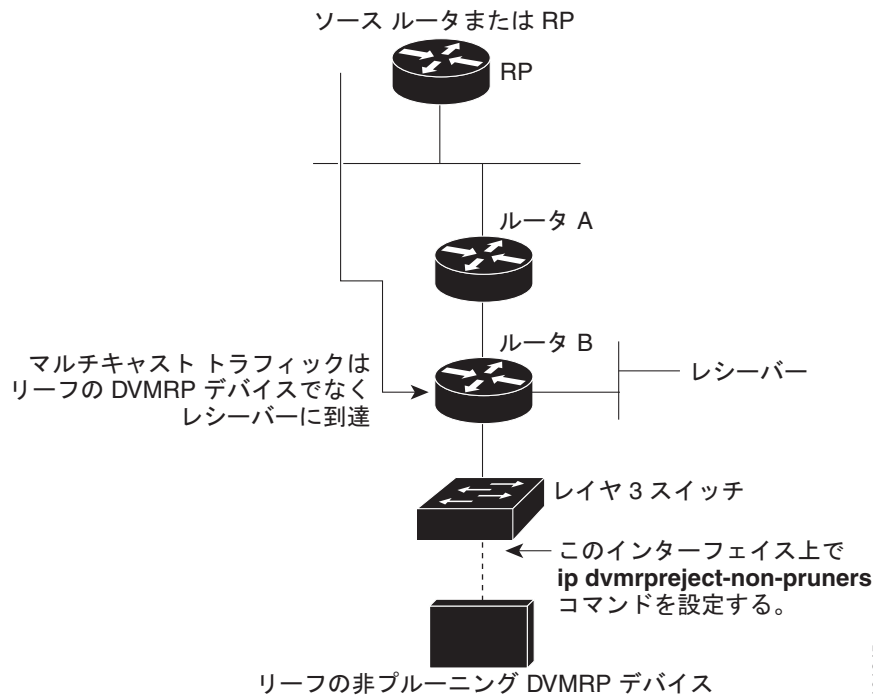
デフォルトでは、DVMRP 機能に関係なく、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の他社製のデバイスでは、プルーニング機能を持たない古いバージョンの DVMRP が動作するため、常時転送パケットが受信されて帯域幅が消費されます。図 46-8 にこの事例を示します。

図 46-8 リーフの非プルーニング DVMRP ネイバー



DVMRP ネイバーで DVMRP プルーニングまたは接合がサポートされていない場合、スイッチとこのネイバーとのピアリング（通信）を禁止できます。これを行うには、非プルーニング デバイスに接続されたインターフェイスで **ip dvmrp reject-non-pruners** インターフェイス コンフィギュレーション コマンドを使用し、スイッチ（リーフの非プルーニング DVMRP デバイスのネイバー）を設定します（図 46-9 を参照）。この場合、プルーニング対応フラグが設定されていない DVMRP プローブまたはレポート メッセージをスイッチが受信すると、Syslog メッセージがロギングされ、メッセージが廃棄されます。

図 46-9 ルータが非ブルーニング DVMRP ネイバーを拒否する例



ip dvmrp reject-non-pruners インターフェイス コンフィギュレーション コマンドを使用すると、ネイバーとのピアリングのみが禁止されます。拒否されていない非ブルーニング ルータが（レシーバー候補のダウンストリーム方向に）2 ホップ以上離れている場合、非ブルーニング DVMRP ネットワークが存在する場合があります。

非ブルーニング DVMRP ネイバーとのピアリングを禁止するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	非ブルーニング DVMRP ネイバーに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 ip dvmrp reject-non-pruners	非ブルーニング DVMRP ネイバーとのピアリングを禁止します。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

この機能をディセーブルにするには、**no ip dvmrp reject-non-pruners** インターフェイス コンフィギュレーション コマンドを使用します。

ルート交換の制御

ここでは、DVMRP ルートに関するシスコ デバイスのアドバタイズメントを調整する方法について説明します。

- 「アドバタイズされる DVMRP ルート数の制限」(P.46-61) (任意)
- 「DVMRP ルートしきい値の変更」(P.46-61) (任意)
- 「DVMRP サマリー アドレスの設定」(P.46-62) (任意)
- 「DVMRP 自動サマライズのディセーブル化」(P.46-64) (任意)
- 「DVMRP ルートへのメトリック オフセットの追加」(P.46-64) (任意)

アドバタイズされる DVMRP ルート数の制限

デフォルトでは、DVMRP を実行するためにイネーブル化されたインターフェイス (つまり、DVMRP トンネル、DVMRP ネイバーが検出されたインターフェイス、または `ip dvmrp unicast-routing` インターフェイス コンフィギュレーション コマンドを実行するように設定されたインターフェイス) を通して、7000 の DVMRP ルートのみがアドバタイズされます。

DVMRP ルートの制限を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip dvmrp route-limit count</code>	DVMRP に対してイネーブル化されたインターフェイスを通してアドバタイズされる DVMRP 数を変更します。 このコマンドを使用すると、 <code>ip dvmrp metric</code> インターフェイス コンフィギュレーション コマンドの設定ミスによって大量のルートが MBONE に入るのを防ぐことができます。 デフォルトでは、7000 のルートがアドバタイズされます。指定できる範囲は 0 ~ 4294967295 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート数が制限されないように設定するには、`no ip dvmrp route-limit` グローバル コンフィギュレーション コマンドを使用します。

DVMRP ルートしきい値の変更

デフォルトでは、1 つのインターフェイスにつき、1 分間に 10000 の DVMRP ルートを受信できます。この速度を超えると、ルート サージが発生した可能性を警告する Syslog メッセージが発行されます。通常この警告は、デバイスの設定ミスにより大量のルートが MBONE に入った場合、迅速な検出を行うために使用されます。

警告送信の基準となるルート数のしきい値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dvmrp routehog-notification <i>route-count</i>	Syslog メッセージの送信基準となるルート数を設定します。 デフォルト値は 10000 ルートで、指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

動作中のルート数を表示するには、**show ip igmp interface** 特権 EXEC コマンドを使用します。このルート数を超えると、***** ALERT ***** が表示行に表示されます。

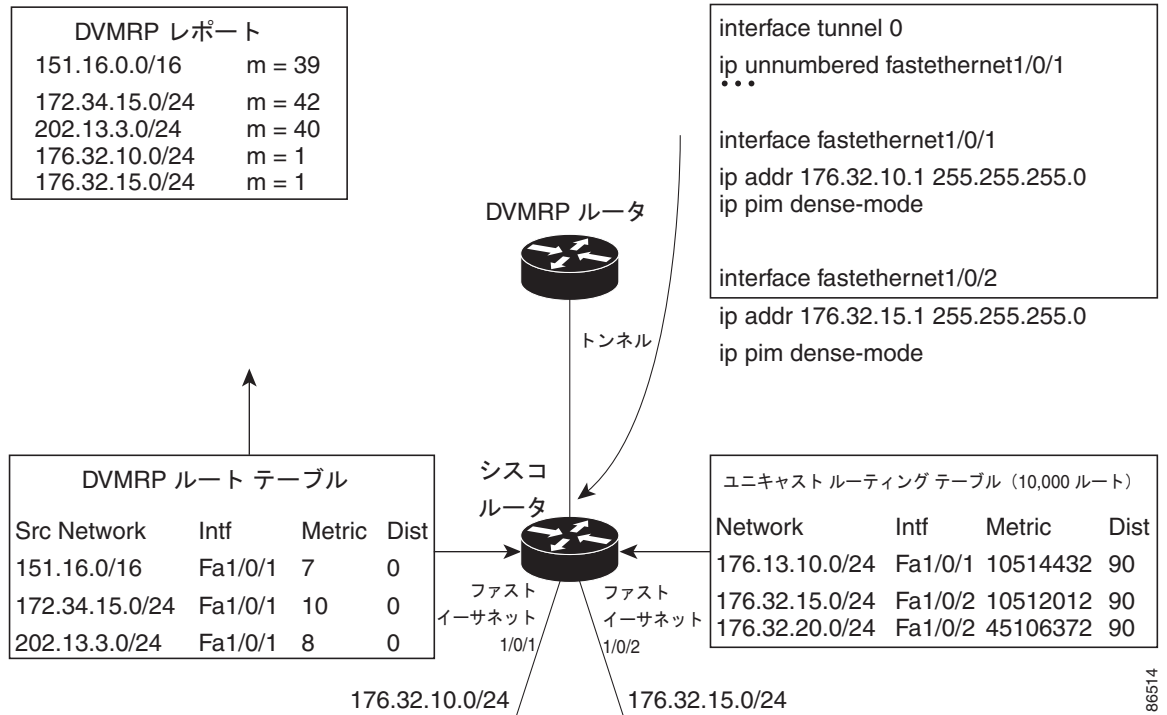
DVMRP サマリー アドレスの設定

デフォルトでは、シスコ デバイスは、ユニキャスト ルーティング テーブル内の接続されたユニキャスト ルートのみ（つまり、ルータに直接接続されたサブネットへのルートのみ）を DVMRP ルートレポート メッセージに格納してアドバタイズします。これらのルートは、通常の DVMRP のクラス指定されたルート サマライズによって処理されます。このプロセスは、アドバタイズされているルートとアドバタイズ中に経由するインターフェイスが、クラス指定された同じネットワーク内にあるかどうかに応じて異なります。

図 46-10 に、デフォルトの動作例を示します。この例では、シスコ ルータによって送信される DVMRP レポートに、DVMRP メトリックに 32 を追加してポイズンリバースされた、DVMRP ルータから受信した 3 つの元のルートが記述されています。これらのルートのあとに、ユニキャスト ルーティング テーブルから取得した、直接接続されている 2 つのネットワーク（176.32.10.0/24 および 176.32.15.0/24）にアドバタイズメントされる 2 つのルートが記述されています。DVMRP トンネルはファスト イーサネット ポート 1 と同じ IP アドレスを共有し、直接接続された 2 つのサブネットと同じクラス B ネットワークに分類されるため、これらのルートに対してクラス指定サマライズは実行されません。その結果、DVMRP ルータは、直接接続されたサブネットへ向かうこれらの 2 つのルートのみをポイズンリバースします。また、これらの 2 つのイーサネット セグメント上の送信元によって送信されたマルチキャスト トラフィックに対しては、RPF のみを適切に実行します。これら 2 つのイーサネット セグメント上にはない、シスコ ルータ背後のネットワーク内の他のマルチキャスト送信元では、DVMRP ルータに関する RPF チェックは適切に行われず、廃棄されます。

サマリー アドレス (**ip dvmrp summary-address address mask** インターフェイス コンフィギュレーション コマンドのアドレスおよびマスクのペアで指定) の範囲内にあるルートの代わりに、サマリー アドレスをアドバタイズするようにシスコ ルータを設定できます。ユニキャスト ルーティング テーブルにサマリー アドレス範囲内のルートが 1 つまたは複数格納されている場合は、サマリー アドレスが DVMRP ルート レポートに格納されて送信されます。それ以外の場合、サマリー アドレスはアドバタイズされません。図 46-10 では、シスコ ルータ トンネル インターフェイスに **ip dvmrp summary-address** コマンドを設定します。その結果、シスコ ルータは、ユニキャスト ルーティング テーブルのネットワーク 176.32.0.0/16 に、サマライズされた単一のクラス B アドバタイズメントを送信します。

図 46-10 接続されたユニキャスト ルートにのみアドバタイズ (デフォルト) する例



デフォルトのクラス指定サマライズが要求を満たさない場合に、DVMRP ルートのサマライズをカスタマイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。



(注)

設定されたサマリー アドレスをアドバタイズする前に、ユニキャスト ルーティング テーブルに具体的なルートを 1 つまたは複数設定する必要があります。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション コマンドを入力します。
ステップ 3 ip dvmrp summary-address address mask [metric value]	DVMRP サマリー アドレスを指定します。 <ul style="list-style-type: none"> summary-address address mask には、サマリー IP アドレス、および具体的なルートの代わりにアドバタイズされるマスクを指定します。 (任意) metric value を指定する場合は、サマリーアドレスとともにアドバタイズされるメトリックを指定します。デフォルト値は 1 です。指定できる範囲は 1 ~ 32 です。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

サマリー アドレスを削除するには、**no ip dvmrp summary-address address mask [metric value]** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP 自動サマライズのディセーブル化

ソフトウェアでは、デフォルトで一部のレベルの DVMRP サマライズが自動実行されます。サマリーだけでなくすべてのルートをアドバタイズする場合は、この機能をディセーブルにします。特別な場合には、すべてのサブネット情報が格納された近接する DVMRP ルータを使用し、DVMRP ネットワーク内のマルチキャストトラフィックの流れを詳細に制御できます。この例としては、PIM ネットワークが DVMRP クラウドに複数のポイントで接続されているとき、具体的な（サマライズされていない）ルートが DVMRP ネットワークに送信され、PIM クラウド内の各サブネットへ向かうさらに適切なパスがアドバタイズされる場合があります。

ip dvmrp summary-address インターフェイス コンフィギュレーション コマンドを設定し、**no ip dvmrp auto-summary** を設定しなかった場合は、カスタムと自動サマリーの両方が得られます。

DVMRP 自動サマリーをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no ip dvmrp auto-summary	DVMRP 自動サマライズをディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

自動サマライズを再びイネーブルにするには、**ip dvmrp auto-summary** インターフェイス コンフィギュレーション コマンドを使用します。

DVMRP ルートへのメトリック オフセットの追加

デフォルトでは、着信 DVMRP レポートに格納されてアドバタイズされた DVMRP ルートのメトリック（ホップ数）は、スイッチによって 1 だけ増加されます。特定のルートの優先度を上下させる場合は、メトリックを変更できます。

たとえば、マルチレイヤ スイッチ A からルートが取得され、より大きなメトリックを持つ同じルートがマルチレイヤ スイッチ B から取得されたとします。スイッチ B を経由するパスの方が高速であるため、このパスを使用する場合は、スイッチ A によって取得されたルートにメトリック オフセットを適用し、スイッチ B によって取得されたメトリックよりもメトリックを大きくできます。この結果、スイッチ B を経由するパスを選択できます。

デフォルトのメトリックを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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

コマンド	目的
ステップ 3 <code>ip dvmrp metric-offset [in out] increment</code>	<p>着信レポートに格納されてアドバタイズされる DVMRP ルートに追加されるメトリックを変更します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • (任意) in - 増分値が着信 DVMRP レポートに追加され、<code>mrinfo</code> 応答内で報告されるように指定します。 • (任意) out - 増分値が、DVMRP ルーティング テーブルのルートに対する発信 DVMRP レポートに追加されるように指定します。 <p>in と out のどちらも指定しない場合は、in がデフォルトになります。</p> <p><code>increment</code> には、レポート メッセージに格納されてアドバタイズされる DVMRP ルータのメトリックの増分値を指定します。指定できる範囲は 1 ~ 31 です。</p> <p><code>ip dvmrp metric-offset</code> コマンドがインターフェイス上で設定されていない場合、着信ルートのデフォルトの増分値は 1 です。発信ルートのデフォルト値は 0 です。</p>
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip dvmrp metric-offset` インターフェイス コンフィギュレーション コマンドを使用します。

IP マルチキャスト ルーティングのモニタおよびメンテナンス

ここでは、IP マルチキャスト ルーティングのモニタ方法およびメンテナンス方法について説明します。

- 「キャッシュ、テーブル、およびデータベースのクリア」(P.46-65)
- 「システムおよびネットワーク統計情報の表示」(P.46-66)
- 「IP マルチキャスト ルーティングのモニタ」(P.46-67)

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

表 46-5 に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 46-5 キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
<code>clear ip cgmp</code>	Catalyst スイッチによってキャッシュに格納されたすべてのグループ エントリをクリアします。
<code>clear ip dvmrp route {* route}</code>	DVMRP ルーティング テーブルからルートを削除します。
<code>clear ip igmp group [group-name group-address interface]</code>	IGMP キャッシュのエントリを削除します。
<code>clear ip mroute {* group [source]}</code>	IP マルチキャスト ルーティング テーブルのエントリを削除します。
<code>clear ip pim auto-rp rp-address</code>	自動 RP キャッシュをクリアします。
<code>clear ip sdr [group-address "session-name"]</code>	Session Directory Protocol バージョン 2 キャッシュ (sdr キャッシュ エントリ) を削除します。

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。



(注)

このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、デバイスのパケットが経由するネットワーク内のパスを検出することもできます。

表 46-6 に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 46-6 システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
<code>ping [group-name group-address]</code>	マルチキャスト グループ アドレスに ICMP エコー要求を送信します。
<code>show ip dvmrp route [ip-address]</code>	DVMRP ルーティング テーブルのエントリを表示します。
<code>show ip igmp groups [group-name group-address type number]</code>	スイッチに直接接続されている、IGMP によって取得されたマルチキャスト グループを表示します。
<code>show ip igmp interface [type number]</code>	インターフェイスのマルチキャスト関連情報を表示します。
<code>show ip mcache [group [source]]</code>	IP 高速スイッチング キャッシュの内容を表示します。
<code>show ip mpacket [source-address name] [group-address name] [detail]</code>	回覧用キャッシュヘッダー バッファの内容を表示します。
<code>show ip mroute [group-name group-address] [source] [summary] [count] [active kbps]</code>	IP マルチキャスト ルーティング テーブルの内容を表示します。

表 46-6 システムおよびネットワーク統計情報を表示するコマンド (続き)

コマンド	目的
<code>show ip pim interface [type number] [count] [detail]</code>	PIM 用に設定されたインターフェイスの情報を表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip pim neighbor [type number]</code>	スイッチによって検出された PIM ネイバーのリストを示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip pim rp [group-name group-address]</code>	SM マルチキャスト グループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
<code>show ip rpf {source-address name}</code>	スイッチの RPF の実行方法 (ユニキャスト ルーティング テーブル、DVMRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれか) を表示します。
<code>show ip sdr [group "session-name" detail]</code>	Session Directory Protocol バージョン 2 のキャッシュを表示します。

IP マルチキャスト ルーティングのモニタ

表 46-7 に示す特権 EXEC コマンドを使用すると、IP マルチキャスト ルータ、パケット、パスをモニタできます。

表 46-7 IP マルチキャスト ルーティングをモニタするためのコマンド

コマンド	目的
<code>mrinfo [hostname address] [source-address interface]</code>	マルチキャスト ルータまたはマルチレイヤ スイッチとピアリングする近接マルチキャスト デバイスに関して、マルチキャスト ルータまたはマルチレイヤ スイッチをクエリーします。
<code>mstat source [destination] [group]</code>	IP マルチキャスト パケット速度および損失情報を表示します。
<code>mtrace source [destination] [group]</code>	指定されたグループのマルチキャスト配信ツリーに対して、送信元から宛先ブランチへのパスをトレースします。



CHAPTER 47

MSDP の設定

この章では、Catalyst 3750 スイッチに Multicast Source Discovery Protocol (MSDP) を設定する方法について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode (PIM-SM) ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol (MBGP) がサポートされていないため、MSDP は完全にサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

この機能を使用するには、スタック マスター上で IP サービス イメージが稼動している必要があります。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』Release 12.2 を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- 「MSDP の概要」 (P.47-1)
- 「MSDP の設定」 (P.47-3)
- 「MSDP のモニタおよびメンテナンス」 (P.47-18)

MSDP の概要

MSDP を使用すると、さまざまなドメイン内のすべての Rendezvous Point (RP; ランデブー ポイント) に、グループのマルチキャスト送信元を通知できます。各 PIM-SM ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は Transmission Control Protocol (TCP) を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。交換されるのは、主にマルチキャスト グループを送信する送信元のリストです。RP 間の TCP 接続は、基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャストデータは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメイン RP で発信する必要があります。

MSDP のドメイン間動作は、Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) または MBGP に大きく依存します。ドメイン内の RP (インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP) で、MSDP を実行してください。

MSDP の動作

図 47-1 に、2 つの MSDP ピア間での MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。MSDP が設定されている場合は、次のシーケンスが発生します。

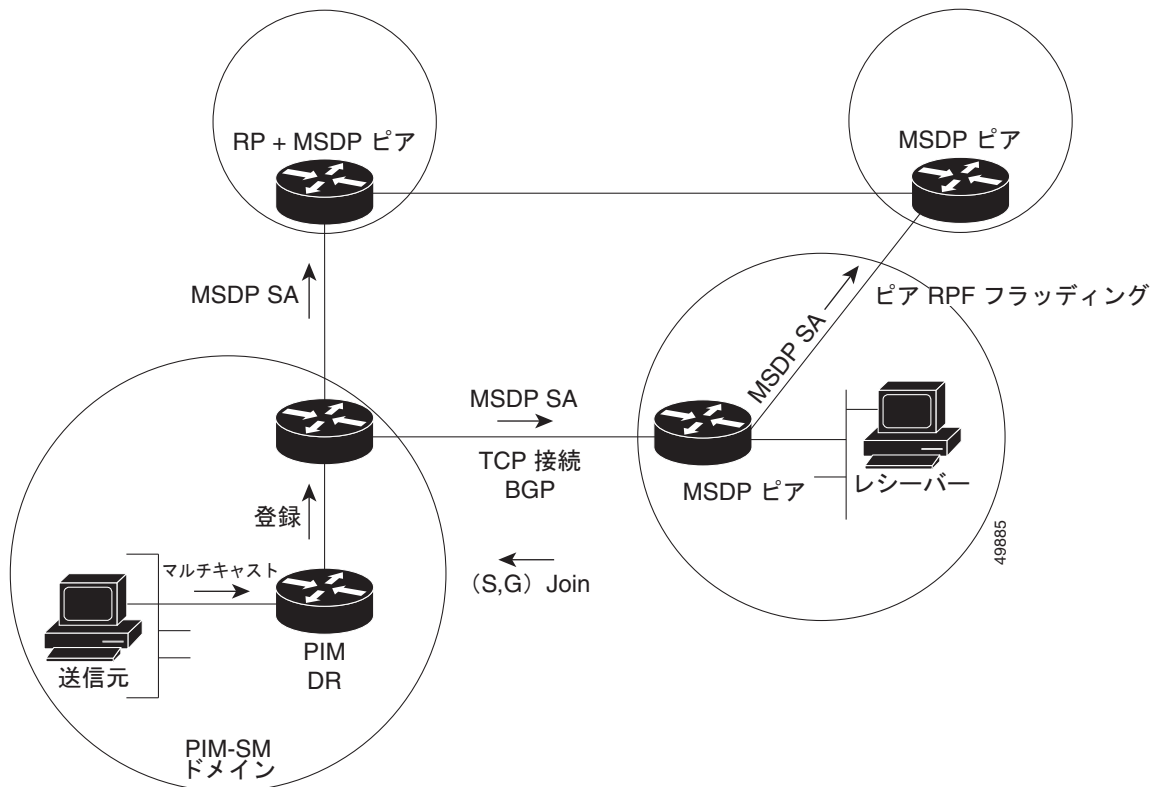
送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ (代表ルータまたは RP) によって RP に PIM Register メッセージが送信されます。RP は Register メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active (SA) メッセージもすべての MSDP ピアに転送されます。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID (RP アドレスとして使用されるインターフェイスの IP アドレス) が設定されている場合は、SA メッセージによってこれらが識別されます。

各 MSDP ピアは SA メッセージを発信元の RP から受信および転送し、ピア Reverse-Path Forwarding (RPF) フラッドングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは RPF ピアと呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、「[デフォルトの MSDP ピアの設定](#)」(P.47-4) を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージを廃棄します。それ以外の場合、その MSDP ピアはすべての MSDP ピアにメッセージを転送します。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの Join 要求を持ち、空でない発信インターフェイス リストに (*,G) エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に (S,G) Join メッセージが送信されます。(S,G) join メッセージが送信元の DR に到達すると、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されます。この結果、マルチキャストトラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバーへと送信できます。

図 47-1 RP ピア間で動作する MSDP



MSDP の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカルメンバーはローカルツリーに加わります。共有ツリーへの Join メッセージをドメイン外へ送信する必要はありません。
- PIM SM ドメインは独自の RP のみを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにすることができ、セキュリティが高まります。
- レシーバーのみが配置されているドメインは、グループメンバーシップをグローバルにアダプタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャストルーティングテーブルステートが不要になり、コストが削減されます。

MSDP の設定

ここでは、次の設定情報について説明します。

- 「MSDP のデフォルト設定」(P.47-4)
- 「デフォルトの MSDP ピアの設定」(P.47-4) (必須)
- 「SA ステートのキャッシング」(P.47-6) (任意)

- 「MSDP ピアからの送信元情報の要求」(P.47-8) (任意)
- 「スイッチから発信される送信元情報の制御」(P.47-8) (任意)
- 「スイッチで転送される送信元情報の制御」(P.47-11) (任意)
- 「スイッチで受信される送信元情報の制御」(P.47-13) (任意)
- 「MSDP メッシュ グループの設定」(P.47-15) (任意)
- 「MSDP ピアのシャットダウン」(P.47-16) (任意)
- 「MSDP への境界 PIM DM 領域の追加」(P.47-16) (任意)
- 「RP アドレス以外の発信元アドレスの設定」(P.47-17) (任意)

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

デフォルトの MSDP ピアの設定

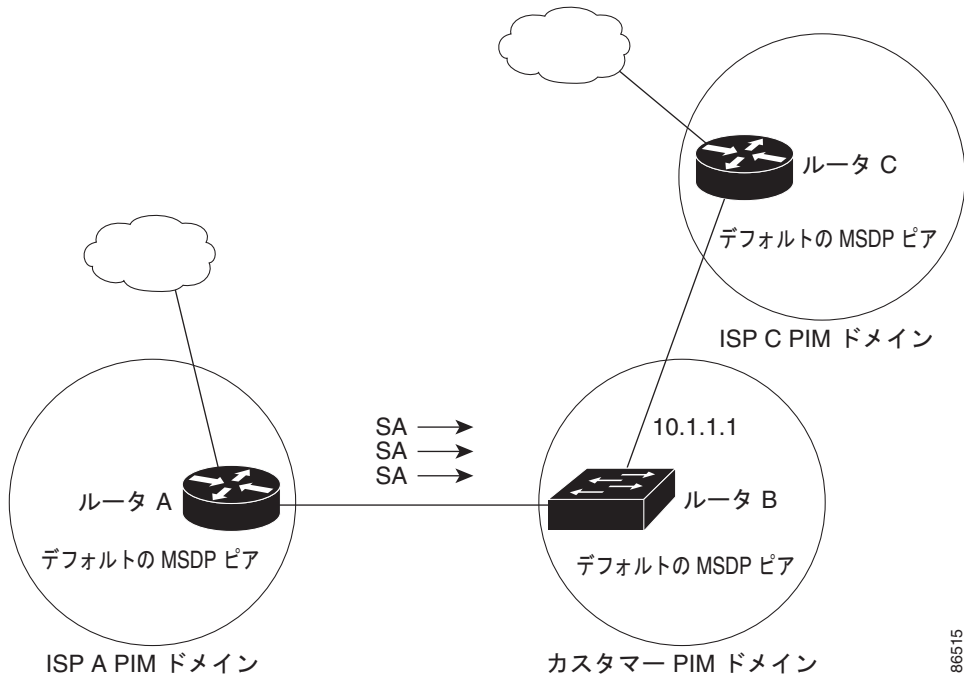
このソフトウェア リリースでは、BGP および MBGP がサポートされていないため、`ip msdp peer` グローバル コンフィギュレーション コマンドを使用して、ローカル スイッチに MSDP ピアを設定することはできません。その代わりに、デフォルトの MSDP ピアを定義し、そこから送信されるスイッチのすべての SA メッセージを受信できます (そのためには、`ip msdp default-peer` グローバル コンフィギュレーション コマンドを使用します)。デフォルトの MSDP ピアは、事前に設定しておく必要があります。スイッチで MSDP ピアによる BGP または MBGP ピアリングが行われない場合は、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチでは常にそのピアからのすべての SA メッセージを受信されます。

図 47-2 に、デフォルトの MSDP ピアを使用できるネットワークを示します。図 47-2 では、スイッチ B を所有するカスタマーが、2 つの Internet Service Provider (ISP; インターネット サービス プロバイダー) に接続されています。一方の ISP はルータ A、もう一方の ISP はルータ C を所有しています。これらの ISP 間で、BGP または MBGP は動作していません。ISP のドメイン内、または他のドメイン内の送信元を学習するため、カスタマー サイトのスイッチ B はルータ A をデフォルトの MSDP ピアとして識別します。スイッチ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、受信するのはルータ A からの SA メッセージ、またはルータ C からの SA メッセージだけです。ルータ A がコンフィギュレーション ファイルの最初に記述されている場合、ルータ A が動作していれば、ルータ A が使用されます。ルータ A が動作していない場合のみ、スイッチ B はルータ C からの SA メッセージを受信します。これが、プレフィクス リストがない場合のデフォルトの動作です。

プレフィクス リストを指定すると、ピアはリスト内のプレフィクス専用のデフォルト ピアになります。プレフィクス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィクス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアのみです (このピアにルータが接続されていて、ピアがアクティブの場合に限ります)。最初に設定されたデフォルト ピアに障害が発生した場合、またはこのピアが正常に接続されていない場合は、2 番めに設定されているピアがアクティブなデフォルト ピアになります。以下同様に処理されます。

通常、ISP はプレフィクス リストを使用して、カスタマーのルータから受信するプレフィクスを定義します。

図 47-2 デフォルトの MSDP ピア ネットワーク



デフォルトの MSDP ピアを指定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip msdp default-peer ip-address name [prefix-list list]	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。 <ul style="list-style-type: none"> • <i>ip-address name</i> には、MSDP デフォルト ピアの IP アドレスまたは Domain Name System (DNS; ドメイン ネーム システム) サーバ名を入力します。 • (任意) prefix-list list を指定する場合は、リスト内のプレフィクス専用のデフォルト ピアとなるピアを指定するリスト名を入力します。プレフィクス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 <p>prefix-list キーワードが指定された ip msdp default-peer コマンドを複数入力すると、複数の RP プレフィクスに対してすべてのデフォルト ピアが同時に使用されます。この構文は通常、スタブ サイトクラウドに接続されたサービス プロバイダー クラウドで使用されます。</p> <p>prefix-list キーワードを指定せずに ip msdp default-peer コマンドを複数入力すると、単一のアクティブ ピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルト ピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。</p>

コマンド	目的
ステップ 3 <code>ip prefix-list name [description string] seq number {permit deny} network length</code>	(任意) ステップ 2 で指定された名前を使用し、プレフィクスリストを作成します。 <ul style="list-style-type: none"> • (任意) <code>description string</code> を指定する場合は、このプレフィクスリストを説明する 80 文字以下のテキストを入力します。 • <code>seq number</code> には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ~ 4294967294 です。 • <code>deny</code> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • <code>permit</code> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • <code>network length</code> には、許可または拒否されているネットワークの番号およびネットワーク マスク長 (ビット単位) を指定します。
ステップ 4 <code>ip msdp description {peer-name peer-address} text</code>	(任意) 設定内で、または <code>show</code> コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト ピアを削除するには、`no ip msdp default-peer ip-address | name` グローバル コンフィギュレーション コマンドを使用します。

次に、[図 47-2](#) のルータ A およびルータ C の設定の一部を示します。それぞれの ISP には、デフォルトピア (BGP または MBGP 以外) を使用する複数のカスタマーが存在します ([図 47-2](#) のカスタマーと同様)。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィクスリストで SA が許可されている場合、デフォルトピアからの SA のみが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング

デフォルトでは、スイッチで受信された SA メッセージ内の送信元とグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、次の SA メッセージによって送信元に関する情報が取得されるまでそのメンバーは待機する必要があります。この遅延は加入遅延と呼ばれます。

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにスイッチを設定できます。

送信元とグループのペアのキャッシングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip msdp cache-sa-state [list access-list-number]	送信元とグループのペアのキャッシングをイネーブルにします (SA ステートを作成します)。アクセス リストを通過したこれらのペアがキャッシュに格納されます。 list access-list-number を指定する場合、範囲は 100 ~ 199 です。
ステップ 3 access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard	IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> access-list-number の範囲は 100 ~ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 protocol には、プロトコル名として ip を入力します。 source には、パケットの送信元であるネットワークまたはホストの番号を入力します。 source-wildcard には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 destination には、パケットの送信先であるネットワークまたはホストの番号を入力します。 destination-wildcard には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

このコマンドの代わりに、**ip msdp sa-request** グローバル コンフィギュレーション コマンドを使用できます。代替コマンドを使用すると、グループの新しいメンバーがアクティブになった場合に、SA 要求メッセージがスイッチから MSDP ピアに送信されます。詳細については、次のセクションを参照してください。

デフォルト設定 (SA ステートが作成されていない状態) に戻すには、**no ip msdp cache-sa-state** グローバル コンフィギュレーション コマンドを使用します。

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャストトラフィックを受信する必要がある場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャストトラフィックを受信する必要がある場合、MSDP ピアに SA 要求メッセージを送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp sa-request {ip-address name}</code>	指定された MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定します。 <i>ip-address name</i> を指定する場合は、グループの新しいメンバーがアクティブになるときにローカル スイッチの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御

スイッチから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元 (送信元ベース)
- 送信元情報のレシーバー (要求元認識ベース)

詳細については、「送信元の再配信」(P.47-9) および「SA 要求メッセージのフィルタリング」(P.47-10) を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に *A* フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</code>	<p>SA メッセージに格納されてアドバタイズされる、マルチキャストルーティング テーブル内の (S,G) エントリを設定します。</p> <p>デフォルトでは、ローカル ドメイン内の送信元のみがアドバタイズされます。</p> <ul style="list-style-type: none"> • (任意) <code>list access-list-name</code> を指定する場合は、IP 標準または IP 拡張アクセス リストの名前または番号を入力します。標準アクセス リストの範囲は 1 ~ 99、拡張アクセス リストの範囲は 100 ~ 199 です。アクセス リストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 • (任意) <code>asn aspath-access-list-number</code> を指定する場合は、1 ~ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、<code>ip as-path access-list</code> コマンドでも設定する必要があります。 • (任意) <code>route-map map</code> を指定する場合は、1 ~ 199 の範囲の IP 標準または IP 拡張アクセス リスト番号を入力します。このアクセス リスト番号は、<code>ip as-path access-list</code> コマンドでも設定する必要があります。 <p>アクセス リストまたは自律システム パス アクセス リストに従って、(S,G) ペアがアドバタイズされます。</p>

コマンド	目的
ステップ 3 <code>access-list access-list-number {deny permit} source [source-wildcard]</code> または <code>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard</code>	<p>IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <p>または</p> <p>IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <code>access-list-number</code> には、標準アクセス リストの範囲は 1 ~ 99、拡張アクセス リストの範囲は 100 ~ 199 です。ステップ 2 で作成した番号と同じ値を入力します。 • <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 • <code>protocol</code> には、プロトコル名として <code>ip</code> を入力します。 • <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <code>source-wildcard</code> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 • <code>destination</code> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <code>destination-wildcard</code> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、`no ip msdp redistribute` グローバル コンフィギュレーション コマンドを使用します。

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているスイッチのみが、SA 要求に応答します。このようなスイッチでは、デフォルトで MSDP ピアからのすべての SA 要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、スイッチを設定できます。標準アクセス リストに記述されたグループのピアからの SA 要求メッセージのみを採用することもできます。アクセス リスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

これらの方法のいずれかを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp filter-sa-request ip-address name</code> または <code>ip msdp filter-sa-request {ip-address name} list access-list-number</code>	指定された MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。 または 標準アクセス リストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセス リストには、複数のグループ アドレスが記述されています。 <code>access-list-number</code> の範囲は 1 ~ 99 です。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	IP 標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none">• <code>access-list-number</code> の範囲は 1 ~ 99 です。• deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。• <code>source</code> には、パケットの送信元であるネットワークまたはホストの番号を入力します。• (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp filter-sa-request {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセス リスト 1 を通過して、受信されます。その他のすべてのメッセージは無視されます。

```
Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1
Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチで転送される送信元情報の制御

デフォルトでは、スイッチで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または Time To Live (TTL; 存続可能時間) 値を設定し、発信メッセージがピアに転送されないようにできます。次のセクションでは、この方法について説明します。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアのみが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp sa-filter out <i>ip-address</i> <i>name</i> または ip msdp sa-filter out { <i>ip-address</i> <i>name</i> } list <i>access-list-number</i> または ip msdp sa-filter out { <i>ip-address</i> <i>name</i> } route-map <i>map-tag</i>	指定された MSDP ピアへの SA メッセージをフィルタリングします。 または IP 拡張アクセス リストを通過する、指定されたピア宛の SA メッセージのみを通過させます。拡張アクセス リスト <i>access-list-number</i> の範囲は 100 ~ 199 です。 list と route-map の両方のキーワードを使用すると、すべての条件が true である場合に、発信 SA メッセージ内のすべての (S,G) ペアが通過します。 または ルート マップ <i>map-tag</i> 内の一致条件を満たす、指定された MSDP ピア宛の SA メッセージを通過させます。 すべての一致条件が true の場合、ルート マップに permit が指定されていれば、ルートはフィルタを通過します。 deny が指定されていれば、ルートはフィルタリングされます。
ステップ 3	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i>	(任意) IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、`no ip msdp sa-filter out {ip-address | name} [list access-list-number] [route-map map-tag]` グローバル コンフィギュレーション コマンドを使用します。

次に、アクセス リスト 100 を通過する (S,G) ペアのみが SA メッセージに格納され、`switch.cisco.com` という名前のピアに転送されるように設定する例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

SA メッセージに格納されて送信されるマルチキャスト データの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が `tth` 引数以上であるマルチキャスト パケットのみが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip msdp ttl-threshold {ip-address name} tth</code>	指定された MSDP ピア宛の最初の SA メッセージにカプセル化されるマルチキャスト データを制限します。 <ul style="list-style-type: none"> <code>ip-address name</code> を指定する場合は、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 <code>tth</code> には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャスト データ パケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ~ 255 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`no ip msdp ttl-threshold {ip-address | name}` グローバル コンフィギュレーション コマンドを使用します。

スイッチで受信される送信元情報の制御

デフォルトでは、スイッチは、MSDP の RPF ピアによって送信されたすべての SA メッセージを受信します。ただし、着信 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信しないようにスイッチを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip msdp sa-filter in ip-address name または ip msdp sa-filter in {ip-address name} list access-list-number または ip msdp sa-filter in {ip-address name} route-map map-tag	指定された MSDP ピアからの SA メッセージをすべてフィルタリングします。 または IP 拡張アクセス リストを通過する、指定されたピアからの SA メッセージのみを通過させます。拡張アクセス リスト <i>access-list-number</i> の範囲は 100 ~ 199 です。 list と route-map の両方のキーワードを使用すると、すべての条件が true である場合に、着信 SA メッセージ内のすべての (S,G) ペアが通過します。 または ルート マップ <i>map-tag</i> 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージを通過させます。 すべての一致条件が true の場合、ルート マップに permit が指定されていれば、ルートはフィルタを通過します。 deny が指定されていれば、ルートはフィルタリングされます。
ステップ 3 access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard	(任意) IP 拡張アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

コマンド	目的
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フィルタを削除するには、**no ip msdp sa-filter in {ip-address | name} [list access-list-number] [route-map map-tag]** グローバル コンフィギュレーション コマンドを使用します。

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

MSDP メッシュ グループの設定

MSDP メッシュ グループは、MSDP によって完全なメッシュ型に相互接続された MSDP スピーカーのグループです。メッシュ グループ内のピアから受信された SA メッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** グローバル コンフィギュレーション コマンドを使用します。特に、ドメインにわたって SA メッセージを送信する場合に使用します。単一のスイッチに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip msdp mesh-group name {ip-address name}	MSDP メッシュ グループを設定するには、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 <ul style="list-style-type: none"> <i>name</i> には、メッシュ グループの名前を入力します。 <i>ip-address name</i> には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show running-config	設定を確認します。
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 6	グループ内の MSDP ピアごとに、この手順を繰り返します。

メッシュ グループから MSDP ピアを削除するには、**no ip msdp mesh-group name {ip-address | name}** グローバル コンフィギュレーション コマンドを使用します。

MSDP ピアのシャットダウン

複数の MSDP コマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP 接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDP セッションをシャットダウンすることもできます。

ピアをシャットダウンするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp shutdown { <i>peer-name</i> <i>peer address</i> }	設定情報を保持したまま、指定された MSDP ピアを管理上のシャットダウン状態にします。 <i>peer-name</i> <i>peer address</i> を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ピアを再起動するには、**no ip msdp shutdown** {*peer-name* | *peer address*} グローバル コンフィギュレーション コマンドを使用します。TCP 接続が再確立されます。

MSDP への境界 PIM DM 領域の追加

Dense-Mode (DM; dense [稠密] モード) 領域と PIM SM 領域の境界となるスイッチに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。



(注) **ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアダプタイズするように SM ドメインを設定してください。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp border sa-address <i>interface-id</i>	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 <i>interface-id</i> には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。

コマンド	目的
ステップ 3 ip msdp redistribute [<i>list access-list-name</i>] [<i>asn aspath-access-list-number</i>] [<i>route-map map</i>]	SA メッセージに格納されてアドバタイズされる、マルチキャストルーティング テーブル内の (S,G) エントリを設定します。 詳細については、「送信元の再配信」(P.47-9) を参照してください。
ステップ 4 end	特権 EXEC モードに戻ります。
ステップ 5 show running-config	設定を確認します。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

デフォルト設定 (DM 領域内のアクティブな送信元が MSDP に加入しない設定) に戻すには、**no ip msdp border sa-address interface-id** グローバル コンフィギュレーション コマンドを使用します。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュ グループ内の複数のスイッチ上で、ローカルな RP を設定する場合
- PIM SM ドメインと DM ドメインの境界となるスイッチがある場合。サイトの DM ドメインの境界となるスイッチがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このスイッチは RP でないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

SA メッセージの発信元である MSDP スピーカーで、インターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip msdp originator-id interface-id	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。 <i>interface-id</i> には、ローカル スイッチのインターフェイスを指定します。
ステップ 3 end	特権 EXEC モードに戻ります。
ステップ 4 show running-config	設定を確認します。
ステップ 5 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ip msdp border sa-address と **ip msdp originator-id** の両方のグローバル コンフィギュレーション コマンドが設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスによって RP アドレスが決まります。

この方法で RP アドレスが取得されないようにするには、**no ip msdp originator-id interface-id** グローバル コンフィギュレーション コマンドを使用します。

MSDP のモニタおよびメンテナンス

MSDP SA メッセージ、ピア、ステート、またはピア ステータスをモニタするには、表 47-1 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 47-1 MSDP のモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>debug ip msdp [peer-address name] [detail] [routes]</code>	MSDP アクティビティをデバッグします。
<code>debug ip msdp resets</code>	MSDP ピアのリセット原因をデバッグします。
<code>show ip msdp count [autonomous-system-number]</code>	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。 <code>ip msdp cache-sa-state</code> コマンドは、このコマンドによって出力が生成されるように設定する必要があります。
<code>show ip msdp peer [peer-address name]</code>	MSDP ピアに関する詳細情報を表示します。
<code>show ip msdp sa-cache [group-address source-address group-name source-name] [autonomous-system-number]</code>	MSDP ピアから学習した (S,G) ステートを表示します。
<code>show ip msdp summary</code>	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするには、表 47-2 に示す特権 EXEC コマンドを使用します。

表 47-2 MSDP 接続、統計情報、または SA キャッシュ エントリをクリアするためのコマンド

コマンド	目的
<code>clear ip msdp peer peer-address name</code>	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
<code>clear ip msdp statistics [peer-address name]</code>	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報 カウンタをクリアします。
<code>clear ip msdp sa-cache [group-address name]</code>	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。



CHAPTER 48

フォールバック ブリッジングの設定

この章では、Catalyst 3750 スイッチにフォールバック ブリッジング (Virtual LAN (VLAN; 仮想 LAN) ブリッジング) を設定する方法について説明します。フォールバック ブリッジングを使用すると、スイッチが VLAN ブリッジ ドメインとルーテッド ポート間でルーティングしない、非 IP パケットを転送できます。

この機能を使用するには、スタック マスター上で IP サービス イメージが稼働している必要があります。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*』 Release 12.2 を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- 「フォールバック ブリッジングの概要」 (P.48-1)
- 「フォールバック ブリッジングの設定」 (P.48-3)
- 「フォールバック ブリッジングのモニタリングおよびメンテナンス」 (P.48-11)

フォールバック ブリッジングの概要

ここでは、フォールバック ブリッジングの機能について説明します。

- 「フォールバック ブリッジングの概要」 (P.48-1)
- 「フォールバック ブリッジングおよびスイッチ スタック」 (P.48-3)

フォールバック ブリッジングの概要

フォールバック ブリッジングを使用すると、スイッチは複数の VLAN またはルーテッド ポート (特に 1 つのブリッジ ドメイン内で複数の VLAN に接続されている VLAN またはルーテッド ポート) をまとめてブリッジングできます。フォールバック ブリッジングを行うと、スイッチでルーティングされないトラフィックや DECnet など、ルーティングできないプロトコルに属するトラフィックが転送されます。

VLAN ブリッジ ドメインは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) によって表されます。(VLAN が関連付けられていない) 一連の SVI およびルーテッド ポートは、ブリッジ グループを形成するように設定 (グループ化) できます。SVI はスイッチ ポートの VLAN を、システム内のルーティング機能またはブリッジング機能へのインターフェイスの 1 つとして表します。1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN 間のルーティング、VLAN 間でルーティングできないプロトコルのフォールバック ブリッジング、またはスイッチと IP ホストの接続を実現する場合にだけ、VLAN に SVI を設定してください。ルーテッド ポートはルータ上のポートと同様に機能する物理ポートですが、ルータには接続されていません。ルーテッド ポートは特定の VLAN と関連付けられておらず、VLAN サブインターフェイスをサポートしていませんが、通常のルーテッド ポートのように動作します。SVI およびルーテッド ポートの詳細については、第 12 章「インターフェイス特性の設定」を参照してください。

ブリッジ グループは、スイッチ上のネットワーク インターフェイスの内部構造です。ブリッジ グループが定義されているスイッチの外側にあるブリッジ グループ内では、スイッチングされるトラフィックを識別するためにブリッジ グループを使用することはできません。同じスイッチ上のブリッジ グループは、異なるブリッジとして機能します。つまり、スイッチ上の異なるブリッジグループ間で、ブリッジド トラフィックおよび Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) は交換されません。

フォールバック ブリッジングを使用しても、ブリッジングされている VLAN のスパンニング ツリーは縮小できません。各 VLAN には、独自のスパンニング ツリー インスタンスと、ループを防止するためにブリッジ グループの一番上で動作する個別のスパンニング ツリー (別名 VLAN ブリッジ スパンニング ツリー) があります。

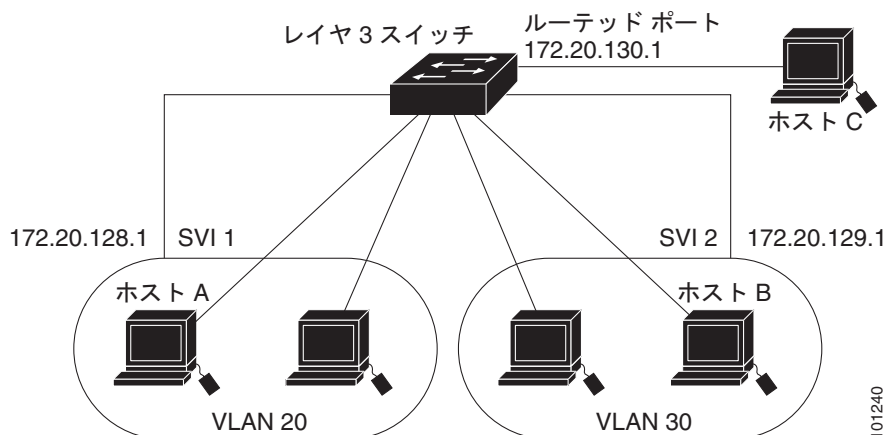
ブリッジ グループが作成されると、スイッチは VLAN ブリッジ スパンニング ツリー インスタンスを作成します。スイッチはブリッジ グループを実行し、ブリッジ グループ内の SVI およびルーテッド ポートをスパンニング ツリー ポートとして処理します。

ネットワーク インターフェイスをブリッジ グループに格納する理由は、次のとおりです。

- ブリッジ グループを構成するネットワーク インターフェイス間でルーティングされない全トラフィックをブリッジングするため。宛先アドレスがブリッジ テーブルに格納されているパケットは、ブリッジ グループ内の単一のインターフェイス上で転送されます。宛先アドレスがブリッジ テーブル内に格納されていないパケットは、ブリッジ グループ内のすべてのインターフェイス上でフラッディングされます。ブリッジ グループで送信元 MAC アドレスが取得されるのは、このアドレスが VLAN 上で取得された場合のみです (この逆は成り立ちません)。スタック メンバーで取得されたアドレスは、スタック内のすべてのスイッチで取得されます。
- 接続されている LAN 上で BPDU を受信 (場合によっては送信) することにより、スパンニング ツリー アルゴリズムに参加するため。設定されたブリッジ グループごとに、個別のスパンニング ツリー プロセスが動作します。各ブリッジ グループは個別のスパンニング ツリー インスタンスに参加します。ブリッジ グループは、メンバー インターフェイスだけが受信する BPDU に基づいて、スパンニング ツリー インスタンスを確立します。VLAN がブリッジ グループに属していないポートに着信したブリッジ Spanning-Tree Bridge Protocol (STP; スパンニング ツリー ブリッジ プロトコル) BPDU は、VLAN のすべての転送ポートでフラッディングされます。

図 48-1 に、フォールバック ブリッジング ネットワークの例を示します。このスイッチには、SVI として 2 つのポートが設定されています。これらの SVI は異なる IP アドレスを持ち、2 つの異なる VLAN に接続されています。さらに、もう 1 つのポートが独自の IP アドレスを持つルーテッド ポートとして設定されています。これらの 3 つのポートがすべて同じブリッジ グループに割り当てられている場合は、これらのポートが異なるネットワークや異なる VLAN にあっても、スイッチに接続されているエンド ステーション間で非 IP プロトコル フレームを転送できます。フォールバック ブリッジングを機能させるために IP アドレスをルーテッド ポートや SVI に割り当てる必要はありません。

図 48-1 フォールバック ブリッジング ネットワークの例



フォールバック ブリッジングおよびスイッチ スタック

スタック マスターに障害が発生すると、第 5 章「スイッチ スタックの管理」に記載された選択プロセスを使用して、スタック メンバーの 1 つが新しいスタック マスターになります。新しいスタック マスターは新しい VLAN ブリッジ スパニング ツリー インスタンスを作成し、このインスタンスはフォールバック ブリッジングに使用されるスパニング ツリー ポートを一時的に非フォワーディング ステートにします。スパニング ツリー ステートがフォワーディング ステートに移行するまでは、一時的にトラフィックが中断されることがあります。ブリッジ グループで、すべての MAC アドレスを取得し直す必要があります。



(注) IP サービス イメージを実行しているスタック マスターで障害が発生し、新しく選択されたスタック マスターが IP ベース イメージ (以前の標準マルチレイヤ イメージ [SMI]) を実行している場合、そのスイッチ スタックのフォールバック ブリッジング機能は失われます。

スタックを統合するか、またはスタックに新しいスイッチを追加すると、ブリッジ グループに属する、アクティブになった新しい VLAN が、VLAN ブリッジ STP に追加されます。

スタック メンバーに障害が発生すると、このメンバーから取得されたアドレスがブリッジ グループ MAC アドレス テーブルから削除されます。

スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

フォールバック ブリッジングの設定

ここでは、次の設定情報について説明します。

- 「フォールバック ブリッジングのデフォルト設定」(P.48-4)
- 「フォールバック ブリッジング設定時の注意事項」(P.48-4)
- 「ブリッジ グループの作成」(P.48-4) (必須)
- 「スパニング ツリー パラメータの調整」(P.48-6) (任意)

フォールバック ブリッジングのデフォルト設定

表 48-1 に、フォールバック ブリッジングのデフォルト設定を示します。

表 48-1 フォールバック ブリッジングのデフォルト設定

機能	デフォルト設定
ブリッジ グループ	未定義であるか、またはポートに割り当てられていません。VLAN ブリッジ STP は定義されていません。
動的に学習されたステーションに対するスイッチからのフレーム転送	イネーブル。
スパニング ツリー パラメータ	
<ul style="list-style-type: none"> スイッチ プライオリティ ポート プライオリティ ポート パス コスト 	<ul style="list-style-type: none"> 32768 128 10 Mbps : 100 100 Mbps : 19 1000 Mbps : 4
<ul style="list-style-type: none"> hello BPDU インターバル 転送遅延インターバル 最大アイドル時間 	<ul style="list-style-type: none"> 2 秒 20 秒 30 秒

フォールバック ブリッジング設定時の注意事項

スイッチには、最大 32 個のブリッジ グループを設定できます。

1 つのインターフェイス (SVI またはルーテッド ポート) が所属できるブリッジ グループは 1 つだけです。

スイッチに接続されている個別のブリッジド ネットワーク (トポロジの上で区別されるネットワーク) ごとに、1 つのブリッジ グループを使用してください。

フォールバック ブリッジングをプライベート VLAN が設定されたスイッチに設定しないでください。

IP (バージョン 4 とバージョン 6)、Address Resolution Protocol (ARP; アドレス解決プロトコル)、Reverse ARP (RARP)、LOOPBACK、フレーム リレー ARP、共有 STP パケットを除くすべてのプロトコルは、フォールバック ブリッジングされます。

ブリッジ グループの作成

一連の SVI またはルーテッド ポートにフォールバック ブリッジングを設定する場合は、これらのインターフェイスをブリッジ グループに割り当てる必要があります。同じグループ内のすべてのインターフェイスは、同じブリッジドメインに属します。各 SVI またはルーテッド ポートは、1 つのブリッジグループだけに割り当てることができます。



(注)

保護ポート機能をフォールバック ブリッジングと併用することはできません。フォールバック ブリッジングがイネーブルである場合、スイッチ上の 1 つの保護ポートから、別の VLAN 内にある同じスイッチ上の別の保護ポートにパケットが転送される可能性があります。

ブリッジグループを作成し、そこにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 bridge bridge-group protocol vlan-bridge	ブリッジグループ番号を割り当て、ブリッジグループで実行する VLAN ブリッジ スパニング ツリー プロトコルを指定します。 ibm および dec キーワードはサポートされていません。 <i>bridge-group</i> には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。最大 32 個のブリッジグループを作成できます。フレームは同じグループ内のインターフェイス間でのみブリッジングされます。
ステップ 3 interface interface-id	ブリッジグループを割り当てるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> • ルーテッド ポート : no switchport インターフェイス コンフィギュレーション コマンドを入力して、レイヤ 3 ポートとして設定された物理ポートです。 • SVI : interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 (注) ルーテッド ポートや SVI に IP アドレスを割り当てることができますが、これは必須ではありません。
ステップ 4 bridge-group bridge-group	ステップ 2 で作成したブリッジグループにインターフェイスを割り当てます。 デフォルトでは、インターフェイスはどのブリッジグループにも割り当てられていません。インターフェイスは 1 つのブリッジグループにのみ割り当てることができます。
ステップ 5 end	特権 EXEC モードに戻ります。
ステップ 6 show running-config	設定を確認します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ブリッジグループを削除するには、**no bridge bridge-group** グローバル コンフィギュレーション コマンドを使用します。**no bridge bridge-group** コマンドを使用すると、該当するブリッジグループからすべての SVI およびルーテッド ポートが自動的に削除されます。ブリッジグループからインターフェイスを削除したり、ブリッジグループを削除するには、**no bridge-group bridge-group** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジグループ 10 を作成してこのブリッジグループ内で実行する VLAN ブリッジ STP を指定し、ポートをルーテッド ポートとして定義して、ブリッジグループにポートを割り当てる例を示します。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# bridge-group 10
```

次に、ブリッジグループ 10 を作成して、このブリッジグループで実行する VLAN ブリッジ STP を指定する例を示します。VLAN 2 の SVI を定義し、これをブリッジグループに割り当てます。

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface vlan2
Switch(config-if)# bridge-group 10
Switch(config-if)# exit
```

スパニング ツリー パラメータの調整

特定のスパニング ツリー パラメータのデフォルト値が不適切な場合は、このパラメータを調整する必要があります。スパニング ツリー全体に影響するパラメータを設定する場合は、さまざまなタイプの **bridge** グローバル コンフィギュレーション コマンドを使用します。インターフェイス固有のパラメータを設定する場合は、さまざまなタイプの **bridge-group** インターフェイス コンフィギュレーション コマンドを使用します。

スパニング ツリー パラメータを調整するには、次に示す作業のいずれかを実行します。

- 「VLAN ブリッジ スパニング ツリー プライオリティの変更」 (P.48-6) (任意)
- 「インターフェイス プライオリティの変更」 (P.48-7) (任意)
- 「パス コストの割り当て」 (P.48-7) (任意)
- 「BPDU インターバルの調整」 (P.48-8) (任意)
- 「インターフェイスでのスパニング ツリーのディセーブル化」 (P.48-10) (任意)



(注)

スパニング ツリー パラメータの調整は、スイッチおよび STP の機能に精通しているネットワーク管理者のみが行ってください。計画が不十分なまま調整を行うと、パフォーマンスの低下を招くことがあります。スイッチングに関する資料としては、IEEE 802.1D 仕様が適しています。詳細については、『Cisco IOS Configuration Fundamentals Command Reference』の付録「References and Recommended Reading」を参照してください。

VLAN ブリッジ スパニング ツリー プライオリティの変更

ルート スイッチの候補として別のスイッチと同等のレベルにあるスイッチには、VLAN ブリッジ スパニング ツリー プライオリティをグローバルに設定できます。このスイッチがルート スイッチとして選択される可能性を設定することもできます。

スイッチ プライオリティを変更するには、特権 EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group priority number	スイッチの VLAN ブリッジ スパニング ツリー プライオリティを変更します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>number</i> には、0 ~ 65535 の数字を入力します。デフォルト値は 32768 です。この値が低いほど、スイッチがルートとして選択される可能性が高くなります。
ステップ 3	end	特権 EXEC モードに戻ります。

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

デフォルト設定に戻すには、**no bridge bridge-group priority** グローバル コンフィギュレーション コマンドを使用します。ポートのプライオリティを変更するには、**bridge-group priority** インターフェイス コンフィギュレーション コマンドを使用します (次のセクションを参照)。

次に、ブリッジグループ 10 のスイッチ プライオリティを 100 に設定する例を示します。

```
Switch(config)# bridge 10 priority 100
```

インターフェイス プライオリティの変更

ポートのプライオリティを変更できます。2 つのスイッチがルート スwitch の候補として同等のレベルにある場合は、レベルに差が付くようにポート プライオリティを設定します。インターフェイスのプライオリティ値が低いスイッチが選択されます。

インターフェイス プライオリティを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	プライオリティを設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bridge-group bridge-group priority number	ポート プライオリティを変更します。 <ul style="list-style-type: none"> bridge-group には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。 number には、0 ~ 255 の値を入力します (増分値は 4)。この値が低いほど、スイッチのポートがルートとして選択される可能性が高くなります。デフォルト値は 128 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、**no bridge-group bridge-group priority** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジグループ 10 内のポートのプライオリティを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1  
Switch(config-if)# bridge-group 10 priority 20
```

パス コストの割り当て

各ポートにはパス コストが割り当てられています。規定では、パス コストは 1000/接続された LAN のデータ速度の値を Mbps 単位で表したものです。

パス コストを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	パス コストを設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>bridge-group bridge-group path-cost cost</code>	ポートのパス コストを割り当てます。 <ul style="list-style-type: none"> • <code>bridge-group</code> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <code>cost</code> には、0 ~ 65535 の数字を入力します。値が大きいほど、コストは大きくなります。 <ul style="list-style-type: none"> - 10 Mbps の場合、デフォルトのパス コストは 100 です。 - 100 Mbps の場合、デフォルトのパス コストは 19 です。 - 1000 Mbps の場合、デフォルトのパス コストは 4 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのパス コストに戻すには、`no bridge-group bridge-group path-cost` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートのパス コストを 20 に変更する例を示します。

```
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# bridge-group 10 path-cost 20
```

BPDU インターバルの調整

ここでは、BPDU インターバルを調整する手順について説明します。

- 「[hello BPDU インターバルの調整](#)」 (P.48-9) (任意)
- 「[転送遅延インターバルの変更](#)」 (P.48-9) (任意)
- 「[最大アイドル時間の変更](#)」 (P.48-10) (任意)



(注)

スパニング ツリーの各スイッチには、個々の設定に関係なく、ルート スイッチの hello BPDU インターバル、転送遅延インターバル、および最大アイドル時間パラメータが採用されています。

hello BPDU インターバルの調整

hello BPDU インターバルを調整するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group hello-time seconds	hello BPDU インターバルを指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、1 ~ 10 の数字を入力します。デフォルト値は 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、ブリッジ グループ 10 内の hello インターバルを 5 秒に変更する例を示します。

```
Switch(config)# bridge 10 hello-time 5
```

転送遅延インターバルの変更

転送遅延インターバルは、ポートでスイッチングがアクティブになってから実際に転送を開始するまでの時間です。この間にトポロジ変更情報のリスニングが行われます。

転送遅延インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group forward-time seconds	転送遅延インターバルを指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジ グループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、4 ~ 200 の数字を入力します。デフォルト値は 20 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、ブリッジ グループ 10 内の転送遅延インターバルを 10 秒に変更する例を示します。

```
Switch(config)# bridge 10 forward-time 10
```

最大アイドル時間の変更

指定時間内にルートスイッチから BPDU が受信されない場合は、スパニングツリートポロジが再計算されます。

最大アイドル時間（最大エージングタイム）を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	bridge bridge-group max-age seconds	ルートスイッチから BPDU をヒアリングするために待機する時間を指定します。 <ul style="list-style-type: none"> • <i>bridge-group</i> には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。 • <i>seconds</i> には、6 ~ 200 の数字を入力します。デフォルトは 30 秒です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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

次に、ブリッジグループ 10 内の最大アイドル時間を 30 秒に変更する例を示します。

```
Switch(config)# bridge 10 max-age 30
```

インターフェイスでのスパニングツリーのディセーブル化

2 つの任意のスイッチングサブネットワーク間にループのないパスが存在する場合は、一方のスイッチングサブネットワークで生成された BPDU の影響が他方のサブネットワーク内のデバイスに及ばないようにできます（ただし、ネットワーク全体に及ぶスイッチングは可能です）。たとえば、スイッチング LAN サブネットワークが WAN によって分離されている場合は、BPDU の WAN リンク間移動を禁止できます。

ポート上でスパニングツリーをディセーブルするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	bridge-group bridge-group spanning-disabled	ポート上でスパニングツリーをディセーブルにします。 <i>bridge-group</i> には、ブリッジグループ番号を指定します。指定できる範囲は 1 ~ 255 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ポート上でスパンニング ツリーを再びイネーブルにするには、**no bridge-group *bridge-group* spanning-disabled** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ブリッジ グループ 10 内のポートのスパンニング ツリーをディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet3/0/1
Switch(config-if)# bridge group 10 spanning-disabled
```

フォールバック ブリッジングのモニタリングおよびメンテナンス

ネットワークをモニタしてメンテナンスするには、表 48-2 に記載された特権 EXEC コマンドを 1 つまたは複数使用します。

表 48-2 フォールバック ブリッジングのモニタリングおよびメンテナンスのためのコマンド

コマンド	目的
clear bridge <i>bridge-group</i>	取得されたエントリを転送データベースから削除します。
show bridge [<i>bridge-group</i>] group	ブリッジ グループの詳細を表示します。
show bridge [<i>bridge-group</i>] [<i>interface-id</i> <i>mac-address</i> verbose]	ブリッジ グループ内で取得された MAC アドレスを表示します。

スタック メンバー上のブリッジ グループ MAC アドレス テーブルを表示するには、スタック マスターからスタック メンバーへのセッションを開始します。そのためには、**session *stack-member-number* global** コンフィギュレーション コマンドを使用します。スタック メンバーのプロンプトに、**show bridge [*bridge-group*] [*interface-id* | *mac-address* | **verbose**]** 特権 EXEC コマンドを入力します。

画面に表示されるフィールドについては、『Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2』Release 12.2 を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。



CHAPTER 49

トラブルシューティング

この章では、Cisco IOS ソフトウェアに関連する、Catalyst 3750 スイッチの問題点を特定し、解決する方法について説明します。問題の性質に応じて、Command-Line Interface (CLI; コマンドラインインターフェイス)、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

LED の説明など、トラブルシューティングの詳細については、『Hardware Installation Guide』を参照してください。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスおよび『Cisco IOS Commands Master List』 Release 12.2 を参照してください。これらのマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- 「ソフトウェアで障害が発生した場合の回復」 (P.49-2)
- 「パスワードを忘れた場合の回復」 (P.49-3)
- 「スイッチ スタック問題の回避」 (P.49-8)
- 「コマンド スイッチで障害が発生した場合の回復」 (P.49-9)
- 「クラスタ メンバー スイッチとの接続の回復」 (P.49-13)



(注) 回復手順を実行するには、スイッチを直接操作しなければなりません。

- 「自動ネゴシエーションの不一致の防止」 (P.49-13)
- 「PoE スイッチ ポートのトラブルシューティング」 (P.49-13)
- 「SFP モジュールのセキュリティと識別」 (P.49-14)
- 「SFP モジュール ステータスのモニタリング」 (P.49-15)
- 「温度のモニタリング」 (P.49-15)
- 「ping の使用」 (P.49-15)
- 「レイヤ 2 traceroute の使用」 (P.49-17)
- 「IP traceroute の使用」 (P.49-18)

- 「TDR の使用」 (P.49-20)
- 「debug コマンドの使用」 (P.49-21)
- 「show platform forward コマンドの使用」 (P.49-23)
- 「crashinfo ファイルの使用」 (P.49-25)
- 「トラブルシューティングの表」 (P.49-26)

ソフトウェアで障害が発生した場合の回復

スイッチ ソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤ったファイルをダウンロードした場合、イメージ ファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは Power-On Self-Test (POST; 電源投入時セルフテスト) に失敗し、接続できなくなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージ ファイルまたは間違ったイメージ ファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多数あり、使用するエミュレーション ソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作しなければなりません。

-
- ステップ 1** PC 上で、Cisco.com から tar 形式のソフトウェア イメージ ファイル (*image_filename.tar*) をダウンロードします。
- Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージ ファイルの検索方法については、リリース ノートを参照してください。
- ステップ 2** tar ファイルから bin ファイルを抽出します。
- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
 - UNIX を使用している場合は、次の手順に従ってください。
 1. **tar -tvf <image_filename.tar>** UNIX コマンドを使用して、tar ファイルの内容を表示します。


```
unix-1% tar -tvf image_filename.tar
```
 2. **tar -xvf <image_filename.tar> <image_filename.bin>** UNIX コマンドを使用して、bin ファイルを特定し、抽出します。


```
unix-1% tar -xvf image_filename.tar image_filename.bin
x c3750-ipservices-mz.122-25.SEB/c3750-ipservices-mz.122-25.SEB.bin, 3970586
bytes, 7756 tape blocks
```
 3. **ls -l <image_filename.bin>** UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。


```
unix-1% ls -l image_filename.bin
-rw-r--r--  1 boba          3970586 Apr 21 12:00
c3750-ipservices-mz.122-25.SEB/c3750-ipservices-mz.122-25.SEB.bin
```
- ステップ 3** XMODEM プロトコルをサポートする端末エミュレーション ソフトウェアを備えた PC を、スイッチのコンソール ポートに接続します。
- ステップ 4** エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。
- ステップ 5** スwitchの電源コードを取り外します。

ステップ 6 [Mode] ボタンを押しながら、電源コードをスイッチに再接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、[Mode] ボタンを離します。ソフトウェアに関する数行分の情報と指示が表示されます。

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#
```

```
flash_init
load_helper
boot
```

ステップ 7 フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 8 コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 9 ヘルパー ファイルがある場合にはロードします。

```
switch: load_helper
```

ステップ 10 XMODEM プロトコルを使用して、ファイル転送を開始します。

```
switch: copy xmodem: flash:image_filename.bin
```

ステップ 11 XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに適切なコマンドを使用して、転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 12 新規にダウンロードされた Cisco IOS イメージを起動します。

```
switch:boot flash:image_filename.bin
```

ステップ 13 **archive download-sw** 特権 EXEC コマンドを使用して、スイッチまたはスイッチ スタックにソフトウェア イメージをダウンロードします。

ステップ 14 **reload** 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。

ステップ 15 スイッチから、**flash:image_filename.bin** ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンド ユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。



(注)

これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようすると、回復プロセスの間、ステータス メッセージにその旨が表示されます。

ここでは、スイッチのパスワードを忘れた場合の回復手順について説明します。

- 「パスワード回復がイネーブルになっている場合の手順」 (P.49-5)
- 「パスワード回復がディセーブルになっている場合の手順」 (P.49-6)

パスワードの回復をイネーブルまたはディセーブルにするには、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。**service password-recovery** または **no service password-recovery** コマンドをスタック マスターに入力すると、スタック全体にコマンドが伝播され、スタック内のすべてのスイッチに適用されます。

スイッチのパスワードを忘れた場合には、次の手順に従ってください。

-
- ステップ 1** 端末エミュレーション ソフトウェアが稼動している端末または PC をスイッチのコンソール ポートに接続します。スイッチ スタックに対してパスワードを回復する場合は、スタック マスターのコンソール ポートに接続します。
- ステップ 2** エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。
- ステップ 3** スタンドアロン スイッチまたはスイッチ スタック全体の電源を切断します。
- ステップ 4** 電源コードをスタンドアロン スイッチまたはスタック マスターに再接続します。その後 15 秒以内に、[Mode] ボタンを押します。このときシステム LED はグリーンに点滅しています。システム LED が一瞬オレンジに点灯してからグリーンになるまで [Mode] ボタンを押したままにしてください。グリーンになったら [Mode] ボタンを離します。

ソフトウェアについての情報および指示が数行表示され、パスワード回復手順がディセーブルであるかどうかが表示されます。

- 次の内容で始まるメッセージが表示された場合

```
The system has been interrupted prior to initializing the flash file system.The
following commands will initialize the flash file system
```

「パスワード回復がイネーブルになっている場合の手順」 (P.49-5) に進んで、その手順に従います。

- 次の内容で始まるメッセージが表示された場合

```
The password-recovery mechanism has been triggered, but is currently disabled.
```

「パスワード回復がディセーブルになっている場合の手順」 (P.49-6) に進んで、その手順に従います。

- ステップ 5** パスワードが回復したら、スタンドアロン スイッチまたはスタック マスターをリロードします。

```
Switch> reload
 slot <stack-master-member-number>
Proceed with reload?[confirm] y
```

- ステップ 6** スイッチ スタックの残りのメンバーの電源をオンにします。
-

パスワード回復がイネーブルになっている場合の手順

パスワード回復メカニズムがイネーブルになっている場合は、次のメッセージが表示されます。

```
The system has been interrupted prior to initializing the flash file system.The following
commands will initialize the flash file system, and finish loading the operating system
software:
```

```
flash_init
load_helper
boot
```

ステップ 1 フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 2 コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 3 ヘルパー ファイルがある場合にはロードします。

```
switch: load_helper
```

ステップ 4 フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
 13 drwx      192  Mar 01 1993 22:30:48 c3750-ipservices-mz-122-25.SEB
 11 -rwx      5825  Mar 01 1993 22:31:59 config.text
 18 -rwx       720  Mar 01 1993 02:21:30 vlan.dat
```

```
16128000 bytes total (10003456 bytes free)
```

ステップ 5 コンフィギュレーション ファイルの名前を `config.text.old` に変更します。

このファイルには、パスワード定義が収められています。

```
switch: rename flash:config.text flash:config.text.old
```

ステップ 6 システムを起動します。

```
switch: boot
```

セットアップ プログラムを起動するように求められます。プロンプトに **N** を入力します。

```
Continue with the configuration dialog?[yes/no]: N
```

ステップ 7 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 8 コンフィギュレーション ファイルを元の名前に戻します。

```
Switch# rename flash:config.text.old flash:config.text
```



(注) 接続されたすべてのスタック メンバーの電源をオンにし、完全に初期化されるまで待機してから、ステップ 9 に進んでください。このステップに従わなかった場合は、スイッチの設定によっては設定を失う可能性もあります。

ステップ 9 コンフィギュレーション ファイルをメモリにコピーします。

```
Switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

確認を求めるプロンプトに、**Return** キーを押して応答します。

これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できます。

ステップ 10 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11 パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ~ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 特権 EXEC モードに戻ります。

```
Switch (config)# exit
Switch#
```

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。



(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン状態になることがあります。この状態になっているインターフェイスを調べるには、**show running-config** 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan vlan-id** グローバル コンフィギュレーション コマンドを入力して、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

ステップ 14 スイッチ スタックをリロードします。

```
Switch# reload
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルになっている場合は、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled.Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

**注意**

スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせ、バックアップ スイッチと VLAN コンフィギュレーション ファイルがあるかどうかを確認してください。

- **n** (no) を入力すると、[Mode] ボタンを押さなかった場合と同様に、通常のブート プロセスが継続されます。ブート ローダ プロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。次のメッセージが表示されます。

```
Press Enter to continue.....
```

- **y** (yes) を入力すると、フラッシュ メモリ内のコンフィギュレーション ファイルおよび VLAN データベース ファイルが削除されます。デフォルト設定がロードされるときに、パスワードをリセットできます。

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)?Y
```

ステップ 2 ヘルパー ファイルがある場合にはロードします。

```
Switch: load_helper
```

ステップ 3 フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
```

```
13 drwx          192   Mar 01 1993 22:30:48 c3750-ipservice-mz-122-25.0
```

```
16128000 bytes total (10003456 bytes free)
```

ステップ 4 システムを起動します。

```
Switch: boot
```

セットアップ プログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog?[yes/no]: N
```

ステップ 5 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 6 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 7 パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ~ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 8 特権 EXEC モードに戻ります。

```
Switch (config)# exit
```

```
Switch#
```



(注) 接続されたすべてのスタック メンバーの電源をオンにし、完全に初期化されるまで待機してから、ステップ 9 に進んでください。

ステップ 9 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。



(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。このステートになっているインターフェイスを調べるには、**show running-config** 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan vlan-id** グローバル コンフィギュレーション コマンドを入力して、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

ステップ 10 ここでスイッチを再設定する必要があります。システム管理者によって、バックアップ スイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

スイッチ スタック問題の回避



- (注)
- スイッチ スタックに追加または削除するスイッチの電源が切断されていることを確認します。スイッチ スタックの電源に関するすべての考慮事項については、『Hardware Installation Guide』の「Switch Installation」の章を参照してください。
 - スタック メンバーを追加または削除したあとで、スイッチ スタックがすべての帯域幅 (32 Gbps) で動作していることを確認します。スタック モード LED が点灯するまで、スタック メンバーの [Mode] ボタンを押します。スイッチ上の最後の 2 つのポート LED は、グリーンに点灯します。スイッチ モデルに応じて、最後の 2 つのポートは 10/100/1000 ポートまたは Small Form-Factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュール ポートになります。最後の 2 つのポート LED のいずれか、または両方がグリーンに点灯しない場合は、スタックがすべての帯域幅で動作していません。
 - スイッチ スタックを管理する場合は、CLI セッションを 1 つのみ使用することを推奨します。スタック マスターに複数の CLI セッションを使用する場合は、慎重に行ってください。特定のセッションで入力したコマンドは、他のセッションに表示されません。したがって、コマンドを入力したセッションを識別できなくなることがあります。
 - スタック内のスイッチの位置に従ってスタック メンバー番号を手動で割り当てると、離れた位置からのスイッチ スタックのトラブルシューティングが容易になります。ただし、あとでスイッチを追加、削除、再編成する場合は、手動で割り当てられた番号を思い出す必要があります。スタック メンバー番号を手動で割り当てるには、**switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用します。スタック メンバー番号の詳細については、「メンバー番号」(P.5-6) を参照してください。

スタック メンバーを同一モデルと交換した場合、新しいスイッチは交換前のスイッチとまったく同じ設定で動作します。また、新しいスイッチでは、交換前のスイッチと同じメンバー番号が使用されません。

電源がオンの状態のスタック メンバーを取り外すと、スイッチ スタックがそれぞれ同じ設定を持つ複数のスイッチ スタックに分割（パーティション化）されます。スイッチ スタックを分割状態のまま使用する場合は、新規に作成されたスイッチ スタックの IP アドレスを変更します。パーティション化されたスイッチ スタックを元に戻す手順は、次のとおりです。

1. 新規に作成されたスイッチ スタックの電源を切断します。
2. 新しいスイッチ スタックを、StackWise ポートを通じて元のスイッチ スタックに再度接続します。
3. スイッチの電源をオンにします。

スイッチ スタックおよびスタック メンバーのモニタに使用できるコマンドについては、「[スタック情報の表示](#)」(P.5-23) を参照してください。

コマンドスイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) を使用すると、冗長コマンドスイッチグループを設定できます。詳細については、[第 6 章「スイッチのクラスタ化」](#) および [第 42 章「HSRP の設定」](#) を参照してください。Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』も参照してください。



(注) HSRP は、クラスタを冗長構成にする場合に適しています。

スタンバイ コマンドスイッチが未設定で、かつコマンドスイッチで電源故障などの障害が発生した場合には、メンバー スイッチとの管理接続が失われるので、新しいコマンドスイッチに交換する必要があります。ただし、接続されているスイッチ間の接続は影響を受けません。また、メンバー スイッチも通常どおりにパケットを転送します。メンバー スイッチは、コンソール ポートを通じてスタンドアロンのスイッチとして管理できます。また、IP アドレスが与えられている場合は、他の管理インターフェイスを使用して管理できます。

コマンド対応メンバー スイッチまたは他のスイッチに IP アドレスを割り当て、コマンドスイッチのパスワードを書き留め、メンバー スイッチと交換用コマンドスイッチ間の冗長接続が得られるようにクラスタを配置することにより、コマンドスイッチ障害に備えます。ここでは、故障したコマンドスイッチの交換方法を 2 通り紹介します。

- 「[故障したコマンドスイッチをクラスタ メンバーと交換する場合](#)」(P.49-10)
- 「[故障したコマンドスイッチを他のスイッチと交換する場合](#)」(P.49-11)

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

コマンド対応スイッチについては、リリース ノートを参照してください。

故障したコマンドスイッチをクラスタメンバーと交換する場合

故障したコマンドスイッチを同じクラスタ内のコマンド対応メンバースイッチに交換するには、次の手順に従ってください。

- ステップ 1** コマンドスイッチとメンバースイッチとの接続を切断し、クラスタからコマンドスイッチを物理的に取り外します。
- ステップ 2** 故障したコマンドスイッチの代わりに新しいメンバースイッチを取り付け、コマンドスイッチとクラスタメンバー間の接続を復元します。
- ステップ 3** 新しいコマンドスイッチで CLI セッションを開始します。
CLI にはコンソールポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。コンソールポートの詳細な使用方法については、スイッチの『Hardware Installation Guide』を参照してください。
- ステップ 4** スイッチプロンプトで、特権 EXEC モードを開始します。
Switch> **enable**
Switch#
- ステップ 5** 故障したコマンドスイッチのパスワードを入力します。
- ステップ 6** グローバルコンフィギュレーションモードを開始します。
Switch# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
- ステップ 7** クラスタからメンバースイッチを削除します。
特権 Switch(config)# **no cluster commander-address**
- ステップ 8** EXEC モードに戻ります。
Switch(config)# **end**
Switch#
- ステップ 9** セットアッププログラムを使用して、スイッチの IP 情報を設定します。IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、**Return** キーを押します。
Switch# **setup**
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:

ステップ 10 最初のプロンプトに **Y** を入力します。

セットアッププログラムのプロンプトは、コマンドスイッチとして選択したメンバースイッチによって異なります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、**Return** キーを押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** キーを押してください。

ステップ 11 セットアッププログラムの質問に回答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字、メンバースイッチ上では 31 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (**n** は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されることに注意してください。

ステップ 12 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 13 スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** キーを押します (要求された場合)。

ステップ 14 クラスタに名前を指定し、**Return** キーを押します (要求された場合)。

クラスタ名には 1 ~ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 16 表示された情報が正しい場合は、**Y** を入力し、**Return** キーを押します。

情報に誤りがある場合には、**N** を入力し、**Return** キーを押して、ステップ 9 からやり直します。

ステップ 17 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 18 クラスタ メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンドスイッチを他のスイッチと交換する場合

故障したコマンドスイッチを、クラスタに組み込まれていないコマンド対応スイッチと交換する場合、次の手順に従ってください。

ステップ 1 故障したコマンドスイッチの代わりに新しいスイッチを取り付け、コマンドスイッチとクラスタメンバー間の接続を復元します。

ステップ 2 新しいコマンドスイッチで CLI セッションを開始します。

CLI にはコンソールポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。コンソールポートの詳しい使用方法については、スイッチの『Hardware Installation Guide』を参照してください。

ステップ 3 スイッチプロンプトで、特権 EXEC モードを開始します。

```
Switch> enable  
Switch#
```

ステップ 4 故障したコマンドスイッチのパスワードを入力します。

ステップ 5 セットアッププログラムを使用して、スイッチの IP 情報を設定します。

IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、**Return** キーを押します。

```
Switch# setup
    --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

ステップ 6 最初のプロンプトに **Y** を入力します。

セットアッププログラムのプロンプトは、コマンドスイッチとして選択したスイッチによって異なります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、**Return** キーを押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** キーを押してください。

ステップ 7 セットアッププログラムの質問に回答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (**n** は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されることに注意してください。

ステップ 8 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 9 スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** キーを押します (要求された場合)。

ステップ 10 クラスタに名前を指定し、**Return** キーを押します (要求された場合)。

クラスタ名には 1 ~ 31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 11 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 12 表示された情報が正しい場合は、**Y** を入力し、**Return** キーを押します。

情報に誤りがある場合には、**N** を入力し、**Return** キーを押して、ステップ 9 からやり直します。

ステップ 13 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 14 クラスタ メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

クラスタ メンバー スイッチとの接続の回復

構成によっては、コマンドスイッチとメンバー スイッチ間の接続を維持できない場合があります。メンバーに対する管理接続を維持できなくなった場合で、かつ、メンバー スイッチが正常にパケットを転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバー スイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、ネットワーク ポートとして定義されたポートを介してコマンドスイッチに接続することはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバー スイッチは、同じ管理 VLAN に所属するポートを介してコマンドスイッチに接続する必要があります。
- セキュア ポートを介してコマンドスイッチに接続するメンバー スイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度 (10 Mbps、100 Mbps、および Small Form-Factor Pluggable [SFP] モジュール ポート以外の 1000 Mbps) およびデュプレックス (半二重または全二重) に関するスイッチの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートが自動ネゴシエーション モードに設定されており、接続ポートが自動ネゴシエーションを指定せずに全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両端のポートに自動ネゴシエーションを実行させます。
- 接続の両端で、ポートの速度およびデュプレックス パラメータを手動設定します。



(注)

リモート デバイスが自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定が一致するように設定します。速度パラメータは、接続ポートが自動ネゴシエーションを行わない場合でも、自動調整が可能です。

PoE スイッチ ポートのトラブルシューティング

ここでは、Power over Ethernet (PoE; イーサネット経由の電源供給) ポートのトラブルシューティングについて説明します。

電力喪失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電装置（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは `errdisable` ステートになることがあります。`errdisable` ステートから回復するには、`shutdown` インターフェイス コンフィギュレーション コマンドを入力してから、`no shutdown` インターフェイス コマンドを入力します。スイッチで自動回復を設定し、`errdisable` ステートから回復することもできます。`errdisable recovery cause loopback` および `errdisable recovery interval seconds` グローバル コンフィギュレーション コマンドは、指定した期間が経過したあと自動的にインターフェイスを `errdisable` ステートから復帰させます。

このリリースのコマンド リファレンスに記載されている次のコマンドを使用すると、PoE ポート ステータスをモニタできます。

- `show controllers power inline` 特権 EXEC コマンド
- `show power inline` 特権 EXEC コマンド
- `debug ilpower` 特権 EXEC コマンド

不正リンクアップによるポート障害

シスコ受電装置をポートに接続し、`power inline never` インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンクアップが発生し、ポートが `errdisable` ステートになることがあります。ポートを `errdisable` ステートから修正するには、`shutdown` および `no shutdown` インターフェイス コンフィギュレーション コマンドを入力します。

`power inline never` コマンドで設定したポートにシスコ受電装置を接続しないでください。

SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および Cyclic Redundancy Check (CRC; 巡回冗長検査) が格納されたシリアル EEPROM (電氣的に消去可能でプログラミング可能な ROM) を備えています。スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを `errdisable` ステートにします。



(注)

セキュリティ エラー メッセージは、`GBIC_SECURITY` ファシリティを参照します。このスイッチは、SFP モジュールをサポートしていますが、GBIC (ギガビット インターフェイス コンバータ) モジュールはサポートしていません。エラー メッセージ テキストは、GBIC インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、`errdisable recovery cause gbic-invalid` グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、`errdisable` ステートから回復するタイム インターバルを入力します。このタイム インターバルが経過すると、スイッチは `errdisable` ステートからインターフェイスを復帰させ、操作を再実行します。`errdisable recovery` コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

`show interfaces transceiver` 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンドリファレンスに記載された `show interfaces transceiver` コマンドの説明を参照してください。

温度のモニタリング

Catalyst 3750G-48TS、3750G-48PS、3750G-24TS-1U、3750G-24PS の各スイッチでは、温度状態をモニタします。スイッチでは温度情報が使用されてファンも制御されます。

温度の値、状態、しきい値を表示するには、`show env temperature status` 特権 EXEC コマンドを使用します。温度の値は、スイッチ内の温度であり、外部の温度ではありません。`system env temperature threshold yellow value` グローバル コンフィギュレーション コマンドを使用してイエローのしきい値レベル（摂氏）のみを設定し、イエローのしきい値およびレッドのしきい値の差を設定できます。グリーンまたはレッドのしきい値を設定することはできません。詳細については、このリリースのコマンドリファレンスを参照してください。

ping の使用

ここでは、次の情報について説明します。

- 「ping の概要」(P.49-15)
- 「ping の実行」(P.49-16)

ping の概要

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答 (*hostname* が存在する) は、ネットワーク トラフィックにもよりますが、1 ~ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返ってきます。
- ホスト不明：ホストが存在しない場合、*unknown host* メッセージが返ってきます。
- 宛先に到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返ってきます。
- ネットワークまたはホストに到達不能：ルート テーブルにホストまたはネットワークに関するエントリがない場合、*network or host unreachable* メッセージが返ってきます。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。詳細は、第 38 章「IP ユニキャスト ルーティングの設定」を参照してください。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。IP ルーティングをイネーブルにする場合、または設定する必要がある場合は、第 38 章「IP ユニキャスト ルーティングの設定」を参照してください。

スイッチからネットワーク上の別のデバイスに ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
<code>ping ip host address</code>	IP またはホスト名やネットワーク アドレスを指定してリモートホストへ ping を実行します。



(注) ping コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 49-1 で、ping の文字出力について説明します。

表 49-1 ping の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス (デフォルトでは **Ctrl-^ X**) を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから離し、そのあと X キーを押します。

レイヤ 2 traceroute の使用

ここでは、次の情報について説明します。

- 「レイヤ 2 traceroute の概要」 (P.49-17)
- 「使用時の注意事項」 (P.49-17)
- 「物理パスの表示」 (P.49-18)

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 traceroute はユニキャスト送信元および宛先 MAC アドレスのみをサポートします。パス内にあるスイッチの MAC アドレス テーブルを使用してパスを識別します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパスで検出すると、スイッチはレイヤ 2 トレース クエリーを送信し続けてタイムアウトにしてしまいます。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

使用時の注意事項

レイヤ 2 traceroute の使用上の注意事項を次に示します。

- Cisco Discovery Protocol (CDP; シスコ検出プロトコル) がネットワーク上のすべてのデバイスでイネーブルでなければなりません。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。
レイヤ 2 traceroute をサポートするスイッチの一覧については、「使用時の注意事項」 (P.49-17) を参照してください。物理パス内のデバイスが CDP に対してトランスペアレントな場合、スイッチはこれらのデバイスを通るパスを識別できません。CDP をイネーブルにする場合の詳細については、第 27 章「CDP の設定」を参照してください。
- スイッチは、**ping** 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別可能なホップ数は 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にはないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。異なる VLAN にある送信元および宛先 MAC アドレスを指定する場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定する場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属している場合、送信元および宛先 MAC アドレスの両方が属する VLAN を指定しなければなりません。VLAN が指定されない場合、パスは識別されず、エラー メッセージが表示されます。

- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して、IP アドレスを対応する MAC アドレスおよび VLAN ID に関連付けます。
 - ARP エントリが指定した IP アドレスにある場合、スイッチは関連する MAC アドレスを使用して物理パスを識別します。
 - ARP エントリが存在しない場合、スイッチは ARP クエリーを送信して IP アドレスを解決しようとします。IP アドレスが解決されない場合、パスは識別されず、エラー メッセージが表示されます。
- 複数のデバイスがハブを介して 1 つのポートに接続されている場合 (たとえば複数の CDP ネイバーがポートで検出された場合)、レイヤ 2 **traceroute** 機能はサポートされません。複数の CDP ネイバーが 1 つのポート上で検出されると、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。
- この機能は、トークンリング VLAN 上ではサポートされません。

物理パスの表示

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを表示できます。

- traceroute mac** [**interface interface-id**] {*source-mac-address*} [**interface interface-id**] {*destination-mac-address*} [**vlan vlan-id**] [**detail**]
- traceroute mac ip** {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

詳細については、このリリースのコマンド リファレンスを参照してください。

IP traceroute の使用

ここでは、次の情報について説明します。

- 「[IP traceroute の概要](#)」 (P.49-18)
- 「[IP traceroute の実行](#)」 (P.49-19)

IP traceroute の概要

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク レイヤ (レイヤ 3) デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。スイッチを **traceroute** の宛先とすると、スイッチは、**traceroute** の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、**traceroute** の出力に中間スイッチは表示されません。ただし、中間スイッチが、特定の packets をルーティングするマルチレイヤスイッチの場合、中間スイッチは **traceroute** の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの TTL (Time To Live; 存続可能時間) フィールドを使用して、ルータおよびサーバで特定のリターンメッセージが生成されるようにします。**traceroute** の実行は、User Datagram Protocol (UDP; ユーザ データグラム プロトコル) を、[TTL] フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) **time-to-live-exceeded** メッセージを送信元に送信します。**traceroute** は、ICMP **time-to-live-exceeded** メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、**traceroute** は TTL 値が 2 の UDP パケットを送信します。1 番目のルータは、[TTL] フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番目のルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、**time-to-live-exceeded** メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで (または TTL の最大値に達するまで) TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、**traceroute** は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛のデータグラムを受信すると、送信元に ICMP **ポート到達不能** エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意味します。

IP traceroute の実行

ネットワーク上でパケットが通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip host	ネットワーク上でパケットが通過するパスを追跡します。



(注) **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

 0 172.2.52.1 0 msec 0 msec 4 msec
 1 172.2.1.203 12 msec 8 msec 0 msec
 2 171.9.16.6 4 msec 0 msec 0 msec
 3 171.9.4.5 0 msec 4 msec 0 msec
 4 171.9.121.34 0 msec 4 msec 4 msec
 5 171.9.15.9 120 msec 132 msec 128 msec
 6 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

ディスプレイには、送信される 3 つのプロープごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ時間 (ミリ秒単位) が表示されます。

表 49-2 traceroute の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	ソース クエンチ。
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは **Ctrl-^ X**）を入力してください。**Ctrl** キー、**Shift** キー、および **6** キーを同時に押してから離し、そのあと **X** キーを押します。

TDR の使用

ここでは、次の情報について説明します。

- 「[TDR の概要](#)」 (P.49-20)
- 「[TDR の実行および結果の表示](#)」 (P.49-21)

TDR の概要

Time Domain Reflector (TDR) 機能を使用してケーブル配線の問題を診断して解決できます。TDR 稼動時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は 10/100/100 の銅線イーサネット ポート上でのみサポートされます。10/100 ポート、10 ギガビット モジュール ポート、または SFP モジュール ポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイストペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行および結果の表示

インターフェイス上で TDR を実行する場合は、スタック マスターまたはスタック メンバーで実行できます。

TDR を実行する場合、**test cable-diagnostics tdr interface interface-id** 特権 EXEC コマンドを実行します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface interface-id** 特権 EXEC コマンドを実行します。出力フィールドの説明に関しては、このリリースに対応するコマンドリファレンスを参照してください。

debug コマンドの使用

ここでは、**debug** コマンドを使用してインターネットワーキングの問題を診断し、解決する方法について説明します。

- 「特定機能に関するデバッグのイネーブル化」(P.49-21)
- 「システム全体診断のイネーブル化」(P.49-22)
- 「デバッグおよびエラー メッセージ出力のリダイレクト」(P.49-22)



注意

デバッグ出力には、CPU プロセスで高いプライオリティが与えられるので、システムが使用不能になる可能性があります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間にデバッグを実行すると、**debug** コマンドの処理の負担によってシステム使用が影響を受ける可能性が少なくなります。



(注)

特定の **debug** コマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスを参照してください。

特定機能に関するデバッグのイネーブル化

デバッグをイネーブルにすると、スタック マスターでのみデバッグがイネーブルになります。スタック メンバーでのデバッグをイネーブルにするには、**session switch-number** 特権 EXEC コマンドを使用して、スタック メンバーからセッションを開始する必要があります。そのあと、スタック メンバーのコマンドライン プロンプトに **debug** を入力します。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。たとえば、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) に対するデバッグをイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug span-session
```

スイッチは **no** 形式のコマンドが入力されるまで、出力を生成し続けます。

debug コマンドをイネーブルにしても、出力が表示されない場合は、次の状況が考えられます。

- モニタするトラフィック タイプを生成するようにスイッチが正しく設定されていない可能性があります。**show running-config** コマンドを使用して、設定を確認してください。
- スイッチが正しく設定されていても、デバッグがイネーブルである間にモニタすべきタイプのトラフィックを生成しないことがあります。デバッグする機能によっては、TCP/IP の **ping** コマンドなどを使用すると、ネットワーク トラフィックを生成できます。

SPAN のデバッグをディセーブルにする場合は、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

また、特権 EXEC モードで **undebug** 形式のコマンドを入力することもできます。

```
Switch# undebug span-session
```

各デバッグ オプションのステータスを表示するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体診断のイネーブル化

システム全体診断をイネーブルにするには、特権 EXEC モードで、次のコマンドを入力します。

```
Switch# debug all
```



注意

デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、コンソール ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

出力先に指定できるのは、コンソール、仮想端末、内部バッファ、および Syslog サーバが稼働している UNIX ホストです。Syslog フォーマットは、4.3 Berkeley Standard Distribution (BSD) UNIX およびそのバリエーションと互換性があります。



(注)

デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。コンソールでメッセージ ロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージ ロギングを行うと、オーバーヘッドが小さくなります。Syslog サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

スタック メンバーによって生成されたシステム エラー メッセージは、スタック マスターによってすべてのスタック メンバーに表示されます。Syslog はスタック マスターに置かれます。



(注) スタック マスターに障害が発生しても Syslog が失われないように、Syslog をフラッシュ メモリに保存してください。

システム メッセージ ログイングの詳細については、第 32 章「システム メッセージ ログイングの設定」を参照してください。

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。



(注) **show platform forward** コマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスを参照してください。

このコマンドで出力される情報のほとんどは、主に、スイッチの **Application Specific Integrated Circuit (ASIC; 特定用途向け集積回路)** に関する詳細情報を使用するテクニカル サポート 担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 のポート 1 に入るパケットが、不明な MAC アドレスにアドレス指定されている場合の **show platform forward** コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべてのポートに対してフラグディングされなければなりません。

```
Switch# show platform forward gigabitethernet01/01/01 vlan 5 1.1.1 2.2.2 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
  Lookup                Key-Used                Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000    01FFA  03000000
L2Local  80_00050002_00020002-00_00000000_00000000        00C71  0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005
```

```
=====  
Egress:Asic 2, switch 1  
Output Packets:
```

```
-----  
Packet 1  
  Lookup                Key-Used                Index-Hit  A-Data  
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000
```

```
Port      Vlan      SrcMac          DstMac          Cos  Dscpv  
Gi1/0/1   0005  0001.0001.0001  0002.0002.0002
```

```
-----  
Packet 2  
  Lookup                Key-Used                Index-Hit  A-Data  
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000
```

```
Port      Vlan      SrcMac          DstMac          Cos  Dscpv  
Gi1/0/2   0005  0001.0001.0001  0002.0002.0002
```

show platform forward コマンドの使用

```
-----
<output truncated>
-----
```

```
Packet 10
  Lookup                               Key-Used                               Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2
```

次に、VLAN 5 のポート 1 に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送信する場合の出力例を示します。パケットは、アドレスを学習したポートから転送する必要があります。

```
Switch# show platform forward gigabitethernet01/01/01 vlan 5 1.1.1 0009.43a8.0145 ip
13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
  Lookup                               Key-Used                               Index-Hit  A-Data
InptACL 40_0D020202_0D010101-00_40000014_000A0000  01FFA  03000000
L2Local 80_00050009_43A80145-00_00000000_00000000  00086  02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003
```

```
=====
Egress:Asic 3, switch 1
Output Packets:
```

```
-----
Packet 1
  Lookup                               Key-Used                               Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000

Port          Vlan      SrcMac          DstMac          Cos  Dscpv
interface-id  0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが不明である場合の出力例を示します。デフォルトルートが設定されていないため、パケットは廃棄されます。

```
Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
  Lookup                               Key-Used                               Index-Hit  A-Data
InptACL 40_0D020202_0D010101-00_41000014_000A0000  01FFA  03000000
L3Local 00_00000000_00000000-90_00001400_0D020202  010F0  01880290
L3Scndr 12_0D020202_0D010101-00_40000014_000A0000  034E0  000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。パケットはルーティング テーブルの指定どおりに転送されます。

```
Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
  Lookup                               Key-Used                               Index-Hit  A-Data
```



```

InptACL 40_10010A05_0A010505-00_41000014_000A0000 01FFA 03000000
L3Local 00_00000000_00000000-90_00001400_10010A05 010F0 01880290
L3Scndr 12_10010A05_0A010505-00_40000014_000A0000 01D28 30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

=====
Egress:Asic 3, switch 1
Output Packets:

-----
Packet 1
  Lookup          Key-Used          Index-Hit  A-Data
OutputACL 50_10010A05_0A010505-00_40000014_000A0000 01FFE 03000000

Port      Vlan      SrcMac          DstMac      Cos  Dscpv
Gi1/0/2   0007     XXXX.XXXX.0246 0009.43A8.0147

```

crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときに使用する情報が保存されます。スイッチは障害発生時にその情報をコンソールに書き込みます。スイッチは次の 2 つのタイプの crashinfo ファイルを作成します。

- 基本 crashinfo ファイル：障害発生後に Cisco IOS イメージを起動すると、スイッチが自動的にこのファイルを作成します。
- 拡張 crashinfo ファイル：システムに障害が発生すると、スイッチが自動的にこのファイルを作成します。

基本 crashinfo ファイル

この基本ファイルに保存される情報は、障害が発生した Cisco IOS イメージの名前とバージョン、プロセッサ レジスタのリスト、およびその他のスイッチ固有の情報です。show tech-support 特権 EXEC コマンドを使用することによって、この情報をシスコのテクニカル サポート担当者に提供できます。

基本 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。
flash:/crashinfo/

ファイル名は crashinfo_n になります。n には一連の番号が入ります。

新しい crashinfo ファイルが作成されるたびに、前のシーケンス番号より大きいシーケンス番号が使用されるので、シーケンス番号が最大のファイルに、最新の障害が記述されています。タイムスタンプではなく、バージョン番号を使用するのは、スイッチにリアルタイム クロックが組み込まれていないからです。ファイル作成時にシステムが使用するファイル名を変更することはできません。ただし、ファイルが作成されたあとに、rename 特権 EXEC コマンドを使用して名前を変更することもできますが、show stacks または show tech-support 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。delete 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示する場合は、show stacks または show tech-support 特権 EXEC コマンドを使用します。more 特権 EXEC コマンド、copy 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、ファイルにアクセスすることもできます。

拡張 crashinfo ファイル

システムに障害が発生すると、スイッチが拡張 **crashinfo** ファイルを作成します。拡張ファイルに保存される情報は、スイッチの障害となった原因を特定するのに役立つ追加情報です。このファイルに手動でアクセスし、**more** または **copy** 特権 EXEC コマンドを使用すると、シスコのテクニカル サポート担当者にこの情報を提供できます。

拡張 **crashinfo** ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。
flash:/crashinfo_ext/

ファイル名は **crashinfo_ext_n** になります。*n* には一連の番号が入ります。

no exception crashinfo グローバル コンフィギュレーション コマンドを使用すると、スイッチが拡張 **crashinfo** ファイルを作成しないように設定できます。

トラブルシューティングの表

次の表は、Cisco.com にあるトラブルシューティング ドキュメントの内容を抜粋してまとめたものです。

- 「[CPU 使用率のトラブルシューティング](#)」(P.-26)
- 「[Power over Ethernet \(PoE\) のトラブルシューティング](#)」(P.-28)
- 「[StackWise のトラブルシューティング](#)」(P.-31)

CPU 使用率のトラブルシューティング

ここでは、CPU の負荷が高くなることによって発生する可能性がある症状を示し、CPU 使用率の問題を確認する方法について説明します。表 49-3 に、特定できる主な CPU 使用率の問題を示します。この表には、考えられる原因および対処法と Cisco.com の「[Troubleshooting High CPU Utilization](#)」へのリンクが記載されています。

CPU 使用率が高い場合に発生する可能性のある症状

CPU 使用率が非常に高くなることで次のような症状が発生する可能性があります。これらの症状は別の原因によっても発生する場合があります。ことに注意してください。

- スパニング ツリー トポロジの変更
- 通信が失われたことによる EtherChannel リンクのダウン
- 管理要求 (ICMP ping、SNMP タイムアウト、低速の Telnet または SSH セッション) に応答しない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA エラー
- スイッチが要求を転送しない場合や要求に応答しない場合の DHCP エラーまたは IEEE 802.1x エラー

レイヤ 3 スイッチ：

- パケットの廃棄、またはソフトウェアでルーティングされているパケットの遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

問題と原因の確認

CPU の高使用率が問題であるかどうかを判断するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目の下線の付いた情報に注意してください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、通常の CPU 使用率を示しています。この出力から、過去 5 秒間の使用率が **8%/0%** だったことがわかります。この意味は次のとおりです。

- 合計 CPU 使用率（Cisco IOS プロセスの実行時間と割り込み処理時間の両方を含む）は 8%。
- 割り込み処理に費やされた時間は 0%。

表 49-3 CPU 使用率の問題のトラブルシューティング

問題の種類	原因	対処法
割り込みの割合が合計 CPU 使用率と同じくらいの高さになっている。	CPU がネットワークから受信しているパケットが多すぎる。	ネットワーク パケットの送信元を確認して、そのフローを止めるかスイッチの設定を変更する。「 Analyzing Network Traffic 」を参照してください。
合計 CPU 使用率は 50% を超えているが、割り込みに費やされている時間はごくわずかになっている。	1 つ以上の Cisco IOS プロセスによって大量の CPU 時間が消費されている。この状況は、一般に、プロセスをアクティブにしたイベントによって引き起こされます。	異常なイベントを見つけて根本原因を解決する。「 Debugging Active Processes 」を参照してください。

CPU 使用率の詳細と、使用率の問題のトラブルシューティング方法の詳細については、Cisco.com で「[Troubleshooting High CPU Utilization](#)」を参照してください。

Power over Ethernet (PoE) のトラブルシューティング

図 49-1 PoE のトラブルシューティング シナリオ

症状または問題	考えられる原因および解決方法
<p>PoE が機能しないポートが 1 つだけある。</p> <p>問題が発生しているスイッチ ポートは 1 つだけで、PoE 装置も非 PoE 装置も他のポートでは動作するのにそのポートでは動作しません。</p>	<p>受電装置が他の PoE ポートで動作することを確認します。</p> <p>show run、show interface status、または show power inline detail のいずれかのユーザ EXEC コマンドを使用して、ポートがシャットダウンしたり errdisable になったりしていないことを確認します。</p> <p>(注) IEEE の仕様ではオプションですが、ほとんどのスイッチでは、ポートがシャットダウンするとポートの電源がオフになります。</p> <p>受電装置とスイッチ ポート間のイーサネット ケーブルに問題がないことを確認します。問題がないことがわかっている非 PoE イーサネット装置をそのイーサネット ケーブルに接続し、受電装置でリンクが確立され、他のホストとトラフィックが交換されることを確認します。</p> <p>スイッチの前面パネルから受電装置までのケーブルの長さの合計が 100 m 以内であることを確認します。</p> <p>スイッチ ポートからイーサネット ケーブルを取り外し、短いイーサネット ケーブルを使って、問題がないことがわかっているイーサネット装置をスイッチの前面パネル（パッチパネルではなく）で直接そのポートに接続します。イーサネット リンクが確立され、他のホストとトラフィックが交換されることを確認するか、ポート VLAN の SVI に ping を実行します。次に、そのポートに受電装置を接続して、電源が入るかどうかを確認します。</p> <p>パッチコードでスイッチ ポートに接続すると受電装置の電源が入らない場合は、接続されている受電装置の数とスイッチのパワー バジェット（利用可能な PoE）を比較します。利用可能な電力量を確認するには、show inline power コマンドと show inline power detail コマンドを使用します。</p> <p>詳細については、Cisco.com で「No PoE On One Port」を参照してください。</p>

図 49-1 PoE のトラブルシューティング シナリオ (続き)

症状または問題	考えられる原因および解決方法
<p>すべてのポートまたはポートのグループで PoE が機能しない。</p> <p>すべてのスイッチ ポートで問題が発生していて、どのポートでも非受電イーサネット装置はイーサネットリンクを確立できず、PoE 装置は電源が入りません。</p>	<p>電源関連のアラームが連続的または断続的に発生したり、繰り返し発生したりする場合は、電源装置を交換するか (Field-Replaceable Unit の場合)、スイッチを交換します (それ以外の場合)。</p> <p>すべてのポートではなく、連続するポートのグループで問題が発生している場合は、電源装置ではなく、スイッチの PoE レギュレータに問題がある可能性があります。</p> <p>show log 特権 EXEC コマンドを使用して、PoE の状態やステータスの変更に関するアラームやシステム メッセージを確認します。</p> <p>アラームがない場合は、show interface status コマンドを使用して、ポートがシャットダウンしたり errdisable になったりしていないかどうかを確認します。ポートが errdisable になっている場合は、インターフェイス コンフィギュレーション コマンドの shut と no shut を使用してポートを再度イネーブルにします。</p> <p>特権 EXEC コマンドの show env power と show power inline を使用して、PoE のステータスとパワー バジェット (利用可能な PoE) を確認します。</p> <p>実行コンフィギュレーションを調べて、ポートで power inline never が設定されていないことを確認します。</p> <p>非受電イーサネット装置を直接スイッチ ポートに接続します。短いパッチコードのみを使用します。既存のディストリビューション ケーブルは使用しないでください。インターフェイス コンフィギュレーション コマンドの shut と no shut を入力して、イーサネットリンクが確立されることを確認します。この接続で問題が発生しない場合は、短いパッチコードを使用してこのポートに受電装置を接続し、電源が入るかどうかを確認します。電源が入る場合は、中間のパッチパネルがすべて正しく接続されていることを確認します。</p> <p>スイッチ ポートのイーサネット ケーブルを、1 つを除いてすべて取り外します。短いパッチコードを使用して、受電装置を 1 つの PoE ポートだけに接続します。受電装置に必要な電力が、スイッチ ポートで供給可能な電力を超えていないことを確認します。</p> <p>show power inline 特権 EXEC コマンドを使用して、ポートがシャットダウンしていないときに受電装置に電力が供給されるかどうかを確認します。または、受電装置を監視して、電源が入るかどうかを確認します。</p> <p>スイッチに接続されている受電装置が 1 つだけなら電源が入る場合は、残りのポートでインターフェイス コンフィギュレーション コマンドの shut と no shut を入力し、イーサネット ケーブルを一度に 1 つずつ、再度スイッチの PoE ポートに接続します。特権 EXEC コマンドの show interface status と show power inline を使用して、インライン電力の統計とポート ステータスをモニタします。</p> <p>まだどのポートでも PoE が機能しない場合は、電源装置の PoE セクションでヒューズが開いている可能性があります。その場合、通常はアラームが生成されます。もう一度ログを調べて、以前にシステム メッセージによってアラームが報告されていないかどうかを確認します。</p> <p>詳細については、Cisco.com で「No PoE On Any Port or a Group of Ports」を確認してください。</p>

図 49-1 PoE のトラブルシューティング シナリオ (続き)

症状または問題	考えられる原因および解決方法
<p>Cisco IP Phone が切断またはリセットされる。</p> <p>正常に動作していたシスコの電話機やワイヤレス アクセス ポイントが、断続的にリロードされたり PoE から切断されたりします。</p>	<p>スイッチから受電装置までの電気系統の接続をすべて確認します。不安定な接続があると、電力が遮断されて、受電装置で異常な動作（不規則な電力供給によってデバイスが切断されたりリロードされたりするなど）が発生する原因になります。</p> <p>スイッチ ポートから受電装置までのケーブルの長さが 100 m 以内であることを確認します。</p> <p>切断が発生するときのスイッチの場所の電気的環境の変化や受電装置の状態を確認します。</p> <p>切断と同時にエラー メッセージが表示されていないかどうかを確認します。 show log 特権 EXEC コマンドを使用して、エラー メッセージを確認します。</p> <p>リロードが発生する直前に IP 電話が Call Manager にアクセスできなくなっていないかどうかを確認します（その場合は、PoE の問題ではなくネットワークの問題である可能性があります）。</p> <p>受電装置を非 PoE 装置に置き換えて、デバイスが正常に動作するかどうかを確認します。非 PoE 装置でリンクの問題が発生したり、高い確率でエラーが発生したりする場合は、スイッチ ポートと受電装置の間のケーブル接続に問題がある可能性があります。</p> <p>詳細については、Cisco.com で「Cisco Phone Disconnects or Resets」を参照してください。</p>
<p>他社製の受電装置がシスコの PoE スイッチで動作しない。</p> <p>他社製の受電装置をシスコの PoE スイッチに接続しても電源が入らなったり、入ってもすぐに切れてしまったりします。非 PoE 装置は正常に動作します。</p>	<p>show power inline コマンドを使用して、スイッチのパワー バジェット（利用可能な PoE）が受電装置を接続する前または後に使い尽くされていないかどうかを確認します。受電装置を接続する前に、利用可能な電力が十分かどうかを確認してください。</p> <p>show interface status コマンドを使用して、接続した受電装置がスイッチで検出されているかどうかを確認します。</p> <p>show log コマンドを使用して、ポートの過電流状態を報告しているシステム メッセージを確認します。正確な症状を特定するために、最初に受電装置の電源が入ってから切断されているかどうかを確認します。その場合は、最初に流れ込む電流（突入電流）がポートの電流制限のしきい値を超えている可能性があります。</p> <p>詳細については、Cisco.com で「Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch」を参照してください。</p>

StackWise のトラブルシューティング

表 49-4 スイッチ スタックのトラブルシューティング シナリオ

症状または問題	問題の確認方法	考えられる原因および解決方法
スイッチ スタックの問題の一般的なトラブルシューティング	このマニュアルを読む。	「 Troubleshooting Switch Stacks 」で、問題の解決方法とチュートリアルを確認する。
スイッチがスタックに参加できない	show switch 特権 EXEC コマンドを入力する。	スタック メンバーと新しいスイッチの Cisco IOS のバージョンに互換性がない (「 Confirming Cisco IOS Versions 」を参照)。
	show version ユーザ EXEC コマンドを入力する。	Catalyst 3750-E スイッチのライセンス レベルに互換性がない (「 Verifying Software License Compatibility 」を参照)。
	show platform stack-manager all コマンドを入力する。	スタック メンバーと新しいスイッチの Cisco IOS のバージョン番号に互換性がない (「 Confirming Cisco IOS Versions 」を参照)。
	ケーブルと接続を入念に確認する。	StackWise ケーブルの信頼性または接続の不備の問題 (「 Testing StackWise Cables and Interfaces 」を参照)。
	show sdm prefer コマンドを入力する。	スイッチをスタックに追加する前に他のアプリケーションで使用していた場合は、設定 (SDM テンプレート) の不一致。スタック メンバーと新しいスイッチの IOS のバージョンに互換性がない (「 Configuration Mismatch 」を参照)。
StackWise ポートのアップ/ダウンの状態が頻繁に変更されたりすばやく切り替わったりする (フラッピング)	エラー メッセージによってスタック リングの問題が報告される。トラフィックが中断されている可能性があります。	StackWise のケーブル接続またはインターフェイスの信頼性の問題 (「 StackWise Port Flapping 」を参照)。
スイッチ メンバー ポートがアクティブにならない	show switch detail 特権 EXEC コマンドを入力する。	StackWise のケーブル接続またはインターフェイスの信頼性の問題 (「 StackWise Port Flapping 」を参照)。
スタック リングの帯域幅が減少している、またはスイッチ ポート間やスタック内のスイッチ間のスループットが遅い。	show switch stack-ring speed ユーザ EXEC コマンドを入力する。	StackWise ケーブル接続とスイッチ シャーシのコネクタが正しく接続されていない (「 Testing StackWise Cables and Interfaces 」を参照)。
	show switch detail ユーザ EXEC コマンドを入力して、問題の原因になっているスタック ケーブルまたは接続を特定する。	StackWise ケーブルの不具合または欠損 (「 Testing StackWise Cables and Interfaces 」を参照)。
	<ul style="list-style-type: none"> StackWise ケーブル コネクタの掛け止めネジを確認する。 show switch 特権 EXEC コマンドを入力して、新しいスイッチについて、Ready、Progressing、Provisioned のどれが表示されるかを確認する。 	<ul style="list-style-type: none"> 掛け止めネジを緩めるか、きつく締める (「Verifying StackWise Cable Connections」を参照)。 スタック メンバーのステータスをチェックする (「Verifying StackWise Cable Connections」を参照)。

表 49-4 スイッチ スタックのトラブルシューティング シナリオ (続き)

症状または問題	問題の確認方法	考えられる原因および解決方法
1 つ以上のスイッチのポートの番号付けが正しくない、または変更されている。	<code>show switch detail</code> ユーザ EXEC コマンドを入力する。	2 つの別のスタックを作成しているスタックメンバーから複数の StackWise ケーブルが取り外されている (「Stack Master Election and Port Number Assignment」 を参照)。
スタック リングのトラフィックスループットが遅い	スイッチ インターフェイスをテストする。	StackWise スイッチ インターフェイスの不具合。 (注) この問題を解決するにはスイッチを交換するしかありません。
スタック マスターの選択、スタックのマージ、または新しいスイッチのスタックへの参加の問題	スタック マスターの選択の規則を確認する。	現在のスタック マスターが再起動または切断された (「Stack Master is Rebooted or Disconnected」 を参照)。
	ポートの番号付けがオフになっているように見える。	ポートの番号付けを確認する (「Stack Master Election and Port Number Assignment」 を参照)。
	<code>show switch</code> 特権 EXEC コマンドを入力する。	状態メッセージを確認する (「Joining a Stack: Typical Sequence States and Rules」 を参照)。
スタック メンバーをアップグレードする必要がある。	スタック メンバーで実行されている Cisco IOS ソフトウェアのメジャーバージョン番号またはマイナーバージョン番号が違っている。	StackWise スイッチ インターフェイスまたは StackWise ケーブルの不具合 (「Quick-and-Easy Catalyst 3750 and Catalyst 3750E Switch Stack Upgrades」 を参照)。
StackWise リンク接続の問題	LED の動作を確認する。	スタックですべての帯域幅が使用されていない (「Verifying StackWise Link Connections Using LEDs」 を参照)。



CHAPTER 50

オンライン診断の設定

この章では、Catalyst 3750 スイッチでオンライン診断を設定する方法について説明します。



(注)

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

http://www.cisco.com/en/US/products/hw/switches/ps5023/prod_command_reference_list.html

この章で説明する内容は、次のとおりです。

- 「オンライン診断の概要」 (P.50-1)
- 「オンライン診断テストの実行」 (P.50-3)

オンライン診断の概要

オンライン診断では、スイッチが稼働中のネットワークに接続されている間にスイッチのハードウェア機能のテストと検証を実行できます。

オンライン診断には、個別のハードウェア コンポーネントをチェックし、データ パスおよび制御信号を検証するパケット スイッチング テストが含まれています。

オンライン診断では、次の領域での問題を検出できます。

- ハードウェア コンポーネント
- インターフェイス (イーサネット ポートなど)
- はんだ接合

オンライン診断は、オンデマンド診断、スケジュール診断、またはヘルス モニタリング診断に分類されます。オンデマンド診断は、CLI (コマンドライン インターフェイス) から実行します。スケジュール診断は、ユーザが指定するタイム インターバルで実行するか、またはスイッチが稼働ネットワークに接続するように指定された時間に実行します。ヘルス モニタリングはバックグラウンドで実行します。

オンライン診断のスケジューリング

特定のスイッチについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。スケジュールを削除するには、このコマンドの **no** 形式を使用します。

オンライン診断をスケジューリングにするには、グローバル コンフィギュレーション モードで、次のコマンドを使用します。

コマンド	目的
diagnostic schedule switch num test { <i>test_id</i> <i>test_id_range</i> all basic non-disruptive } { daily <i>hh:mm</i> on <i>mm dd yyyy hh:mm</i> } weekly <i>day_of_week hh:mm</i> }	特定日時のオンデマンド診断テスト、テストの実行回数（反復）、エラーを検出したときに実行する処理をスケジューリングします。

次に、特定のスイッチに対して、特定の日にオンデマンド診断テストを実行するようにスケジューリングする例を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 on january 3 2006 23:32
```

次に、特定のスイッチに対して、毎週一定の時間にオンデマンド診断テストを実行するようにスケジューリングする例を示します。

```
Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly friday 09:23
```

ヘルス モニタリング診断の設定

スイッチが稼働中のネットワークに接続している間に、指定したスイッチでヘルス モニタリング診断テストを設定できます。ヘルス モニタリング診断テストの実行間隔と、テストに障害が発生したときにシステム メッセージを生成するかどうか、あるいは各テストをイネーブルにするかディセーブルにするかを設定できます。テストをディセーブルにするには、このコマンドの **no** 形式を使用します。

ヘルス モニタリング診断を設定するには、グローバル コンフィギュレーション モードで、次のコマンドを使用します。

コマンド	目的
diagnostic monitor interval switch num test { <i>test_id</i> <i>test_id_range</i> all } <i>hour:mm:ss milliseconds day</i>	指定したスイッチに対して指定したテストのヘルス モニタリングの間隔を設定します。モニタリングは、デフォルトではディセーブルに設定されています。
diagnostic monitor syslog	ヘルス モニタリング テストに失敗した場合の syslog メッセージの生成をイネーブルにします。syslog は、デフォルトではディセーブルに設定されています。
diagnostic monitor threshold switch num test { <i>test_id</i> <i>test_id_range</i> all } failure count <i>count</i>	モニタリング テストの障害しきい値を設定します。モニタリングは、デフォルトではディセーブルに設定されています。

間隔をデフォルト値またはゼロに変更するには、**no diagnostic monitor interval switch {num} test {test-id | test-id-range | all}** グローバル コンフィギュレーション コマンドを使用します。ヘルス モニタリング テストに失敗した場合の **syslog** メッセージの生成をディセーブルにするには、**no diagnostic monitor syslog** コマンドを使用します。障害しきい値を削除するには、**diagnostic monitor threshold switch num test {test_id | test_id_range | all} failure count** コマンドを使用します。

次に、2 分ごとに指定したテストを実行するように設定する例を示します。

```
Switch(config)# diagnostic monitor interval switch 1 test 1 00:02:00 0 1
```

次に、スイッチでのモニタリング テストの障害しきい値を設定する例を示します。

```
Switch(config)# diagnostic monitor threshold switch 1 test 1 failure count 50
```

次の例では、ヘルス モニタリング テストが失敗した場合に Syslog メッセージの生成をイネーブルにする方法を示します。

```
Switch(config)# diagnostic monitor syslog
```

オンライン診断テストの実行

オンライン診断を設定したあと、診断テストを開始したり、テスト結果を表示したりできます。また、各スイッチに設定されているテストの種類、およびすでに実行された診断テスト名を確認できます。

ここでは、オンライン診断テストの設定後に、実行する例を示します。

- 「オンライン診断テストの開始」 (P.50-3)
- 「オンライン診断テストおよびテスト結果の表示」 (P.50-4)

オンライン診断テストの開始

スイッチまたは各スイッチで実行する診断テストを設定したあと、**start** を使用して診断テストを開始できます。

オンライン診断テストを開始するには、グローバル コンフィギュレーション モードで、次のコマンドを使用します。

コマンド	目的
diagnostic start switch num test {test-id test-id-range all basic non-disruptive}	特定のスイッチで診断テストを開始します。

次に、特定のスイッチで診断テストを開始する例を示します。

```
Switch# diagnostic start switch 1 test 1
Switch#
06:27:50: %DIAG-6-TEST_RUNNING: Switch 1:Running TestPortAsicStackPortLoopback{ID=1} ...
(switch-1)
06:27:51: %DIAG-6-TEST_OK: Switch 1:TestPortAsicStackPortLoopback{ID=1} has completed
successfully (switch-1)
Switch#
```

次に、通常のシステム動作を中断させ、スイッチのスタック接続を切断してからスタックをリロードする診断テスト 2 をスイッチで実行する例を示します。

```
Switch# diagnostic start switch 1 test 2
Switch 1: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 1: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]: y
Switch#
16:43:29: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state DOWN
16:43:30: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 9 has changed to state DOWN
16:43:30: %STACKMGR-4-SWITCH_REMOVED: Switch 1 has been REMOVED from the stack
Switch#
16:44:35: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 2 has changed to state UP
```

```

16:44:37: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 2 has changed to state UP
16:44:45: %STACKMGR-4-SWITCH_ADDED: Switch 1 has been ADDED to the stack
16:45:00: %STACKMGR-5-SWITCH_READY: Switch 1 is READY
16:45:00: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state UP
16:45:00: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state UP
00:00:20: %STACKMGR-4-SWITCH_ADDED: Switch 1 has been ADDED to the stack (Switch-1)
00:00:20: %STACKMGR-4-SWITCH_ADDED: Switch 2 has been ADDED to the stack (Switch-1)
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan (Switch-1)
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console (Switch-1)
00:00:29: %STACKMGR-5-SWITCH_READY: Switch 2 is READY (Switch-1)
00:00:29: %STACKMGR-5-MASTER_READY: Master Switch 2 is READY (Switch-1)
00:00:30: %STACKMGR-5-SWITCH_READY: Switch 1 is READY (Switch-1)
00:00:30: %DIAG-6-TEST_RUNNING: Switch 1: Running TestPortAsicLoopback{ID=2} ...
(Switch-1)
00:00:30: %DIAG-6-TEST_OK: Switch 1: TestPortAsicLoopback{ID=2} has completed successfully
(Switch-1)

```

テストでスタック パーティションが発生する場合、次のメッセージが表示されます。

```

Switch 6: Running test(s) 2 will cause the switch under test to reload after completion of
the test list.
Switch 6: Running test(s) 2 will partition stack
Switch 6: Running test(s) 2 may disrupt normal system operation
Do you want to continue?[no]:

```

オンライン診断テストおよびテスト結果の表示

show コマンドを使用すると、特定のスイッチに設定されたオンライン診断テストの表示と、テスト結果の確認をすることができます。

スイッチに設定されている診断テストとテスト結果を表示するには、この特権 EXEC コマンドを使用します。

表 50-1 show diagnostic コマンド

コマンド	目的
show diagnostic content switch [num all]	スイッチに設定されたオンライン診断を表示します。
show diagnostic status	スイッチでテストが実行中かどうかを表示します。
show diagnostic result switch [num all] detail show diagnostic result switch [num all] test [test_id test_id_range all] [detail]	オンライン診断テスト結果を表示します。
show diagnostic schedule switch [num all]	オンライン診断テスト スケジュールを表示します。
show diagnostic post	POST の結果を表示します (show post コマンドと同様)。

次に、スイッチに設定されたオンライン診断を表示する例を示します。

```

Switch# show diagnostic content switch 3
Switch 3:
Diagnostics test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a health monitoring test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA

```

A/I - Monitoring is active / Monitoring is inactive
 R/* - Switch will reload after test list completion / NA
 P/* - will partition stack / NA

ID	Test Name	attributes	Test Interval day hh:mm:ss.ms	Thre- shold
1)	TestPortAsicStackPortLoopback	B*N***A**	000 00:01:00.00	n/a
2)	TestPortAsicLoopback	B*D*X**IR*	not configured	n/a
3)	TestPortAsicCam	B*D*X**IR*	not configured	n/a
4)	TestPortAsicRingLoopback	B*D*X**IR*	not configured	n/a
5)	TestMicRingLoopback	B*D*X**IR*	not configured	n/a
6)	TestPortAsicMem	B*D*X**IR*	not configured	n/a

次に、スイッチのオンライン診断結果を表示する例を示します。

```
Switch# show diagnostic resultswitch 1
Switch 1: SerialNo :
Overall diagnostic result: PASS
Test results: (. = Pass, F = Fail, U = Untested)
1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback -----> .
3) TestPortAsicCam -----> .
4) TestPortAsicRingLoopback -----> .
5) TestMicRingLoopback -----> .
6) TestPortAsicMem -----> .
```

次に、オンライン診断テストステータスを表示する例を示します。

```
Switch# show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
=====
Card  Description                               Current Running Test          Run by
-----
1                                           N/A                           N/A
2                                           TestPortAsicStackPortLoopback <OD>
                                           TestPortAsicLoopback         <OD>
                                           TestPortAsicCam               <OD>
                                           TestPortAsicRingLoopback     <OD>
                                           TestMicRingLoopback          <OD>
                                           TestPortAsicMem              <OD>
3                                           N/A                           N/A
4                                           N/A                           N/A
=====
Switch#
```

次に、スイッチのオンライン診断テストスケジュールを表示する例を示します。

```
Switch# show diagnostic scheduleswitch 1
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```




APPENDIX A

Catalyst 3750G Integrated Wireless LAN Controller スイッチの設定

Catalyst 3750 Integrated Wireless LAN Controller スイッチは、Catalyst 3750 スイッチと最大 25 または 50 の Lightweight アクセス ポイントをサポートする Cisco 4400 シリーズ ワイヤレス LAN コントローラを統合したものです。スイッチおよび内部コントローラでは個別のソフトウェア バージョンが稼動していて、個別にアップグレードする必要があります。スイッチとコントローラとの相互作用は最小限ですが、ソフトウェア イメージが正確に動作するためには、ワイヤレス LAN コントローラ スイッチと互換性がなければいけません。スイッチとコントローラ ソフトウェアとの互換性に関する情報は、Catalyst 3750 スイッチのリリース ノートを参照してください。



(注) ワイヤレス LAN コントローラ スイッチをスタックで使用する場合、このイメージをスタック内のすべてのスイッチにロードします。ただし、ワイヤレス機能は Catalyst 3750G Integrated Wireless LAN Controller スイッチに限り利用可能です。

統合コントローラでは、Cisco 4402 ワイヤレス コントローラ用のソフトウェアが稼動しています。コントローラ ソフトウェア リリースの詳細については、『[Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point](#)』 Release 4.0.x.0 を参照してください。コントローラ ソフトウェアのアップグレード手順については、『[Cisco Wireless LAN Controller Configuration Guide](#)』 Release 4.0 を参照してください。

スイッチとコントローラ ソフトウェアに互換性がない場合、互換性を持たせるようにソフトウェアをアップグレードまたはダウングレードする必要があります。

- Catalyst 3750 イメージとコントローラ イメージで Wireless LAN Control Protocol (WCP) のバージョンが異なる場合、スイッチで Syslog メッセージが生成されます。システムが機能している場合、イメージを同期させるためにソフトウェアをアップグレードまたはダウングレードします。
- WCP が動作を停止した場合、スイッチ上の 2 番目のコンソール ポートを使用してコントローラ ソフトウェアをアップグレードまたはダウングレードすることができます。WCP が動作を停止した場合、スイッチは約 320 秒毎にワイヤレス LAN コントローラをリセットします。

この付録は、スイッチで動作するソフトウェアに適用される情報およびワイヤレス LAN コントローラ スイッチに固有の機能だけについて説明します。Catalyst 3750G スイッチに固有のスイッチ コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

この付録で説明する内容は、次のとおりです。

- 「[ワイヤレス LAN コントローラ スイッチの概要](#)」 (P.A-2)
- 「[ワイヤレス LAN コントローラ スイッチの設定](#)」 (P.A-4)
- 「[内部ワイヤレス コントローラ情報の表示](#)」 (P.A-7)

ワイヤレス LAN コントローラ スイッチの概要

Catalyst 3750 Integrated Wireless LAN Controller スイッチは、最大 25 または 50 の Lightweight アクセス ポイントをサポートする統合ワイヤレス LAN コントローラを備えた、レイヤ 3 IEEE 802.3af 準拠のスイッチです。このスイッチは、Catalyst 3750 スイッチのインフラストラクチャにワイヤレス LAN コントローラとアクセス ポイントを組み合わせて、IEEE 802.11 モバイル ワイヤレス ソリューションを提供します。

ワイヤレス LAN コントローラ スイッチの機能は次のとおりです。

- レイヤ 2 および レイヤ 3 ワイヤレス モビリティ
- レイヤ 3 Lightweight Access Point Protocol (LWAPP) を使用してコントローラと同一または異なるサブネットにあるアクセス ポイントを制御する、アプライアンス モードのワイヤレス LAN コントローラ
- レイヤ 3 ローミング
- ワイヤレス トラフィックの単一の入力点
- ワイヤレス トラフィックと既存の有線ネットワーク インフラストラクチャとの統合
- レイヤ 2 スwitチングおよびレイヤ 3 ルーティング機能
- Catalyst 3750 IP ベースおよび IP サービス暗号化と非暗号化イメージを保有しているソフトウェア パリティ
- 25 と 50 のアクセス ポイントと最大 500 ワイヤレス ユーザに最適化
- アクセス ポイントや IP 電話などの他のネットワーク アプライアンスに対する給電用の Power over Ethernet (PoE; イーサネット経由の電源供給) ポート

Catalyst 3750G スイッチ ソフトウェアは、ルーティング、ブリッジング、Access Control List (ACL; アクセス コントロール リスト)、および QoS (Quality of Service) など、すべてのスイッチ機能を扱います。コントローラは、すべてのワイヤレス機能を扱います。Catalyst 3750G スイッチおよび内部 ワイヤレス コントローラは、2 つのギガビット イーサネット リンクによって内部的に接続されています。これらのリンクは、スイッチ ワイヤレス トラフィックをコントローラに転送するように自動的に設定されるため、ユーザの設定は最小限で済みます。

ワイヤレス LAN コントローラ スイッチおよびスイッチ スタック

ワイヤレス LAN コントローラ スイッチは、スイッチ スタック内の他の Catalyst 3750 スイッチと共存できます。ただし、コントローラを機能させるには、スタック内のすべてのスイッチでコントローラをサポートするソフトウェアが稼働している必要があります。ワイヤレス コントローラの冗長性をサポートするには、少なくとも 2 つの LAN コントローラ スイッチをスタック内に搭載します。スタックに搭載するワイヤレス LAN コントローラ スイッチは、4 台以下にします。

ワイヤレス LAN コントローラ スイッチは、スタック内のマスター スイッチまたはメンバー スイッチです。ワイヤレス LAN コントローラ スイッチのスタック動作は、他の Catalyst 3750 スイッチの動作と一貫性があります。ワイヤレス機能を使用すると、スタック内のあるワイヤレス LAN コントローラ スイッチがシャットダウンした場合に、このスイッチ内のコントローラが制御するアクセス ポイントとワイヤレス クライアントが、スタック内の他のワイヤレス LAN コントローラ スイッチのコントローラに自動的に移行するように、アクセス ポイントを設定することができます。ワイヤレス クライアントのトラフィックは、再アソシエーションおよび再認証のために短時間中断します。

スイッチ スタック内では、各スイッチに固有のスイッチ番号 (1 ~ 9) が割り当てられます。これと同じスイッチ番号がスタック内のスイッチまたはスタンドアロン スイッチ内のコントローラにアクセスする際にも使用され、スイッチ番号はデフォルトで 1 になります。たとえば、スタック メンバー 3 のコントローラにアクセスするには、**session 3 processor 1** 特権 EXEC コマンドを使用します (processor 1 はコントローラを表します)。スタンドアロン スイッチのコントローラにアクセスするには、コマンド **session 1 processor 1** を使用します。



(注)

スイッチ スタックへのスイッチの追加または取り外しの際には、必ずスイッチの電源をオフにしてください。

コントローラとスイッチの相互作用

Catalyst 3750G スイッチとその内部コントローラは、個別に管理されます。スイッチ CLI (コマンドライン インターフェイス)、eXpresso、または CNA を使用してスイッチを管理することができます。コントローラの CLI、内蔵コントローラ GUI、または WCS を使用してコントローラを管理できます。GUI または WCS を使用するには、3750 CLI、コントローラ CLI、eXpresso、または Express Setup を使用してコントローラ管理インターフェイスを設定する必要があります。eXpresso および Express Setup の使用方法については、『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』を参照してください。コントローラ CLI にアクセスするには、**session switch-number processor 1** 特権 EXEC コマンドを入力します。

ワイヤレス LAN コントローラ スイッチの電源をオンにすると、Catalyst 3750 スイッチとワイヤレス コントローラで Power-On Self Test (POST; 電源投入時自己診断テスト) が個別に実行されます。両方で個別のコンフィギュレーション ファイルを保持しており、これらは個別に保存またはクリアする必要があります。

これらのスイッチとコントローラとの相互作用について、以下の点に注意してください。

- Catalyst 3750G スイッチとコントローラは、個別のコンフィギュレーション ファイルを保持しています。これらは自動的に同期しません。
- スイッチをリセットすると、スイッチがコントローラを自動的にリセットします。コントローラがスイッチによってリセットされる場合、コントローラ設定は自動的に保存されません。
- スイッチとコントローラでパスワード回復は別々に機能します。
 - スイッチの **Mode** ボタンを押すと、スイッチのパスワード回復手順をトリガーできます (スイッチパスワード回復手順の詳細については、第 49 章「トラブルシューティング」を参照してください)。
 - コントローラのパスワード回復機能は、ユーザがコントローラ ブートアップ プロセスでエスケープを開始する場合にアクセス可能な非表示のブートアップ メニューから **clear config** を選択することで実行できます。これには、2 番めのコンソール ポートを通じてコントローラにシリアル コンソール アクセスする必要があります。

内部ポート

2 つの内部ギガビット ポートでスイッチとコントローラ ハードウェアが接続されています。これらのポートは、ワイヤレス制御とデータ トラフィックを伝送し、またスイッチとコントローラの管理トラフィックも伝送します。スイッチとコントローラ間の内部トラフィックが可能になるように、リンクが自動的に設定されます。さらに、Catalyst 3750G スイッチによって内部 VLAN ID が選択され、コントローラに伝えられます。内部 VLAN (仮想 LAN) を設定することはできません。

コントローラを使用して正確に操作するには、(ギガビット イーサネット ポート 27 および 28 として識別される) 内部ポートには次のような特性が必要です。

- IEEE 802.1Q トランク モード
- ポート集約プロトコル (PAgP) および Link Aggregation Control Protocol (LACP) がディセーブルなスタティック EtherChannel ポート
- Dynamic Trunking Protocol (DTP; ダイナミック トランッキング プロトコル) フレーム生成がディセーブル
- Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) PortFast モードがイネーブル
- Cisco Discovery Protocol (CDP) がディセーブル
- UniDirectional Link Detection (UDLD) がディセーブル

EtherChannel ポート グループ内のメンバシップを含むこれらのパラメータでポートは自動的に設定され、これらの設定は変更できません。ただし、EtherChannel ポート グループはスイッチとスタックで一意であることが重要です。内部ポートを含む他のポートは、そのポートグループに属することはできません。スイッチ スタックに複数のワイヤレス LAN コントローラ スイッチが含まれている場合、内部ポート チャンネル番号が各スイッチで異ならなければなりません。

必要に応じてポート チャンネル番号を再設定することができ、他のパラメータを使用してこれらのポートを明示的に設定することが可能です。ただし、ACL、VLAN マップ、IP ソースガードなどのトラフィック フローを制限する機能を設定しないようにします。

ワイヤレス LAN コントローラ スイッチの設定

(スタンドアロンまたはスイッチ スタック内の) Catalyst 3750 スイッチを設定したときに使用したのと同じコマンドを使用して、ワイヤレス LAN コントローラ スイッチを設定します。このセクションでは、ワイヤレス LAN コントローラ スイッチ固有の設定だけについて説明します。内容は次のとおりです。

- 「内部ポート設定」(P.A-4)
- 「内部ポートの再設定」(P.A-6)
- 「コントローラへのアクセス」(P.A-7)

内部ポート設定

「内部ポート」(P.A-3) で説明しているように、スイッチとコントローラを接続する内部ポートはギガビット イーサネット ポート 27 および 28 です。スイッチとコントローラとの相互作用に必要なため、そのセクションで定義したパラメータを変更しないでください。内部ポートの設定例は次のとおりです。

```
!
interface Port-channel41
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
end

!
interface GigabitEthernet2/0/27
  description This interface is permanently connected to wireless controller
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

```

switchport nonegotiate
no cdp enable
channel-group 41 mode on
spanning-tree portfast trunk
end

!
interface GigabitEthernet2/0/28
description This interface is permanently connected to wireless controller
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
no cdp enable
channel-group 41 mode on
spanning-tree portfast trunk
end

```

インターフェイス コンフィギュレーション モードで、これらのポートにある他のパラメータを設定することも可能です。たとえば、デフォルトでは、全 VLAN 上にあるすべてのトラフィックがコントローラに送信されます。**switchport trunk allowed vlan** インターフェイス コンフィギュレーション コマンドを使用して、内部トランクで許可されている VLAN を制限します。他のポートと同じように内部ポートに対してインターフェイス コンフィギュレーション モードを開始します。たとえば、ワイヤレス LAN コントローラ スイッチがスタンドアロンスイッチまたはスタックのスイッチ メンバー 1 の場合、このコマンドを使用して内部ポート 27 でインターフェイス コンフィギュレーション モードを開始します。

```

Switch(config)# gigabitethernet1/0/27
Switch(config-if)#

```

内部ポートは、PAgP と LACP がディセーブルなスタティック EtherChannel に属するように自動的に設定されます。スイッチ スタック内の他のポート（内部またはそれ以外）は、この EtherChannel のメンバーにはなれません。スイッチが自動的に設定した内部ポート チャネル番号を識別するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次の出力は、スタック内のスイッチ 1 の内部ポートがポート チャネル 40 に属していることを示しています。このポートチャネルはスタック内の他のポートに使用しないようにします。

```

Switch# show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

```

```

Number of channel-groups in use: 36
Number of aggregators:          36

```

Group	Port-channel	Protocol	Ports
1	Po1 (SD)	LACP	Gi2/0/1 (D)
<output truncated>			
33	Po33 (SD)	LACP	Gi2/0/17 (D)
40	Po40 (SU)	-	Gi1/0/27 (P) Gi1/0/28 (P)

内部ポートの再設定

内部ポートの自動設定は修正できませんが、何らかの理由で自動設定がなくなった場合、ポートをその設定で再設定します。

自動設定で内部ポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	内部ポートの 1 つを指定し、インターフェイス コンフィギュレーション モードを開始します。内部ポートは、 gigabitethernet switch-number/0/27 および gigabitethernet switch-number/0/28 です。
ステップ 3	<code>channel-group channel-group-number mode on</code>	チャンネル グループにポートを割り当て、PAgP モードまたは LACP モードをディセーブルにします。 <ul style="list-style-type: none"> <code>channel-group-number</code> の範囲は 1 ~ 48 です。 <code>mode on</code> を選択すると、ポートで PAgP または LACP が機能しなくなります。 <p>(注) スイッチ スタック内の他のポートは、このチャンネル グループのメンバーにはなれません。</p>
ステップ 4	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>interface interface-id</code>	他の内部ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<code>channel-group channel-group-number mode on</code>	ステップ 3 で使用したのと同じチャンネル グループをポートに割り当てます。
ステップ 7	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>interface port-channel channel-group-number</code>	内部ポートを含むポート チャンネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<code>channel-group channel-group-number mode on</code>	ステップ 3 で使用したのと同じチャンネル グループをポートに割り当てます。
ステップ 10	<code>switchport mode trunk</code>	内部ポートをトランク モードにします。
ステップ 11	<code>switchport trunk encapsulation dot1q</code>	トランク カプセル化方式を IEEE 802.1Q に設定します。
ステップ 12	<code>switchport no negotiate</code>	DTP フレームの生成をディセーブルにします。
ステップ 13	<code>spanning tree portfast</code>	STP PortFast モードをイネーブルにします。
ステップ 14	<code>no cdp</code>	CDP をディセーブルにします。
ステップ 15	<code>no udld</code>	UDLD をディセーブルにします (デフォルトはディセーブルです)。
ステップ 16	<code>switchport trunk allowed vlan remove vlan-list</code>	指定した VLAN からのトランク上で VLAN トラフィックを許可しないことで、コントローラに送信される VLAN トラフィックを制御します。
ステップ 17	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 18	<code>show running-config</code>	設定を確認します。
ステップ 19	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

コントローラへのアクセス

内蔵コントローラ GUI、WCS、またはコントローラ CLI を使用して内部ワイヤレス コントローラを設定することができます。管理インターフェイス IP アドレスを使用してブラウザまたは WCS からコントローラ GUI にアクセスします。

session stack-member-number processor 1 特権 EXEC コマンドを使用して、スイッチ スタックのマスタースイッチまたはスタンドアロンワイヤレス LAN コントローラ スイッチからコントローラ CLI にアクセスします。このコマンドを使用すると、コントローラ CLI でコントローラ コンフィギュレーション コマンドを開始することができます。次に、スタック内のスイッチ 2 をワイヤレス LAN コントローラ スイッチと想定している例を示します。

```
Switch# session 1 processor 1
(Cisco Controller)
User:
```

コントローラ CLI 設定情報については、『[Cisco Wireless LAN Controller Configuration Guide](#)』 Release 4.0 を参照してください。

内部ワイヤレス コントローラ情報の表示

コントローラ GUI のアクセスを使用する場合、管理インターフェイス IP アドレスを入力する必要があります。スイッチ CLI から、キーワードを指定またはなしで **show platform wireless-controller** 特権 EXEC コマンドを入力して、管理 IP アドレスと内部コントローラの他の情報を表示します。以下に例を示します。

```
Switch# show platform wireless-controller
Wireless Controller in Switch 2
Operational Status of the Controller : operational
Service VLAN                          : 4095
Service Port Mac Address               : 000b.8540.3783
Service IP Address                     : 127.0.1.2
Management IP Address                  : 22.2.2.2
Management VLAN                        : 7
Software Version                       : 3.3.0.3
Keepalive Version(controller/switch)  : 1/1
Keepalives Missed                      : 0
Controller accepts http/https          : 0/1
Controller's Status Line                : up
Watchdog resets of Controller          : 0
Controller resets total                 : 0
Unacknowledged control messages       : 0

Wireless Controller in Switch 3
Operational Status of the Controller : operational
Service VLAN                          : 4095
Service Port Mac Address               : 000b.8540.33e3
Service IP Address                     : 127.0.1.3
Management IP Address                  : 8.8.8.8
Management VLAN                        : 8
Software Version                       : 3.3.0.3
Keepalive Version(controller/switch)  : 1/1
Keepalives Missed                      : 0
Controller accepts http/https          : 0/1
Controller's Status Line                : up
Watchdog resets of Controller          : 0
Controller resets total                 : 0
Unacknowledged control messages       : 0
```




APPENDIX B

サポート対象 MIB

この付録では、このリリースでサポートされている Catalyst 3750 スイッチの MIB (Management Information Base; 管理情報ベース) を示します。内容は次のとおりです。

- 「MIB の一覧」 (P.B-1)
- 「FTP による MIB ファイルへのアクセス」 (P.B-4)

MIB の一覧

- BRIDGE-MIB



(注) BRIDGE-MIB は単一 VLAN (仮想 LAN) のコンテキストをサポートします。デフォルトで、設定済みのコミュニティ スtring を使用している SNMP (簡易ネットワーク管理プロトコル) メッセージは、常に VLAN 1 の情報を提供します。他の VLAN (VLAN x など) の BRIDGE-MIB 情報を取得するには、SNMP メッセージ内でコミュニティ スtring `configured community string @x` を使用します。

- CISCO-ADMISSION-POLICY-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- CISCO-CABLE-DIAG-MIB
- CISCO-CDP-MIB
- CISCO-CLUSTER-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-ERR-DISABLE-MIB
- CISCO-FLASH-MIB (すべてのスイッチのフラッシュ メモリは着脱式フラッシュ メモリとしてモデル化されています)
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-MIB

- CISCO-HSRP-EXT-MIB (一部サポート)
- CISCO-IETF-IP-MIB
- CISCO-IETF-IP-FORWARDING-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB (スタック マスター イメージの詳細のみ表示)
- CISCO IP-STAT-MIB
- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-AUTH-BYPASS
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB (スタック マスター イメージの詳細のみ表示)
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB (パケット カウンタのみサポート。オクテット カウンタはサポートされません)
- CISCO-POWER-ETHERNET-EXT-MIB
- CISCO-PRODUCTS-MIB
- CISCO-PROCESS-MIB (スタック マスターの詳細のみ表示)
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- CISCO-STACK-MIB (一部サポート。オブジェクトによっては、スタック マスター情報だけサポートされます。ENTITY MIB を代替として推奨)
- CISCO-STACKMAKER-MIB
- CISCO-STACKWISE MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TC-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-CONFIG-COPY-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8021-PAE-MIB

- IEEE8023-LAG-MIB
- IF-MIB (VLAN の入出力カウンタはサポートされていません)
- IGMP-MIB
- INET-ADDRESS-MIB
- IPMROUTE-MIB
- LLDP MED MIB
- OLD-CISCO-CHASSIS-MIB (一部サポート。オブジェクトによっては、スタック マスターのみ反映されています)
- OLD-CISCO-FLASH-MIB (スタック マスターのみサポート。CISCO-FLASH_MIB を使用します)
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- PIM-MIB
- RFC1213-MIB (機能は CISCO-RFC1213-CAPABILITY.my で指定されているエージェント機能により異なります)
- RFC1253-MIB (OSPF-MIB)
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB



(注)

次の URL でも Catalyst 3750 スイッチでサポートされる MIB の一覧を確認できます。
<ftp://ftp.cisco.com/pub/mibs/supportlists/cat3750/cat3750-supportlist.html>

次のシスコの Web サイトで MIB およびシスコ製品に関する他の情報を入手できます。
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

FTP による MIB ファイルへのアクセス

各 MIB ファイルを入手する手順は、次のとおりです。

ステップ 1 ご使用の FTP クライアントがパッシブ モードであることを確認してください。



(注) パッシブ モードをサポートしていない FTP クライアントもあります。

ステップ 2 FTP を使用してサーバ **ftp.cisco.com** にアクセスします。

ステップ 3 ユーザ名 **anonymous** を使用してログインします。

ステップ 4 パスワードが要求されたら、E メールユーザ名を入力します。

ステップ 5 ftp> プロンプトで、ディレクトリを **/pub/mibs/v1** および **/pub/mibs/v2** に変更します。

ステップ 6 **get MIB_filename** コマンドを使用して、MIB ファイルのコピーを入手します。



APPENDIX C

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

この付録では、Catalyst 3750 スイッチのフラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、スイッチにソフトウェア イメージをアーカイブ（アップロードおよびダウンロード）する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用するコマンドの構文と使い方の詳細は、このリリースのスイッチ コマンド リファレンス および『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 を参照してください。これらのマニュアルは、[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示される Cisco.com のページでご利用になれます。

この付録で説明する内容は、次のとおりです。

- 「フラッシュ ファイル システムの操作」(P.C-1)
- 「コンフィギュレーション ファイルの操作」(P.C-9)
- 「ソフトウェア イメージの操作」(P.C-25)

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェア イメージおよびコンフィギュレーション ファイルの管理に役立つ複数のコマンドも備えています。スイッチのデフォルトのフラッシュ ファイル システムは *flash:* です。

スタック マスターまたはスタック メンバーで表示される *flash:* は、表示中のファイル システムが存在するスイッチと同じスイッチに接続されたローカル フラッシュ デバイスを意味します。スイッチ スタックでは、スタック マスターから各スタック メンバーのフラッシュ デバイスをそれぞれ参照できます。これらのフラッシュ ファイル システム名には、対応するスイッチ メンバー番号が含まれます。たとえば、スタック マスターで表示される *flash3:* は、スタック メンバー 3 上の *flash:* を意味します。スイッチ スタック内のフラッシュ ファイル システムを含むすべてのファイル システムのリストを表示するには、**show file systems** 特権 EXEC コマンドを使用します。

スイッチ スタックのソフトウェア イメージおよびコンフィギュレーション ファイルを管理できるのは、一度に 1 名のユーザだけです。

ここでは、次の設定情報について説明します。

- 「使用可能なファイル システムの表示」 (P.C-2)
- 「デフォルト ファイル システムの設定」 (P.C-3)
- 「ファイル システムのファイルに関する情報の表示」 (P.C-3)
- 「ディレクトリの作成および削除」 (P.C-4)
- 「ファイルのコピー」 (P.C-5)
- 「ファイルの削除」 (P.C-6)
- 「tar ファイルの作成、表示、および抽出」 (P.C-6)
- 「ファイルの内容の表示」 (P.C-8)

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します (次の例を参照)。次の例では、スタック マスターはスタック メンバー 3 であるため、flash3: は flash: というエイリアスで表されます。スタック メンバー 5 のファイル システムは、スタック マスターでは flash5 として表示されます。

```
Switch# show file systems
File Systems:
      Size (b)      Free (b)      Type  Flags  Prefixes
*   15998976      5135872      flash  rw     flash:flash3:
      -            -            opaque  rw     bs:
      -            -            opaque  rw     vb:
      524288      520138      nvram   rw     nvram:
      -            -            network  rw     tftp:
      -            -            opaque  rw     null:
      -            -            opaque  rw     system:
      -            -            opaque  ro     xmodem:
      -            -            opaque  ro     ymodem:
      15998976      645120      unknown  rw     flash5:
      -            -            network  rw     rcp:
      -            -            network  rw     ftp:
```

表 C-1 show file systems フィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ (バイト単位)
Free(b)	ファイル システムの空きメモリ サイズ (バイト単位)
Type	ファイル システムのタイプ flash : ファイル システムはフラッシュ メモリ デバイス用です。 nvram : ファイル システムは NVRAM (不揮発性 RAM) デバイス用です。 opaque : ファイル システムはローカルに生成された <i>pseudo</i> ファイル システム (<i>system</i> など)、または <i>brimux</i> などのダウンロード インターフェイスです。 unknown : ファイル システムのタイプは不明です。

表 C-1 show file systems フィールドの説明 (続き)

フィールド	値
Flags	ファイル システムの権限 ro : 読み取り専用です。 rw : 読み取り / 書き込みです。 wo : 書き込み専用です。
Prefixes	ファイル システムのエイリアス flash: : フラッシュ ファイル システムです。 nvram: : NVRAM です。 null: : コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。 rcp: : Remote Copy Protocol (RCP) ネットワーク サーバです。 system: : 実行コンフィギュレーションを含むシステム メモリが格納されています。 tftp: : TFTP ネットワーク サーバです。 xmodem: : XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 ymodem: : YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルト ファイル システムの設定

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd filesystem:** 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。

ファイル システムのファイルに関する情報を表示するには、表 C-2 に記載された特権 EXEC コマンドのいずれかを使用します。

表 C-2 ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [filesystem:][filename]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。

表 C-2 ファイルに関する情報を表示するためのコマンド（続き）

コマンド	説明
<code>show file information file-url</code>	特定のファイルに関する情報を表示します。
<code>show file descriptors</code>	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <i>filesystem:</i> に、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。
ステップ 2	<code>cd new_configs</code>	目的のディレクトリに変更します。 コマンド例では、 <i>new_configs</i> という名前のディレクトリに変更する方法を示します。
ステップ 3	<code>pwd</code>	作業ディレクトリを表示します。

ディレクトリの作成および削除

ディレクトリを作成および削除するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <i>filesystem:</i> に、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。
ステップ 2	<code>mkdir old_configs</code>	新しいディレクトリを作成します。 コマンド例では、 <i>old_configs</i> という名前のディレクトリの作成方法を示します。 ディレクトリ名では大文字と小文字が区別されます。 スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	<code>dir filesystem:</code>	設定を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force/recursive filesystem:/file-url** 特権 EXEC コマンドを使用します。

名前指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem に、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

**注意**

ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy source-url destination-url** 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム (**xmodem:**、**ymodem:**) を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、**tftp:** などがあり、構文は次のとおりです。

- FTP : **ftp:**[[//username [:password]@location]/directory]/filename
- RCP : **rcp:**[[//username@location]/directory]/filename
- TFTP : **tftp:**[[//location]/directory]/filename

ローカルにある書き込み可能なファイル システムには **flash:** などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ（たとえば、**copy flash: flash:** コマンドは無効）

コンフィギュレーション ファイルによる **copy** コマンドの具体的な使用例については、「[コンフィギュレーション ファイルの操作](#)」(P.C-9) を参照してください。

新しいバージョンをダウンロードするか、または既存のバージョンをアップロードして、ソフトウェア イメージをコピーするには、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドを使用します。詳細については、「[ソフトウェア イメージの操作](#)」(P.C-25) を参照してください。

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [/force] [/recursive] [filesystem:] /file-url 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem: オプションを省略すると、**cd** コマンドで指定したデフォルトのデバイスが使用されます。**file-url** には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとする時、削除の確認を求めるとプロンプトが表示されます。



注意

ファイルが削除された場合、その内容は回復できません。

次に、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次のセクションを参照）。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないスイッチにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

```
archive tar/create destination-url flash:/file-url
```

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:

- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rnp:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、作成される tar ファイルです。

flash:/file-url には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルにおけるすべてのファイルおよびディレクトリが、新規に作成された tar ファイルに書き込まれます。

次に、tar ファイルの作成方法を示します。次のコマンドを実行すると、ローカル フラッシュ デバイスのディレクトリ *new-configs* の内容が、172.20.10.30 にある TFTP サーバ上のファイル *saved.tar* に書き込まれます。

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table source-url

source-url には、ローカルまたはネットワーク ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:
- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rnp:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、表示する tar ファイルです。

tar ファイルの後ろにオプションのファイルまたはディレクトリのリストを指定して、表示するファイルを制限することもできます。リストを指定すると、リスト内のファイルだけが表示されます。何も指定しないと、すべてのファイルおよびディレクトリが表示されます。

次に、フラッシュ メモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)
```

次に、*/html* ディレクトリおよびその内容だけを表示する例を示します。

```
Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
```

```
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマンドを使用します。

```
archive tar/xtract source-url flash:/file-url [dir/file...]
```

source-url には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
flash:
- FTP の場合の構文は次のとおりです。
ftp:[[/username[:password]@location]/directory]/tar-filename.tar
- RCP の場合の構文は次のとおりです。
rcp:[[/username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。
tftp:[[/location]/directory]/tar-filename.tar

tar-filename.tar は、ファイルの抽出元の tar ファイルです。

flash:/file-url [dir/file...] には、tar ファイルの抽出先にするローカル フラッシュ ファイル システム上の場所を指定します。抽出対象の tar ファイル内の任意のファイルまたはディレクトリのリストを指定するには、*dir/file...* オプションを使用します。何も指定しないと、すべてのファイルおよびディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。このコマンドを実行すると、*new-configs* ディレクトリがローカル フラッシュ ファイル システムのルート ディレクトリに抽出されます。*saved.tar* ファイルの残りのファイルは無視されます。

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、**more [ascii | /binary | /ebcdic].file-url** 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenummer
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説明します。



(注)

スイッチ スタックのコンフィギュレーション ファイルの詳細については、「[スタックのコンフィギュレーション ファイル](#)」(P.5-14) を参照してください。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成するには、**setup** プログラムを使用するか、または **setup** 特権 EXEC コマンドを使用します。詳細は、[第 3 章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」](#) を参照してください。

TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップコンフィギュレーションにコンフィギュレーション ファイルをコピー（ダウンロード）できます。次のいずれかの目的でこの操作が必要になります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーション ファイルを別のスイッチに使用するため。たとえば、ネットワークに別のスイッチを追加して、元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連部分を変更できます。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのスイッチに同じコンフィギュレーション コマンドをロードするため。

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（アップロード）するには、TFTP、FTP、または RCP を使用します。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておくと、あとでサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

ここでは、次の設定情報について説明します。

- 「[コンフィギュレーション ファイルの作成および使用上の注意事項](#)」(P.C-10)
- 「[コンフィギュレーション ファイルのタイプおよび場所](#)」(P.C-10)
- 「[テキスト エディタによるコンフィギュレーション ファイルの作成](#)」(P.C-11)
- 「[TFTP によるコンフィギュレーション ファイルのコピー](#)」(P.C-11)
- 「[FTP によるコンフィギュレーション ファイルのコピー](#)」(P.C-13)
- 「[RCP によるコンフィギュレーション ファイルのコピー](#)」(P.C-17)
- 「[設定情報の消去](#)」(P.C-20)
- 「[コンフィギュレーションの交換またはロールバック](#)」(P.C-21)

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要なコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソール ポートから接続することを推奨します。コンソール ポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更によっては（スイッチの IP アドレスの変更やポートのディセーブル化など）、スイッチとの接続が切断される可能性があることにご注意ください。
- スイッチにパスワードが設定されていない場合は、**enable secret secret-password** グローバル コンフィギュレーション コマンドを使用して、パスワードを設定することを推奨します。



(注)

copy {ftp: | rcp: | tftp:} system:running-config 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力した場合と同様に、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わせられた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成するには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーして（**copy {ftp: | rcp: | tftp:} nvram:startup-config** 特権 EXEC コマンドを使用）、スイッチを再起動します。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2 つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更したあと、**copy running-config startup-config** 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

-
- ステップ 1** スイッチからサーバに既存のコンフィギュレーションをコピーします。
- 詳細については、「[TFTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.C-12)、「[FTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.C-14)、または「[RCP によるコンフィギュレーション ファイルのダウンロード](#)」(P.C-18) を参照してください。
- ステップ 2** UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。
- ステップ 3** 目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出して、新しいファイルに保存します。
- ステップ 4** コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ (UNIX ワークステーションの場合は、通常は /tftpboot) にコピーします。
- ステップ 5** ファイルに関する権限が world-read に設定されていることを確認します。
-

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用してスイッチを設定したり、別のスイッチからダウンロードしたり、TFTP サーバからダウンロードしたりできます。また、コンフィギュレーション ファイルを TFTP サーバにコピー (アップロード) して、格納できます。

ここでは、次の設定情報について説明します。

- 「[TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備](#)」(P.C-11)
- 「[TFTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.C-12)
- 「[TFTP によるコンフィギュレーション ファイルのアップロード](#)」(P.C-13)

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

/etc/services ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



(注) /etc/inetd.conf および /etc/services ファイルを変更したあとに、inetd デーモンを再起動する必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) や **reboot** コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットワークに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 /tftpboot)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch filename** コマンドを入力します。filename は、サーバにアップロードするとき使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

- ステップ 1** コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。
- ステップ 2** 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-11) を参照して、TFTP サーバが適切に設定されていることを確認します。
- ステップ 3** コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
- ステップ 4** TFTP サーバからコンフィギュレーション ファイルをダウンロードして、スイッチを設定します。TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy tftp:[[[//location]/directory]/filename] system:running-config**
- **copy tftp:[[[//location]/directory]/filename] nvram:startup-config**

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-config* からソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

ステップ 1 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-11)を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 2 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

ステップ 3 スイッチのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:[[/location]/directory]/filename]**
- **copy nvram:startup-config tftp:[[/location]/directory]/filename]**

TFTP サーバにファイルがアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードをクライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)
- **ip ftp username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- **anonymous**

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password password** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した **username@switchname.domain** パスワード。変数 **username** は現在のセッションに関連付けられているユーザ名、**switchname** は設定されているホスト名、**domain** はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられていなければなりません。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にだけ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

詳細については、FTP サーバのマニュアルを参照してください。

ここでは、次の設定情報について説明します。

- 「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-14)
- 「FTP によるコンフィギュレーション ファイルのダウンロード」(P.C-14)
- 「FTP によるコンフィギュレーション ファイルのアップロード」(P.C-16)

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットワークに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip ftp username username グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にだけ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定します。
- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-14) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

コマンド	目的
ステップ 3 configure terminal	スイッチ上で、グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合だけです (ステップ 4、5、および 6 を参照)。
ステップ 4 ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5 ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 copy ftp:[[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config または copy ftp:[[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvram:startup-config	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-config* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-config* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-14) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3 configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合だけです (ステップ 4、5、および 6 を参照)。
ステップ 4 ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5 ip ftp password password	(任意) デフォルトのパスワードを変更します。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 copy system:running-config ftp:[[//[username[:password]@]location]/directory]/filename] または copy nvram:startup-config ftp:[[//[username[:password]@]location]/directory]/filename]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定場所に格納します。

次に、実行コンフィギュレーション ファイル *switch2-config* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[ ]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチ間でコンフィギュレーション ファイルをダウンロード、アップロード、およびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の `copy` コマンドは、リモート システム上の `rsh` サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは `rsh` をサポートするサーバにアクセスするだけで済みます（ほとんどの UNIX システムは `rsh` をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- `copy` コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
- `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、`username` コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スwitchのホスト名。

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

ここでは、次の設定情報について説明します。

- [「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 \(P.C-17\)](#)
- [「RCP によるコンフィギュレーション ファイルのダウンロード」 \(P.C-18\)](#)
- [「RCP によるコンフィギュレーション ファイルのアップロード」 \(P.C-19\)](#)

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- スwitchに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スswitchとサーバは同じサブネットワークに置かれていなければなりません。`ping` コマンドを使用して、RCP サーバへの接続を確認します。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、そのユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。特定のコピー操作にだけ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。
- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の **.rhosts** ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の **.rhosts** ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-17) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモートユーザ名を上書きする場合だけです (ステップ 4 および 5 を参照)。
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy rcp:[[[/[username@]/location]/directory]/filename] system:running-config または copy rcp:[[[/[username@]/location]/directory]/filename] nvrnram:startup-config	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-config* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-config* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

ステップ	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-17) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合だけです (ステップ 4 および 5 を参照)。
ステップ 4	ip rcmd remote-username <i>username</i>	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy system:running-config rcp:[[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] または copy nvram:startup-config rcp:[[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、実行コンフィギュレーション ファイル *switch2-config* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[ ]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーション から設定情報を消去できます。スタートアップ コンフィギュレーション を使用しないでスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーション の内容を消去するには、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。



注意

削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、**delete flash:filename** 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、有害なファイル操作を行った場合に、確認を求めるプロンプトが表示されます。**file prompt** コマンドの詳細については、『*Cisco IOS Command Reference*』 Release 12.2 を参照してください。



注意

削除されたファイルは復元できません。

コンフィギュレーションの交換またはロールバック

コンフィギュレーション交換およびロールバック機能を使用すると、実行コンフィギュレーションと保存されている任意の Cisco IOS コンフィギュレーション ファイルを交換できます。ロールバック機能を使用すると以前のコンフィギュレーションに戻すことができます。

ここでは、次の情報について説明します。

- 「コンフィギュレーション交換およびロールバックの概要」(P.C-21)
- 「設定時の注意事項」(P.C-22)
- 「コンフィギュレーション アーカイブの設定」(P.C-23)
- 「コンフィギュレーション交換またはロールバック動作の実行」(P.C-24)

コンフィギュレーション交換およびロールバックの概要

コンフィギュレーション交換およびロールバック機能を使用する場合、次の内容を理解しておく必要があります。

- 「コンフィギュレーションのアーカイブ」(P.C-21)
- 「コンフィギュレーションの交換」(P.C-21)
- 「コンフィギュレーションのロールバック」(P.C-22)

コンフィギュレーションのアーカイブ

コンフィギュレーション アーカイブは、コンフィギュレーション ファイルのアーカイブを保管、構成、管理するメカニズムです。**configure replace** 特権 EXEC コマンドを使用すると、コンフィギュレーション ロールバック機能が向上します。または、**copy running-config destination-url** 特権 EXEC コマンドを使用して実行コンフィギュレーションのコピーを保存し、交換ファイルをローカルまたはリモートで保存することができます。ただし、この方法ではファイルの自動管理を行うことはできません。コンフィギュレーション交換およびロールバック機能を使用すれば、実行コンフィギュレーションのコピーを自動的にコンフィギュレーション アーカイブに保存できます。

archive config 特権 EXEC コマンドを使用して、コンフィギュレーションをコンフィギュレーション アーカイブに保存します。その際は標準のディレクトリとファイル名のプレフィックスが使用され、連続ファイルを保存するたびにバージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。このときのバージョン番号は 1 つずつ大きくなります。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。保存したファイル数が指定数に達した場合は、次の新しいファイルを保存するときに最も古いファイルが自動的に削除されます。**show archive** 特権 EXEC コマンドを使用すると、コンフィギュレーション アーカイブに保存されたすべてのコンフィギュレーション ファイルを表示できます。

Cisco IOS コンフィギュレーション アーカイブでは、コンフィギュレーション ファイルを保存し、**configure replace** コマンドで使用します。ファイル システムは

コンフィギュレーションの交換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存されている任意のコンフィギュレーション ファイルを交換できます。**configure replace** コマンドを入力すると実行コンフィギュレーションと指定した交換コンフィギュレーションが比較され、コンフィギュレーションの差分が生成されます。生成された差分がコンフィギュレーションの交換に使用されます。コンフィギュレーション交換は、通常 3 回以下のパスで完了します。ループを防ぐために 6 回以上のパスが実行されることはありません。

copy source-url running-config 特権 EXEC コマンドを使用すると、保存されているコンフィギュレーション ファイルが実行コンフィギュレーションに保存できます。このコマンドを **configure replace target-url** 特権コマンドの代わりに使用する場合は、次のような違いがある点に注意してください。

- **copy source-url running-config** コマンドはマージ動作であり、コピー元ファイルと実行コンフィギュレーションのコマンドをすべて保存します。このコマンドでは、コピー元ファイルに実行コンフィギュレーションのコマンドがない場合でも実行コンフィギュレーションのコマンドを削除しません。**configure replace target-url** コマンドの場合は、交換先のファイルに実行コンフィギュレーションのコマンドがない場合は実行コンフィギュレーションから削除し、実行コンフィギュレーションにないコマンドがある場合はそのコマンドを追加します。
- **copy source-url running-config** コマンドのコピー元ファイルとして、部分コンフィギュレーション ファイルを使用できます。**configure replace target-url** コマンドの交換ファイルとして、完全なコンフィギュレーション ファイルを使用する必要があります。

コンフィギュレーションのロールバック

configure replace コマンドを使用して、前回コンフィギュレーションを保存したあとで行った変更をロールバックさせることもできます。コンフィギュレーション ロールバック機能では、コンフィギュレーションを特定の変更時点に戻すのではなく、保存されているコンフィギュレーション ファイルに基づいて特定のコンフィギュレーションに戻します。

コンフィギュレーション ロールバック機能を利用する場合は、コンフィギュレーションを変更する前に実行コンフィギュレーションを保存する必要があります。その後、コンフィギュレーションを変更したあとで **configure replace target-url** コマンドを使用し、保存したコンフィギュレーション ファイルを使って変更をロールバックします。

保存されている任意のファイルをロールバック コンフィギュレーションとして指定できます。一部のロールバック モデルと同様、ロールバック回数は無制限です。

設定時の注意事項

コンフィギュレーション交換およびロールバックを設定し実行する場合は、次の注意事項に従ってください。

- スイッチのメモリの空き容量が、2つのコンフィギュレーション ファイル（実行コンフィギュレーションと保存されている交換コンフィギュレーション）の合計容量よりも大きいことを確認します。スイッチのメモリ容量の方が小さい場合、コンフィギュレーション交換は実行されません。
- また、スイッチにコンフィギュレーション交換やロールバック コンフィギュレーション コマンドが実行できるほどの空き容量があることも確認してください。
- ネットワーク デバイスの物理コンポーネント（物理インターフェイスなど）に関連するコンフィギュレーション コマンドを実行コンフィギュレーションに追加または削除することはできません。
 - インターフェイスがデバイス上に物理的に存在する場合、コンフィギュレーション交換を行っても実行コンフィギュレーションから **interface interface-id** コマンドラインを削除することはできません。
 - インターフェイスがデバイス上に物理的に存在しない場合、**interface interface-id** コマンドラインを実行コンフィギュレーションに追加することはできません。
- **configure replace** コマンドを使用する場合、保存されているコンフィギュレーションを実行コンフィギュレーションの交換コンフィギュレーション ファイルとして指定する必要があります。交換ファイルは Cisco IOS デバイスによって生成された完全なコンフィギュレーションであることが必要です（たとえば **copy running-config destination-url** コマンドで生成したコンフィギュレーション）。



(注) 交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、コンフィギュレーション ロールバックを行うときに大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 archive	アーカイブ コンフィギュレーション モードを開始します。
ステップ 3 path url	コンフィギュレーション アーカイブに、ファイルのディレクトリとファイル名プレフィクスを指定します。
ステップ 4 maximum number	(任意) コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を指定します。 <i>number</i> : コンフィギュレーション アーカイブでの実行コンフィギュレーション ファイルの最大数。有効な値は、1 ~ 14 です。デフォルト値は 10 です。 (注) このコマンドを使用する前に path アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブのファイルのディレクトリとファイル名プレフィクスを指定しておく必要があります。
ステップ 5 time-period minutes	(任意) コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 <i>minutes</i> : コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブを自動保存する間隔を、分単位で指定します。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 show running-config	設定を確認します。
ステップ 8 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

コンフィギュレーション交換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1 archive config	(任意) 実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 (注) path アーカイブ コンフィギュレーション コマンドを入力してから、このコマンドを実行します。
ステップ 2 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	実行コンフィギュレーションに必要な変更を行います。
ステップ 4 exit	特権 EXEC モードに戻ります。
ステップ 5 configure replace target-url [list] [force] [time seconds] [nolock]	実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換します。 <i>target-url</i> : 保存されているコンフィギュレーション ファイルの URL (ファイル システムからアクセス可能)。実行コンフィギュレーションと交換するファイルで、ステップ 2 で archive config 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなどです。 list : コンフィギュレーション交換動作のパスごとにソフトウェア パーサーによって適用されるコマンドエントリのリストを表示します。パスの合計数も表示されます。 force : 実行コンフィギュレーション ファイルと指定した保存済みコンフィギュレーション ファイルの交換を確認なしで実行します。 time seconds : configure confirm コマンドを入力して実行コンフィギュレーション ファイルとの交換を確認するまでの時間を秒単位で指定します。指定時間内に configure confirm コマンドを入力しない場合、コンフィギュレーション交換動作が自動的に停止します (つまり、実行コンフィギュレーション ファイルは configure replace コマンドを入力する以前に存在していたコンフィギュレーションに復元されます)。 (注) time seconds コマンドライン オプションを使用する前に、コンフィギュレーション アーカイブをイネーブルにしておく必要があります。 nolock : コンフィギュレーション交換動作時に他のユーザが実行コンフィギュレーションを変更できないようにする実行コンフィギュレーション ファイルのロックをディセーブルにします。
ステップ 6 configure confirm	(任意) 実行コンフィギュレーションと保存されているコンフィギュレーション ファイルとの交換を確認します。 (注) このコマンドは、 time seconds キーワードと configure replace コマンドの引数が指定されている場合にだけ使用します。
ステップ 7 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフトウェアを格納するソフトウェア イメージ ファイルをアーカイブ（ダウンロードおよびアップロード）する方法を示します。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスタック内のスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないスイッチにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

スイッチ ソフトウェアをアップグレードするには、TFTP、FTP、または RCP サーバからスイッチ イメージ ファイルをダウンロードします。TFTP サーバへアクセスできない場合、Web ブラウザ (HTTP) で PC またはワークステーションへ直接ソフトウェア イメージ ファイルをダウンロードします。次にデバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードします。TFTP サーバまたは Web ブラウザ (HTTP) を使用したスイッチのアップグレードについては、リリース ノートを参照してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保存したりできます。

Cisco IOS Release 12.2(35)SE 以降では、**archive-download-sw /allow-feature-upgrade** 特権 EXEC コマンドを使用して、IP ベース イメージから IP サービス イメージへのアップグレードなど、別のフィーチャセットを有するイメージをインストールすることができます。このリリース以降では、**boot auto-download-sw** グローバル コンフィギュレーション コマンドを使用して、自動ソフトウェア アップグレードのイメージを取得するのに使用する URL を指定することができます。このコマンドを入力する際に、マスター スイッチではバージョン不一致の場合にこの URL を使用します。

バックアップのために、スイッチ イメージ ファイルを TFTP、FTP、または RCP サーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

ここでは、次の設定情報について説明します。

- 「スイッチ上のイメージの場所」 (P.C-26)
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」 (P.C-26)
- 「TFTP によるイメージ ファイルのコピー」 (P.C-27)
- 「FTP によるイメージ ファイルのコピー」 (P.C-31)
- 「RCP によるイメージ ファイルのコピー」 (P.C-36)
- 「スタック メンバー間のイメージ ファイルのコピー」 (P.C-41)



(注)

ソフトウェア イメージ、およびサポートされているアップグレード パスのリストについては、スイッチに付属のリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ (flash:) に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼働しているソフトウェア バージョンを参照できます。画面上で、`System image file is...` で始まる行を調べます。この行は、イメージが格納されているフラッシュ メモリ内のディレクトリ名を示します。

dir filesystem: 特権 EXEC コマンドを使用して、フラッシュ メモリに格納されている他のソフトウェア イメージのディレクトリ名を調べることもできます。 **archive download-sw /directory** 特権 EXEC コマンドを使用して、各 tar ファイルに対してパス全体を指定する代わりに、ディレクトリの後ろにダウンロードする tar ファイルまたは tar ファイルのリストを続けることでディレクトリの指定を 1 回で済ませることが可能です。たとえば、**archive download-sw /directory tftp://10.1.1.10/c3750-ipservices-tar.122-35.SE.tar c3750-ipbase-tar.122-35.SE.tar** と入力することができます。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- tar ファイルの内容を表形式で示す *info* ファイル
- Cisco IOS イメージや Web 管理用ファイルなど、他のイメージおよびファイルが格納された 1 つまたは複数のサブディレクトリ

次に、*info* ファイルに格納された情報の一部の例を示します。表 C-3 に、この情報の詳細を示します。

```
system_type:0x00000000:image-name
  image_family:xxxx
  stacking_number:x
  info_end:
version_suffix:xxxx
  version_directory:image-name
  image_system_type_id:0x00000000
  image_name:image-nameB.bin
  ios_image_file_size:6398464
  total_image_file_size:8133632
  image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
  image_family:xxxx
  stacking_number:x
  board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
  info_end:
```

表 C-3 info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージ バージョン スtring のサフィックスを指定します。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされているディレクトリを指定します。

表 C-3 info ファイルの説明 (続き)

フィールド	説明
image_name	tar ファイル内の Cisco IOS イメージの名前を指定します。
ios_image_file_size	tar ファイル内の Cisco IOS イメージのサイズを指定します。このサイズは、Cisco IOS イメージだけを保持するために必要なフラッシュ メモリ サイズの概算値です。
total_image_file_size	tar ファイル内のすべてのイメージ (Cisco IOS イメージおよび Web 管理ファイル) のサイズを指定します。このサイズは、これらのファイルを保持するために必要なフラッシュ メモリ サイズの概算値です。
image_feature	イメージの主な機能に関する説明です。
image_min_dram	このイメージを実行するために必要な DRAM の最小サイズを指定します。
image_family	ソフトウェアをインストールできる製品ファミリに関する説明です。

TFTP によるイメージ ファイルのコピー

TFTP サーバからスイッチ イメージをダウンロードしたり、スイッチから TFTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードするために使用できます。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないスイッチにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

ここでは、次の設定情報について説明します。

- 「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」 (P.C-28)
- 「TFTP によるイメージ ファイルのダウンロード」 (P.C-28)
- 「TFTP によるイメージ ファイルのアップロード」 (P.C-30)

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

`/etc/services` ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



(注) `/etc/inetd.conf` および `/etc/services` ファイルを変更したあとに、`inetd` デーモンを再起動する必要があります。このデーモンを再起動するには、`inetd` プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) や **reboot** コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットワークに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 `/tftpboot`)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-read` でなければなりません。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch filename** コマンドを入力します。filename は、イメージをサーバにアップロードするとき使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-write` でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 3 を実行します。現在のイメージを保存するには、ステップ 4 に進んでください。

コマンド	目的
ステップ 1	イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します (「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-28) を参照)。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

コマンド	目的
ステップ 3 archive download-sw /allow-feature-upgrade /overwrite /reload ftp:[[/location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> • /allow-feature-upgrade オプションを使用して、異なるフィチャセットを持つイメージをインストールすることができます。 • /overwrite オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //location には、TFTP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 4 archive download-sw /leave-old-sw /reload ftp:[[/location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 <ul style="list-style-type: none"> • /leave-old-sw オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • //location には、TFTP サーバの IP アドレスを指定します。 • /directory/image-name.tar には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロードアルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロードアルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (flash:) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロードプロセス中に古いイメージを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete/force/recursive filesystem:/file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。`filesystem` に、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。`file-url` には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

TFTP によるイメージ ファイルのアップロード

スイッチから TFTP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	TFTP サーバが適切に設定されていることを確認します (「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」 (P.C-28) を参照)。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	<p><code>archive upload-sw</code> <code>tftp:[[/location]/directory]/image-name.tar</code></p> <p>現在稼働中のスイッチ イメージを TFTP サーバにアップロードします。</p> <ul style="list-style-type: none"> <code>//location</code> には、TFTP サーバの IP アドレスを指定します。 <code>/directory/image-name.tar</code> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。<code>image-name.tar</code> は、サーバ上に格納するソフトウェア イメージの名前です。

`archive upload-sw` 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのコピー

FTP サーバからスイッチ イメージをダウンロードしたり、スイッチから FTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないスイッチにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

ここでは、次の設定情報について説明します。

- 「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-31)
- 「FTP によるイメージ ファイルのダウンロード」(P.C-32)
- 「FTP によるイメージ ファイルのアップロード」(P.C-35)

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードをクライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)
- **ip ftp username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- **anonymous**

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password password** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)

- スイッチが作成した `username@switchname.domain` パスワード。変数 `username` は現在のセッションに関連付けられているユーザ名、`switchname` は設定されているホスト名、`domain` はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられていなければなりません。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットワークに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username username** グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。ユーザ名をこの処理のためだけに指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンド内でユーザ名を指定します。
- イメージ ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 7 の手順を実行します。現在のイメージを保存するには、ステップ 8 に進んでください。

コマンド	目的
ステップ 1	「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-31) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

コマンド	目的
ステップ 3 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合だけです (ステップ 4、5、および 6 を参照)。
ステップ 4 <code>ip ftp username <i>username</i></code>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5 <code>ip ftp password <i>password</i></code>	(任意) デフォルトのパスワードを変更します。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>archive download-sw /allow-feature-upgrade /overwrite /reload ftp:[[/username[:password]@location]/directory]/ image-name.tar</code>	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> • <code>/allow-feature-upgrade</code> オプションを使用して、異なるフィーチャセットを持つイメージをインストールすることができます。 • <code>/overwrite</code> オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • <code>/reload</code> オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • <code>//username[:password]</code> には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられていなければなりません。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-31) を参照してください。 • <code>@location</code> には、FTP サーバの IP アドレスを指定します。 • <code>directory/image-name.tar</code> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

コマンド	目的
ステップ 8 <code>archive download-sw /leave-old-sw /reload</code> <code>ftp:[[/username[:password]@location]/directory]/</code> <code>image-name.tar</code>	<p>FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。</p> <ul style="list-style-type: none"> • <code>/leave-old-sw</code> オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • <code>/reload</code> オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • <code>//username[:password]</code> には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられていなければなりません。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-31) を参照してください。 • <code>@location</code> には、FTP サーバの IP アドレスを指定します。 • <code>directory/image-name.tar</code> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。`/overwrite` オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注)

フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、`/overwrite` オプションを指定する必要があります。

`/leave-old-sw` を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (flash:) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete /force/recursive filesystem:/file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。`filesystem` に、システム ボードのフラッシュ デバイスを指定する場合は `flash:` を使用します。`file-url` には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのアップロード

スイッチから FTP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.C-14) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3 configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合だけです (ステップ 4、5、および 6 を参照)。
ステップ 4 ip ftp username <i>username</i>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5 ip ftp password <i>password</i>	(任意) デフォルトのパスワードを変更します。
ステップ 6 end	特権 EXEC モードに戻ります。
ステップ 7 archive upload-sw ftp:[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/ <i>image-name.tar</i>	現在稼働中のスイッチ イメージを FTP サーバにアップロードします。 <ul style="list-style-type: none"> //username:password には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられていなければなりません。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-31) を参照してください。 @location には、FTP サーバの IP アドレスを指定します。 /directory/image-name.tar には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。image-name.tar は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのコピー

RCP サーバからスイッチ イメージをダウンロードしたり、スイッチから RCP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないスイッチにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。

ここでは、次の設定情報について説明します。

- 「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36)
- 「RCP によるイメージ ファイルのダウンロード」(P.C-38)
- 「RCP によるイメージ ファイルのアップロード」(P.C-40)

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の **copy** コマンドは、リモート システム上の **rsh** サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは **rsh** をサポートするサーバにアクセスするだけで済みます（ほとんどの UNIX システムは **rsh** をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは、次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）。

- 現在の TTY (端末) プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スwitch のホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、**rsh** がサポートされていることを確認します。
- スwitch に RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スswitch とサーバは同じサブネットワークに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスswitch にアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスswitch にアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スswitch 上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の **.rhosts** ファイルにエントリを追加する必要があります。

たとえば、スswitch に次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスswitch の IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の **.rhosts** ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 6 の手順を実行します。現在のイメージを保存するには、ステップ 7 に進んでください。

コマンド	目的
ステップ 1	「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2	コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合だけです (ステップ 4 および 5 を参照)。
ステップ 4 <code>ip rcmd remote-username <i>username</i></code>	(任意) リモート ユーザ名を指定します。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>archive download-sw /allow-feature-upgrade /overwrite /reload rcp:[[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>image-name.tar</i>]</code>	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 <ul style="list-style-type: none"> • <code>/allow-feature-upgrade</code> オプションを使用して、異なるフィーチャ セットを持つイメージをインストールすることができます。 • <code>/overwrite</code> オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • <code>/reload</code> オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • <code>//<i>username</i></code> には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36) を参照してください。 • <code>@<i>location</i></code> には、RCP サーバの IP アドレスを指定します。 • <code>/<i>directory</i>/<i>image-name.tar</i></code> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

コマンド	目的
ステップ 7 <code>archive download-sw /leave-old-sw /reload</code> <code>rcp:[[[/[username@]/location]/directory]/image-name.tar]</code>	<p>RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。</p> <ul style="list-style-type: none"> • <code>/leave-old-sw</code> オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • <code>/reload</code> オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • <code>//username</code> には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36)を参照してください。 • <code>@location</code> には、RCP サーバの IP アドレスを指定します。 • <code>/directory]/image-name.tar</code> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。`/overwrite` オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注)

フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、`/overwrite` オプションを指定する必要があります。

`/leave-old-sw` を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (`flash:`) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete /force/recursive filesystem:/file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。`filesystem` に、システム ボードのフラッシュ デバイスを指定する場合は `flash:` を使用します。`file-url` には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合だけです (ステップ 4 および 5 を参照)。
ステップ 4	<code>ip rcmd remote-username username</code>	(任意) リモート ユーザ名を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>archive upload-sw rcp:[[[/[username@]/location]/directory]/image-name.tar]</code>	現在稼働中のスイッチ イメージを RCP サーバにアップロードします。 <ul style="list-style-type: none"> • <code>//username</code> には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.C-36) を参照してください。 • <code>@/location</code> には、RCP サーバの IP アドレスを指定します。 • <code>/directory]/image-name.tar</code> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • <code>image-name.tar</code> は、サーバ上に格納するソフトウェア イメージの名前です。

`archive upload-sw` 特権 EXEC コマンドを実行すると、これらのファイルが `info`、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって `tar` ファイル形式が作成されます。



注意

ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

スタック メンバー間のイメージ ファイルのコピー

スイッチ スタックの場合、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドは必ずスタック マスターを通して使用してください。スタック マスターにダウンロードされたソフトウェア イメージは、残りのスタック メンバーに自動的にダウンロードされます。

互換性のないソフトウェア イメージが格納されたスイッチをアップグレードする場合は、**archive copy-sw** 特権 EXEC コマンドを使用して、既存のスタック メンバーから互換性のないソフトウェアのメンバーにソフトウェア イメージをコピーします。このスイッチは自動的にリロードされ、完全な機能を備えたメンバーとしてスタックに参加します。



(注) **archive copy-sw** 特権 EXEC コマンドを正しく使用するには、追加するスタック メンバー スイッチおよびスタック マスターの両方のイメージを TFTP サーバからダウンロードしておく必要があります。ダウンロードを行うには、**archive download-sw** 特権 EXEC コマンドを使用します。

別のスタック メンバーのフラッシュ メモリから現在のイメージ ファイルをコピーするには、アップグレードするスタック メンバーから特権 EXEC モードを開始し、次の手順を実行します。

コマンド	目的
ステップ 1 archive copy-sw /destination-system destination-stack-member-number /force-reload source-stack-member-number	スタック メンバーから現在のイメージ ファイルをコピーし、更新されたスタック メンバーを無条件にリロードします。 (注) 少なくともスタック メンバー 1 つが、互換性のないソフトウェアを稼動するスイッチにコピーするイメージを実行していなければいけません。 /destination-system destination-stack-member-number には、現在の送信元イメージ ファイルのコピー先であるスタック メンバー (宛先) 番号を指定します。このスタック メンバー番号を指定しない場合、デフォルトでは、現在のイメージ ファイルがすべてのスタック メンバーにコピーされます。 ソフトウェア イメージのダウンロードが正常に終了したら、 /force-reload を指定して、無条件でシステムをリロードさせます。 source-stack-member-number には、現在のイメージ ファイルのコピー元となるスタック メンバー (送信元) のスタック メンバー番号を指定します。スタック メンバー番号の範囲は、1 ~ 9 です。
ステップ 2 reload slot stack-member-number	更新したスタック メンバーをリセットし、この設定変更を有効にします。

■ ソフトウェア イメージの操作



APPENDIX **D**

Cisco IOS Release 12.2(52)SE でサポートされていないコマンド

この付録では、Catalyst 3750 スイッチのプロンプトに疑問符 (?) を入力したときに表示される CLI (コマンドライン インターフェイス) コマンドの中で、まだテストが済んでいないため、または Catalyst 3750 スイッチのハードウェアの制限により、このリリースでサポートされていないコマンドを示します。このリストがすべてではありません。サポートされていないコマンドは、ソフトウェア機能およびコマンド モード別に掲載されています。

- 「ACL」 (P.D-2)
- 「アーカイブ コマンド」 (P.D-2)
- 「ブート ローダ コマンド」 (P.D-3)
- 「組み込みイベント マネージャ」 (P.D-3)
- 「フォールバック ブリッジング」 (P.D-4)
- 「ハイ アベイラビリティ」 (P.D-5)
- 「HSRP」 (P.D-6)
- 「IGMP スヌーピング コマンド」 (P.D-6)
- 「インターフェイス コマンド」 (P.D-6)
- 「IP マルチキャスト ルーティング」 (P.D-7)
- 「IP SLA」 (P.D-8)
- 「IP ユニキャスト ルーティング」 (P.D-8)
- 「IPv6」 (P.D-10)
- 「レイヤ 3」 (P.D-11)
- 「MAC アドレス コマンド」 (P.D-13)
- 「その他」 (P.D-13)
- 「MSDP」 (P.D-14)
- 「マルチキャスト」 (P.D-14)
- 「NetFlow コマンド」 (P.D-15)
- 「NAT コマンド」 (P.D-15)
- 「QoS」 (P.D-15)
- 「RADIUS」 (P.D-16)
- 「SNMP」 (P.D-16)

- 「SNMPv3」 (P.D-16)
- 「スパニング ツリー」 (P.D-16)
- 「VLAN」 (P.D-17)
- 「VTP」 (P.D-17)

ACL

サポートされていない特権 EXEC コマンド

```
access-enable [host] [timeout minutes]
access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
clear access-template [access-list-number | name] [dynamic-name] [source] [destination]
show access-lists rate-limit [destination]
show accounting
show ip accounting [checkpoint] [output-packets | access violations]
show ip cache [prefix-mask] [type number]
```

サポートされていないグローバル コンフィギュレーション コマンド

```
access-list rate-limit acl-index {precedence | mask prec-mask}
access-list dynamic extended
```

サポートされていないルートマップ コンフィギュレーション コマンド

```
match ip address prefix-list prefix-list-name [prefix-list-name...]
```

アーカイブ コマンド

サポートされていない特権 EXEC コマンド

```
archive config
logging persistent
show archive config
show archive log
```

ARP コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
arp ip-address hardware-address smds
arp ip-address hardware-address srp-a
arp ip-address hardware-address srp-b
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
arp probe
ip probe proxy
```

ブート ローダ コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
boot buffersize
```

組み込みイベント マネージャ

サポートされていない特権 EXEC コマンド

```
event manager update user policy [policy-filename | group [group name expression] ] | repository [url location]
```

次のコマンドでは、パラメータがサポートされていません。

```
event manager run [policy name] |<parameter1>|... <parameter15>|
```

サポートされていないグローバル コンフィギュレーション コマンド

```
no event manager directory user repository [url location ]
event manager applet [applet-name] maxrun
```

アプレット コンフィギュレーション モードでサポートされていないコマンド

```
no event interface name [interface-name] parameter [counter-name] entry-val [entry counter value]
entry-op {gt|ge|eq|ne|lt|le} [entry-type {increment | rate | value}] [exit-val [exit value] exit-op
{gt|ge|eq|ne|lt|le} exit-type { increment | rate | value}][average-factor <average-factor-value>]
no trigger
tag
```

フォールバック ブリッジング

サポートされていない特権 EXEC コマンド

```
clear bridge [bridge-group] multicast [router-ports | groups | counts] [group-address] [interface-unit]
[counts]
clear vlan statistics
show bridge [bridge-group] circuit-group [circuit-group] [src-mac-address] [dst-mac-address]
show bridge [bridge-group] multicast [router-ports | groups] [group-address]
show bridge vlan
show interfaces crb
show interfaces {ethernet | fastethernet} [interface | slot/port] irb
show subscriber-policy range
```

サポートされていないグローバル コンフィギュレーション コマンド

```
bridge bridge-group acquire
bridge bridge-group address mac-address {forward | discard} [interface-id]
bridge bridge-group aging-time seconds
bridge bridge-group bitswap_l3_addresses
bridge bridge-group bridge ip
bridge bridge-group circuit-group circuit-group pause milliseconds
bridge bridge-group circuit-group circuit-group source-based
bridge cmf
bridge crb
bridge bridge-group domain domain-name
bridge irb
bridge bridge-group mac-address-table limit number
bridge bridge-group multicast-source
```


bridge *bridge-group* **protocol** *dec*
bridge *bridge-group* **route** *protocol*
bridge *bridge-group* **subscriber** *policy* *policy*
subscriber-policy *policy* [**no** | **default**] *packet* [**permit** | **deny**]

サポートされていないインターフェイス コンフィギュレーション コマンド

bridge-group *bridge-group* **cbus-bridging**
bridge-group *bridge-group* **circuit-group** *circuit-number*
bridge-group *bridge-group* **input-address-list** *access-list-number*
bridge-group *bridge-group* **input-lat-service-deny** *group-list*
bridge-group *bridge-group* **input-lat-service-permit** *group-list*
bridge-group *bridge-group* **input-lsap-list** *access-list-number*
bridge-group *bridge-group* **input-pattern-list** *access-list-number*
bridge-group *bridge-group* **input-type-list** *access-list-number*
bridge-group *bridge-group* **lat-compression**
bridge-group *bridge-group* **output-address-list** *access-list-number*
bridge-group *bridge-group* **output-lat-service-deny** *group-list*
bridge-group *bridge-group* **output-lat-service-permit** *group-list*
bridge-group *bridge-group* **output-lsap-list** *access-list-number*
bridge-group *bridge-group* **output-pattern-list** *access-list-number*
bridge-group *bridge-group* **output-type-list** *access-list-number*
bridge-group *bridge-group* **sse**
bridge-group *bridge-group* **subscriber-loop-control**
bridge-group *bridge-group* **subscriber-trunk**
bridge *bridge-group* **lat-service-filtering**
frame-relay **map** **bridge** *dci* **broadcast**
interface **bvi** *bridge-group*
x25 **map** **bridge** *x.121-address* **broadcast** [*options-keywords*]

ハイ アベイラビリティ

サポートされていない SSO 認識 HSRP コマンド

すべて

HSRP

サポートされていないグローバル コンフィギュレーション コマンド

```
interface Async
interface BVI
interface Dialer
interface Group-Async
interface Lex
interface Multilink
interface Virtual-Template
interface Virtual-Tokenring
```

サポートされていないインターフェイス コンフィギュレーション コマンド

```
mtu
standby mac-refresh seconds
standby use-bia
```

IGMP スヌーピング コマンド

サポートされていないグローバル コンフィギュレーション コマンド

```
ip igmp snooping tcn
```

インターフェイス コマンド

サポートされていない特権 EXEC コマンド

```
show interfaces [interface-id | vlan vlan-id] [crb | fair-queue | irb | mac-accounting | precedence | irb | random-detect | rate-limit | shape]
```

サポートされていないグローバル コンフィギュレーション コマンド

```
interface tunnel
```

サポートされていないインターフェイス コンフィギュレーション コマンド

`transmit-interface type number`

IP マルチキャスト ルーティング

サポートされていない特権 EXEC コマンド

`clear ip rtp header-compression [type number]`

`debug ip packet` コマンドを実行すると、スイッチの CPU で受信されるパケットが表示されます。ハードウェアでスイッチングされるパケットは表示されません。

`debug ip mcache` コマンドは、スイッチの CPU で受信されるパケットに影響します。ハードウェアでスイッチングされるパケットは表示されません。

`debug ip mpacket [detail] [access-list-number [group-name-or-address]]` コマンドは、スイッチの CPU で受信されるパケットだけ影響します。ほとんどのマルチキャスト パケットはハードウェアでスイッチングされるため、このコマンドは、パケットが CPU に転送されることがわかっている場合だけ使用してください。

`debug ip pim atm`

`show frame-relay ip rtp header-compression [interface type number]`

`show ip mcache` コマンドを実行すると、スイッチの CPU に送信されるパケット用のキャッシュ内のエントリが表示されます。ほとんどのマルチキャスト パケットは CPU の関与を受けずにハードウェアでスイッチングされるため、このコマンドを使用しても、マルチキャスト パケット情報は表示されません。

`show ip mpacket` コマンドはサポートされていますが、スイッチの CPU で受信されるパケットに対してだけ効果があります。ルートがハードウェアによってスイッチングされる場合、このコマンドは効果がありません。CPU はパケットを受信せず、パケット情報が表示されないためです。

`show ip pim vc [group-address | name] [type number]`

`show ip rtp header-compression [type number] [detail]`

サポートされていないグローバル コンフィギュレーション コマンド

`ip multicast-routing [vrf vrf-name] [distributed]`

`ip pim accept-rp {address | auto-rp} [group-access-list-number]`

`ip pim message-interval seconds`

サポートされていないインターフェイス コンフィギュレーション コマンド

`frame-relay ip rtp header-compression [active | passive]`

`frame-relay map ip ip-address dlci [broadcast] compress`

`frame-relay map ip ip-address dlci rtp header-compression [active | passive]`

`ip igmp helper-address ip-address`

ip multicast helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*}
extended-access-list-number

ip multicast rate-limit {*in* | *out*} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*]
kbps

ip multicast ttl-threshold *ttl-value* (代わりに **ip multicast boundary** *access-list-number* インターフェイス コンフィギュレーション コマンドを使用)

ip multicast use-functional

ip pim minimum-vc-rate *pps*

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count *number*

ip rtp compression-connections *number*

ip rtp header-compression [**passive**]

IP SLA

サポートされていない MPLS ヘルス モニタ コマンド

すべて

サポートされていないイーサネット ゲートキーパー登録コマンド

すべて

サポートされていない VoIP コール セットアップ プローブ コマンド

すべて

IP ユニキャスト ルーティング

サポートされていない特権 EXEC コマンドまたはユーザ EXEC コマンド

clear ip accounting [**checkpoint**]

clear ip bgp *address* flap-statistics

clear ip bgp prefix-list

debug ip cef stats

show cef [**drop** | **not-cef-switched**]

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

show ip bgp dampened-paths
show ip bgp inconsistent-as
show ip bgp regexp *regular expression*
show ip prefix-list *regular expression*

サポートされていないグローバル コンフィギュレーション コマンド

ip accounting precedence {input | output}
ip accounting-list *ip-address wildcard*
ip accounting-transits *count*
ip cef traffic-statistics [load-interval *seconds*] [update-rate *seconds*]
ip flow-aggregation
ip flow-cache
ip flow-export
ip gratuitous-arps
ip local
ip prefix-list
ip reflexive-list
router egp
router-isis
router iso-igrp
router mobile
router odr
router static

サポートされていないインターフェイス コンフィギュレーション コマンド

ip accounting
ip load-sharing [per-packet]
ip mtu *bytes*
ip ospf dead-interval minimal hello-multiplier *multiplier*
ip verify
ip unnumbered *type number*
すべての **ip security** コマンド

サポートされていない BGP ルータ コンフィギュレーション コマンド

address-family vpnv4
default-information originate
neighbor advertise-map
neighbor allowas-in
neighbor default-originate
neighbor description
network backdoor
table-map

サポートされていない VPN コンフィギュレーション コマンド

すべて

サポートされていないルート マップ コマンド

Policy-Based Routing (PBR; ポリシーベース ルーティング) の **match route-type**
set as-path {tag | prepend *as-path-string*}
set automatic-tag
set dampening *half-life reuse suppress max-suppress-time*
set default interface *interface-id* [*interface-id*.....]
set interface *interface-id* [*interface-id*.....]
set ip default next-hop *ip-address* [*ip-address*.....]
set ip destination *ip-address mask*
set ip next-hop verify-availability
set ip precedence *value*
set ip qos-group
set metric-type internal
set origin
set metric-type internal
set tag *tag-value*

IPv6

IPv4/v6 トンネリング コマンド

すべて

レイヤ 3

BGP

次の機能のすべてのコマンド

- ネットワーク AS 移行のためのデュアル AS 構成に対する BGP サポート
- グローバル テーブルから VRF テーブルへの IP プレフィックスのインポートに対する BGP サポート
- 名前付き拡張コミュニティ リストに対する BGP サポート
- 拡張コミュニティ リストのシーケンス エントリに対する BGP サポート
- TTL セキュリティ チェックに対する BGP サポート
- BGP ルートマップ ポリシー リストのサポート
- BGP ネクスト ホップ伝播
- BGP ポリシー アカウンティング
- BGP ポリシー アカウンティング出力インターフェイス アカウンティング
- BGP リンク帯域幅
- BGP ハイブリッド CLI サポート
- BGP コスト コミュニティ
- BGP ダイナミック アップデート ピアグループ
- BGP 条件付きルート インジェクション
- ピア テンプレートを使用した BGP 設定
- AS パス アクセス リスト 500 番までに対する BGP サポートの拡張

その他のサポートされていない BGP コマンド

address-family l2vpn

address-family vpnv4

bgp-policyclear bgp nsapaddress-family nsap

clear bgp nsap dampening

clear bgp nsap external

clear bgp nsap flap-statistics

clear bgp nsap peer-group

clear ip bgp ipv6

clear ip bgp l2vpn

clear ip bgp vpnv4

clear ip bgp vpnv6

ha-mode graceful-restartip extcommunity-list redistribute (BGP から ISO IS-IS)

ip policy-listredistribute (ISO IS-IS から BGP)

match extcommunity

neighbor ha-mode graceful-restart
neighbor sooredistribute dvmrp
neighbor ttl-securityset extcommunity
set extcommunity cost
show bgp nsap
show bgp nsap community
show bgp nsap community-list
show bgp nsap dampening
show bgp nsap dampened-paths
show bgp nsap filter-list
show bgp nsap flap-statistics
show bgp nsap inconsistent-as
show bgp nsap neighbors
show bgp nsap paths
show bgp nsap quote-regexp
show bgp nsap regexp
show bgp nsap summary
show ip bgp ipv4 multicast
show ip bgp ipv4 multicast summary
show ip bgp l2vpn
show ip bgp vpnv4
show ip extcommunity-list
show ip policy-list

OSPF

area sham-link
ignore lsa mospf
nsf ietf
nsf ietf helper disable
nsf ietf helper strict-lsa-checking
show ip ospf sham-links

VRF 認識 AAA

すべて

MAC アドレス コマンド

サポートされていない特権 EXEC コマンド

```
show mac-address-table
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table multicast
show mac-address-table notification
show mac-address-table static
show mac-address-table vlan
show mac address-table multicast
```



(注) VLAN (仮想 LAN) のレイヤ 2 マルチキャスト アドレス テーブル エントリを表示するには、**show ip igmp snooping groups** 特権 EXEC コマンドを使用します。

サポートされていないグローバル コンフィギュレーション コマンド

```
mac-address-table aging-time
mac-address-table notification
mac-address-table static
```

その他

サポートされていないユーザ EXEC コマンド

```
verify
```

サポートされていない特権 EXEC コマンド

```
file verify auto
show cable-diagnostics prbs
test cable-diagnostics prbs
```

サポートされていないグローバル コンフィギュレーション コマンド

`errdisable recovery cause unicast flood`
`l2protocol-tunnel global drop-threshold`
`memory reserve critical`
`service compress-config`
`track object-number rtr`

MSDP

サポートされていない特権 EXEC コマンド

`show access-expression`
`show exception`
`show location`
`show pm LINE`
`show smf [interface-id]`
`show subscriber-policy [policy-number]`
`show template [template-name]`

サポートされていないグローバル コンフィギュレーション コマンド

`ip msdp default-peer ip-address | name [prefix-list list]` (BGP/MBGP がサポートされていないため、このコマンドの代わりに、`ip msdp peer` コマンドを使用してください)

マルチキャスト

サポートされていない BiDirectional PIM (bidir-PIM; 双方向 PIM) コマンド

すべて

サポートされていないマルチキャスト ルーティング マネージャ コマンド

すべて

サポートされていない IP マルチキャスト レート制限コマンド

すべて

サポートされていない UDLR コマンド

すべて

サポートされていない GRE でのマルチキャスト コマンド

すべて

NetFlow コマンド

サポートされていないグローバル コンフィギュレーション コマンド

`ip flow-aggregation cache`

`ip flow-cache entries`

`ip flow-export`

NAT コマンド

サポートされていない特権 EXEC コマンド

`show ip nat statistics`

`show ip nat translations`

QoS

サポートされていないグローバル コンフィギュレーション コマンド

`priority-list`

サポートされていないインターフェイス コンフィギュレーション コマンド

`priority-group`

`rate-limit`

サポートされていないポリシーマップ コンフィギュレーション コマンド

`class-default` が `class-map-name` である場合の `class class-default`

RADIUS

サポートされていないグローバル コンフィギュレーション コマンド

```
aaa nas port extended
aaa authentication feature default enable
aaa authentication feature default line
aaa nas port extended
radius-server attribute nas-port
radius-server configure
radius-server extended-portnames
```

SNMP

サポートされていないグローバル コンフィギュレーション コマンド

```
snmp-server enable informs
snmp-server ifindex persist
```

SNMPv3

サポートされていない 3DES 暗号化コマンド

すべて

スパニング ツリー

サポートされていないグローバル コンフィギュレーション コマンド

```
spanning-tree pathcost method {long | short}
```

サポートされていないインターフェイス コンフィギュレーション コマンド

`spanning-tree stack-port`

VLAN

サポートされていないグローバル コンフィギュレーション コマンド

`vlan internal allocation policy {ascending | descending}`

サポートされていないユーザ EXEC コマンド

`show running-config vlan`

`show vlan ifindex`

`vlan database`

サポートされていない VLAN データベース コマンド

`vtp`

`vlan`

VTP

サポートされていない特権 EXEC コマンド

`vtp {password password | pruning | version number}`



(注) このコマンドは、**vtp** グローバル コンフィギュレーション コマンドに置き換えられています。



INDEX

数字

10 ギガビット イーサネット インターフェイス

設定時の注意事項 [12-19](#)

定義 [12-7](#)

3750G 統合ワイヤレス LAN コントローラ スイッチ

コントローラとスイッチの相互作用 [A-3](#)

スイッチの設定 [A-4](#)

内部ポート

再設定 [A-6](#)

設定 [A-4](#)

802.1X ユーザ分散の設定 [10-56](#)

A

AAA ダウン ポリシー、NAC レイヤ 2 IP 検証 [1-12](#)

ABR [38-28](#)

access-class コマンド [35-20](#)

Access Control Entry (アクセス コントロール エントリ)

「ACE」を参照

ACE

IP [35-2](#)

QoS [36-7](#)

イーサネット [35-2](#)

定義 [35-2](#)

ACL

ACE [35-2](#)

any キーワード [35-13](#)

host キーワード [35-13](#)

IP

暗黙の拒否 [35-10, 35-15, 35-17](#)

一致条件 [35-8](#)

作成 [35-8](#)

フラグメントおよび QoS に関する注意事項 [36-34](#)

未定義 [35-21](#)

無視マスク [35-10](#)

IPv4

一致条件 [35-8](#)

インターフェイスへの適用 [35-20](#)

作成 [35-8](#)

サポートされない機能 [35-7](#)

端末回線、設定 [35-19](#)

名前付き [35-15](#)

番号 [35-9](#)

IPv6

一致条件 [41-3](#)

インターフェイスへの適用 [41-8](#)

サポートされない機能 [41-3](#)

サポート対象 [41-3](#)

スタック [41-4](#)

制限事項 [41-3](#)

設定 [41-4, 41-5](#)

他の機能との相互作用 [41-5](#)

名前付き [41-3](#)

表示 [41-9](#)

優先 [41-2](#)

MAC 拡張 [35-28, 36-46](#)

QoS [36-7, 36-44](#)

QoS クラス マップあたりの個数 [36-34](#)

QoS のトラフィックの分類 [36-44](#)

VLAN マップ

設定 [35-31](#)

設定時の注意事項 [35-32](#)

エントリのシーケンスの再編集 [35-15](#)

拡張 IP、QoS の分類設定 [36-45](#)

- 拡張 IPv4
 - 一致条件 [35-8](#)
 - 作成 [35-11](#)
- コメント [35-19](#)
- コンパイル [35-23](#)
- サポート [1-11](#)
- サポートされない機能、IPv4 [35-7](#)
- サポートされない機能、IPv6 [41-3](#)
- サポートされるタイプ [35-2](#)
- 時間範囲 [35-17](#)
- 照合 [35-8, 35-21, 41-3](#)
- 定義 [35-1, 35-8](#)
- 適用
 - IPv6 インターフェイス [41-8](#)
 - QoS [36-7](#)
 - インターフェイス [35-20, 41-8](#)
 - 時間範囲 [35-17](#)
 - スイッチド パケット [35-39](#)
 - ブリッジド パケット [35-40](#)
 - マルチキャスト パケット [35-41](#)
 - ルーテッド パケット [35-41](#)
- 名前 [41-5](#)
- 名前付き、IPv4 [35-15](#)
- 名前付き、IPv6 [41-3](#)
- ハードウェアおよびソフトウェアの処理 [35-22](#)
- ハードウェアのサポート [35-22](#)
- 標準 IP、QoS の分類設定 [36-44](#)
- 標準 IPv4
 - 一致条件 [35-8](#)
 - 作成 [35-10](#)
- ポート [35-2, 41-2](#)
- モニタリング [35-42, 41-9](#)
- 優先 [35-2](#)
- ルータ [35-2, 41-2](#)
- ルータ ACL と VLAN マップの設定時の注意事項 [35-38](#)
- ルータ ACL を VLAN マップと組み合わせて使用する
方法 [35-38](#)
- 例 [35-23, 36-44](#)
- レイヤ 4 情報 [35-39](#)
- ログ メッセージ [35-9](#)
- AC (アクティブ クラスタ コマンド スイッチ) [6-11](#)
- Address Resolution Protocol (アドレス解決プロトコル)
「ARP」を参照
- Area Border Router (エリア境界ルータ)
「ABR」を参照
- ARP
 - カプセル化 [38-12](#)
 - スタティック キャッシュの設定 [38-11](#)
 - 設定 [38-11](#)
 - 定義 [1-6, 7-32, 38-10](#)
 - テーブル
 - アドレス解決 [7-32](#)
 - 管理 [7-32](#)
- AS、BGP 内 [38-52](#)
- ASBR [38-28](#)
- AS パス フィルタ、BGP [38-59](#)
- Auto-MDIX
 - 設定 [12-23](#)
 - 説明 [12-23](#)
- Autonomous System Boundary Router (自律システム境界
ルータ)
「ASBR」を参照
- Auto Smartport マクロ
 - 組み込みマクロ [13-3, 13-9](#)
 - Cisco Medianet [13-2](#)
 - IOS シェル [13-1, 13-15](#)
 - LLDP [13-2](#)
 - イネーブル化 [13-5, 13-6, 13-8](#)
 - イベント トリガー [13-12](#)
 - 設定時の注意事項 [13-4](#)
 - 定義 [13-1](#)
 - デフォルト設定 [13-3](#)
 - 表示 [13-20](#)
 - マッピング [13-9](#)
 - ユーザ定義マクロ [13-15](#)
 - 「Smartport マクロ」も参照
- autostate exclude [12-6](#)

B

BackboneFast

イネーブル化 [21-17](#)サポート [1-9](#)説明 [21-7](#)ディセーブル化 [21-17](#)Berkeley r-tools の代わり [9-57](#)

BGP

CIDR [38-65](#)clear コマンド [38-68](#)show コマンド [38-68](#)イネーブル化 [38-52](#)コミュニティ フィルタリング [38-61](#)サポート [1-15](#)集約アドレス [38-65](#)集約ルート、設定 [38-65](#)スーパーネット [38-65](#)セッションのリセット [38-55](#)説明 [38-48](#)デフォルト設定 [38-49](#)ネイバー、タイプ [38-52](#)ネイバーの設定 [38-63](#)バージョン 4 [38-49](#)パスの選択 [38-56](#)ピア、設定 [38-63](#)プレフィクス フィルタリング [38-60](#)マルチ VRF CE におけるルーティング セッション [38-89](#)マルチパス サポート [38-56](#)モニタリング [38-68](#)ルーティング ドメイン連合 [38-66](#)ルート ダンピング化 [38-67](#)ルート マップ [38-58](#)ルート リフレクタ [38-66](#)

Border Gateway Protocol

「BGP」を参照

BPDU

errdisable ステート [21-2](#)RSTP フォーマット [20-13](#)フィルタリング [21-3](#)

BPDU ガード

イネーブル化 [21-13](#)サポート [1-9](#)説明 [21-2](#)ディセーブル化 [21-14](#)

BPDU フィルタリング

イネーブル化 [21-15](#)サポート [1-9](#)説明 [21-3](#)ディセーブル化 [21-15](#)

Bridge Protocol Data Unit (ブリッジ プロトコル データ ユニット)

「BPDU」を参照

C

Catalyst 3750G ワイヤレス LAN コントローラ スイッチ

機能 [A-2](#)コントローラ情報の表示 [A-7](#)コントローラとの相互作用 [A-3](#)コントローラへのアクセス [A-7](#)スイッチ スタック [A-2](#)内部 VLAN [A-3](#)内部ポート [A-3](#)内部ポート EtherChannel [A-4](#)内部ポート設定 [A-4](#)内部ポートの再設定 [A-6](#)

Catalyst 6000 スイッチ

認証の互換性 [10-8](#)

CA の信頼点

設定 [9-54](#)定義 [9-52](#)

CDP

LLDP による定義 [28-1](#)アップデート [27-2](#)

イネーブル化およびディセーブル化

インターフェイス [27-4](#)

- スイッチ **27-3**
- 概要 **27-1**
- サポート **1-7**
- 信頼境界機能 **36-40**
- スイッチ クラスタの自動検出 **6-5**
- スイッチ スタックの考慮事項 **27-2**
- 設定 **27-2**
- 説明 **27-1**
- タイマーおよびホールドタイム、設定 **27-2**
- デフォルト設定 **27-2**
- 電力ネゴシエーションの拡張機能 **12-8**
- モニタリング **27-5**
- ルーティング デバイスでのディセーブル化 **27-3 ~ 27-4**
- レイヤ 2 プロトコル トンネリング **18-8**
- CEF
 - distributed **38-96**
 - IPv6 **39-20**
 - イネーブル化 **38-96**
 - 定義 **38-95**
- CE デバイス **38-81**
- CE デバイス内のマルチ VRF
 - 「マルチ VRF CE」を参照
- CGMP
 - IGMP スヌーピングの学習方法 **25-9**
 - 概要 **46-10**
 - キャッシュに格納されたグループ エントリのクリア **46-66**
 - サーバ サポート機能 **46-10**
 - サーバ サポート機能のイネーブル化 **46-48**
 - スイッチ サポート **1-5**
 - マルチキャスト グループへの加入 **25-3**
- CIDR **38-65**
- CipherSuite **9-53**
- Cisco 7960 IP Phone **16-1**
- Cisco Discovery Protocol
 - 「CDP」を参照
- Cisco Express Forwarding
 - 「CEF」を参照
- Cisco Group Management Protocol
 - 「CGMP」も参照
- Cisco IOS DHCP サーバ
 - 「DHCP」、「Cisco IOS サーバ」を参照
- Cisco IOS File System
 - 「IFS」を参照
- Cisco IOS IP SLA **43-1**
- Cisco Medianet
 - 「Auto Smartport マクロ」を参照
- Cisco Redundant Power System 2300
 - 管理 **12-32**
 - 設定 **12-32**
- Cisco Secure ACS
 - ダウンロード可能な ACL に対するアトリビュート値ペア **10-20**
 - リダイレクト URL に対するアトリビュート値ペア **10-19**
- Cisco Secure ACS Configuration Guide **10-61**
- Cisco StackWise テクノロジー **1-3**
 - 「スタック、スイッチ」も参照
- CiscoWorks 2000 **1-6, 33-4**
- CISP **10-30**
- CIST リージョナル ルート
 - 「MSTP」を参照
- CIST ルート
 - 「MSTP」を参照
- Classless Interdomain Routing
 - 「CIDR」を参照
- Class of Service (サービス クラス)
 - 「CoS」を参照
- CLI
 - エラー メッセージ **2-5**
 - クラスタの管理 **6-17**
 - コマンド出力のフィルタリング **2-10**
 - コマンドの no 形式および default 形式 **2-4**
 - コマンドの省略 **2-4**
 - コマンド モード **2-1**
 - コンフィギュレーション ロギング **2-5**
 - 説明 **1-6**

- ヘルプの表示 [2-3](#)
 - 編集機能
 - イネーブル化およびディセーブル化 [2-7](#)
 - 画面幅よりも長いコマンドライン [2-9](#)
 - キーストロークによる編集 [2-7](#)
 - 履歴
 - コマンドの呼び出し [2-6](#)
 - 説明 [2-6](#)
 - ディセーブル化 [2-7](#)
 - バッファ サイズの変更 [2-6](#)
 - Client Information Signalling Protocol
 - 「CISP」を参照
 - CLNS
 - 「ISO CLNS」を参照
 - CNS [1-6](#)
 - Configuration Engine
 - ConfigID、DeviceID、Hostname [4-3](#)
 - イベント サービス [4-3](#)
 - コンフィギュレーション サービス [4-2](#)
 - 説明 [4-1](#)
 - 管理機能 [1-6](#)
 - 組み込み型エージェント
 - イベント エージェントのイネーブル化 [4-8](#)
 - コンフィギュレーション エージェントのイネーブル化 [4-9](#)
 - 自動設定のイネーブル化 [4-7](#)
 - 説明 [4-5](#)
 - Coarse Wave Division Multiplexer
 - 「CWDM SFP」を参照
 - CoA 要求コマンド [9-24](#)
 - config.text [3-18](#)
 - configure terminal コマンド [12-13](#)
 - config-vlan モード [2-2](#)
 - CoS
 - プライオリティの信頼 [16-7](#)
 - プライオリティの変更 [16-7](#)
 - レイヤ 2 フレーム [36-2](#)
 - CoS/DSCP マップ、QoS [36-62](#)
 - CoS 出力キューしきい値マップ、QoS [36-19](#)
 - CoS 入力キューしきい値マップ、QoS [36-16](#)
 - CPU 使用率、トラブルシューティング [49-26](#)
 - crashinfo ファイル [49-25](#)
 - Cross-Stack UplinkFast、STP
 - サポート [1-9](#)
 - CWDM SFP [1-30](#)
-
- ## D
- DAACL
 - 「ダウンロード可能な ACL」を参照
 - dCEF、スイッチ スタック内 [38-95](#)
 - default コマンド [2-4](#)
 - description コマンド [12-27](#)
 - DHCP
 - Cisco IOS サーバ データベース
 - 設定 [23-15](#)
 - 説明 [23-7](#)
 - デフォルト設定 [23-10](#)
 - IPv6 DHCP
 - 「DHCPv6」を参照
 - イネーブル化
 - リレー エージェント [23-12](#)
 - DHCP Option 82
 - 回線 ID サブオプション [23-5](#)
 - 概要 [23-4](#)
 - 設定時の注意事項 [23-10](#)
 - デフォルト設定 [23-9](#)
 - 転送アドレス、指定 [23-12](#)
 - パケット フォーマット、サブオプション
 - 回線 ID [23-5](#)
 - リモート ID [23-5](#)
 - 表示 [23-17](#)
 - ヘルパー アドレス [23-12](#)
 - リモート ID サブオプション [23-5](#)
 - DHCPv6
 - DHCPv6 サーバ機能のイネーブル化 [39-17](#)
 - クライアント機能のイネーブル化 [39-19](#)
 - サポート [1-15](#)

- 設定時の注意事項 [39-16](#)
- 説明 [39-6](#)
- デフォルト設定 [39-16](#)
- DHCP オブジェクト トラッキング、プライマリ インターフェイスの設定 [44-11](#)
- DHCP サーバのポートベースのアドレス割り当て
 - 予約済みアドレス [23-29](#)
- DHCP サーバ ポート ベースのアドレス割り当て
 - イネーブル化 [23-29](#)
 - サポート [1-6](#)
 - 設定時の注意事項 [23-28](#)
 - 説明 [23-28](#)
 - デフォルト設定 [23-28](#)
 - 表示 [23-31](#)
- DHCP スヌーピング
 - Option 82 データ挿入 [23-4](#)
 - trusted インターフェイス [23-3](#)
 - untrusted インターフェイス [23-3](#)
 - untrusted メッセージ [23-3](#)
 - エッジ スイッチからの untrusted パケットの受信 [23-3, 23-14](#)
 - 設定時の注意事項 [23-10](#)
 - デフォルト設定 [23-9](#)
 - バインディング データベース
 - 「DHCP スヌーピング バインディング データベース」を参照
 - バインディング テーブルの表示 [23-17](#)
 - プライベート VLAN [23-15](#)
 - メッセージ交換プロセス [23-4](#)
- DHCP スヌーピング バインディング データベース
 - イネーブル化 [23-16](#)
 - エージェント統計情報の消去 [23-17](#)
 - エントリ [23-7](#)
 - 削除
 - データベース エージェント [23-16](#)
 - バインディング [23-17](#)
 - バインディング ファイル [23-16](#)
 - 設定 [23-16](#)
 - 設定時の注意事項 [23-11](#)
 - 説明 [23-7](#)
- データベースの更新 [23-17](#)
- デフォルト設定 [23-9, 23-10](#)
- バインディング [23-7](#)
- バインディングの追加 [23-16](#)
- バインディング ファイル
 - 位置 [23-7](#)
 - フォーマット [23-8](#)
- 表示 [23-17](#)
 - ステータスおよび統計情報 [23-17](#)
 - バインディング エントリ [23-17](#)
- リセット
 - タイムアウト値 [23-16](#)
 - 遅延値 [23-16](#)
- DHCP スヌーピング バインディング テーブル
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP バインディング データベース
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP バインディング テーブル
 - 「DHCP スヌーピング バインディング データベース」を参照
- DHCP ベースの自動設定
 - BOOTP との関係 [3-4](#)
 - 概要 [3-4](#)
 - クライアント要求のメッセージ交換 [3-4](#)
 - サポート [1-6](#)
 - 設定
 - DNS [3-9](#)
 - TFTP サーバ [3-8](#)
 - クライアント側 [3-4](#)
 - サーバ側 [3-7](#)
 - リレー デバイス [3-9](#)
 - リース オプション
 - IP アドレス情報 [3-7](#)
 - コンフィギュレーションファイルの受信 [3-7](#)
 - リレー サポート [1-6, 1-15](#)
 - 例 [3-11](#)
- DHCP ベースの自動設定およびイメージ アップデート
 - 概要 [3-5 ~ 3-6](#)

- 設定 [3-12 ~ 3-15](#)
- Differentiated Services Code Point [36-2](#)
- DiffServ アーキテクチャ、QoS [36-2](#)
- Diffusing Update Algorithm (DUAL) [38-38](#)
- Distance Vector Multicast Routing Protocol (ディスタンスベクトル マルチキャスト ルーティング プロトコル)
 - 「DVMRP」を参照
- distribute-list コマンド [38-108](#)
- DNS
 - DHCP ベースの自動設定 [3-9](#)
 - IPv6 [39-4](#)
 - 概要 [7-16](#)
 - サポート [1-6](#)
 - 設定 [7-17](#)
 - 設定の表示 [7-18](#)
 - デフォルト設定 [7-17](#)
- DNS ベースの SSM マッピング [46-21, 46-23](#)
- Domain Name System (ドメイン ネーム システム)
 - 「DNS」を参照
- DoS 攻撃 [26-1](#)
- dot1q-tunnel switchport モード [14-17](#)
- DRP
 - IPv6 [39-5](#)
 - サポート [1-15](#)
 - 設定 [39-14](#)
 - 説明 [39-5](#)
- DSCP [1-13, 36-2](#)
- DSCP/CoS マップ、QoS [36-65](#)
- DSCP/DSCP 変換マップ、QoS [36-66](#)
- DSCP 出力キューしきい値マップ、QoS [36-19](#)
- DSCP 入力キューしきい値マップ、QoS [36-16](#)
- DTP [1-9, 14-16](#)
- DUAL 有限状態マシン、EIGRP [38-39](#)
- DVMRP
 - DVMRP ルータへの PIM ドメインの接続 [46-54](#)
 - mrinfo 要求、応答 [46-57](#)
 - 概要 [46-10](#)
 - サポート [1-15](#)
 - 自動サマライズ
- サマリー アドレスの設定 [46-62](#)
- ディセーブル化 [46-64](#)
- 相互運用性
 - Cisco IOS ソフトウェア [46-10](#)
 - シスコ デバイス [46-52](#)
- 送信元配信ツリー、構築 [46-10](#)
- トンネル
 - 設定 [46-54](#)
 - ネイバー情報の表示 [46-57](#)
- ネイバー
 - 情報の表示 [46-57](#)
 - デフォルト ルートのアドバタイズ [46-56](#)
 - 非ブルーニング ネイバーとのピアリングの禁止 [46-60](#)
 - 非ブルーニング ネイバーの拒否 [46-59](#)
 - プローブ メッセージによる検出 [46-52](#)
- ユニキャスト ルーティングのイネーブル化 [46-58](#)
- ルーティング テーブル [46-10](#)
- ルート
 - MBONE に入る個数の制限 [46-61](#)
 - Syslog メッセージのしきい値の変更 [46-61](#)
 - 削除 [46-66](#)
 - すべてをアドバタイズ [46-64](#)
 - ネイバーへのデフォルト ルートのアドバタイズ [46-56](#)
 - 表示 [46-66](#)
 - メトリック オフセットの追加 [46-64](#)
 - 優先度 [46-64](#)
 - ユニキャスト ルート アドバタイズメントの制限 [46-52](#)
 - レポート メッセージで取得された DVMRP ルートのキャッシュへの格納 [46-58](#)
- dynamic auto トランキング モード [14-17](#)
- dynamic desirable トランキング モード [14-17](#)
- Dynamic Host Configuration Protocol
 - 「DHCP ベースの自動設定」を参照
- Dynamic Trunking Protocol (ダイナミック トランキング プロトコル)
 - 「DTP」を参照

E

EBGP [38-47](#)EEM 3.2 [34-6](#)

EIGRP

インターフェイス パラメータ、設定 [38-43](#)コンポーネント [38-39](#)スタブルーティング [38-45](#)設定 [38-42](#)定義 [38-38](#)デフォルト設定 [38-40](#)認証 [38-44](#)モニタリング [38-46](#)ELIN ロケーション [28-3](#)

Enhanced IGRP

「EIGRP」を参照

errdisable ステート、BPDU [21-2](#)

EtherChannel

IEEE 802.3ad、説明 [37-7](#)

LACP

システム プライオリティ [37-23](#)ステータスの表示 [37-25](#)他の機能との相互作用 [37-8](#)ポート プライオリティ [37-24](#)ホットスタンバイ ポート [37-23](#)モード [37-8](#)

PAGP

Catalyst 1900 との互換性 [37-22](#)学習方式およびプライオリティの設定 [37-21](#)仮想スイッチとの相互作用 [37-6](#)サポート [1-4](#)集約ポート ラーナー [37-21](#)ステータスの表示 [37-25](#)他の機能との相互作用 [37-7](#)デュアル アクティブ検出 [37-6](#)モード [37-6](#)サポート [1-4](#)自動作成 [37-5, 37-7](#)スタックの変更、作用 [37-10](#)ステータスの表示 [37-25](#)

設定

レイヤ 2 インターフェイス [37-14](#)レイヤ 3 物理インターフェイス [37-17](#)レイヤ 3 ポートチャンネル論理インターフェイス [37-16](#)設定時の注意事項 [37-12](#)説明 [37-2](#)

相互作用

STP [37-12](#)VLAN [37-13](#)

チャンネル グループ

番号付け [37-4](#)物理インターフェイスと論理インターフェイスの
バインド [37-4](#)デフォルト設定 [37-12](#)転送方式 [37-9, 37-20](#)ポート グループ [12-7](#)

ポートチャンネル インターフェイス

説明 [37-4](#)番号付け [37-4](#)レイヤ 3 インターフェイス [38-5](#)ロード バランシング [37-9, 37-20](#)論理インターフェイス、説明 [37-4](#)

EtherChannel ガード

イネーブル化 [21-17](#)説明 [21-10](#)ディセーブル化 [21-18](#)EUI [39-4](#)Express Setup [1-2](#)

「Getting Started Guide」も参照

Extended Universal Identifier

「EUI」を参照

Extensible Authentication Protocol over LAN [10-1](#)

External BGP

「EBGP」を参照

F

- fa0 インターフェイス [1-7](#)
- Fast Uplink Transition Protocol [21-6](#)
- FIB [38-95](#)
- Flex Link
 - VLAN [22-3](#)
 - VLAN ロード バランシングの設定 [22-11](#)
 - 設定 [22-9, 22-10](#)
 - 設定時の注意事項 [22-8](#)
 - 説明 [22-2](#)
 - デフォルト設定 [22-8](#)
 - モニタリング [22-14](#)
 - 優先 VLAN の設定 [22-12](#)
 - リンク ロード バランシング [22-3](#)
- Flex Link マルチキャスト高速コンバージェンス flowcontrol [22-3](#)
 - 設定 [12-22](#)
 - 説明 [12-22](#)
- Forwarding Information Base (転送情報ベース)
 - 「FIB」を参照
- FTP
 - MIB ファイルへのアクセス [B-4](#)
 - イメージ ファイル
 - アップロード [C-35](#)
 - サーバの準備 [C-31](#)
 - ダウンロード [C-32](#)
 - 古いイメージの削除 [C-34](#)
 - コンフィギュレーション ファイル
 - アップロード [C-16](#)
 - 概要 [C-13](#)
 - サーバの準備 [C-14](#)
 - ダウンロード [C-14](#)

G

- get-bulk-request 動作 [33-3](#)
- get-next-request 動作 [33-3, 33-4](#)
- get-request 動作 [33-3, 33-4](#)

get-response 動作 [33-3](#)

GUI

「デバイス マネージャ」および「Network Assistant」を参照

H

- hello タイム
 - MSTP [20-24](#)
 - STP [19-23](#)
- Hot Standby Router Protocol (ホットスタンバイ ルータ プロトコル)
 - 「HSRP」を参照
- HP OpenView [1-6](#)
- HSRP
 - ICMP リダイレクトメッセージのサポート [42-13](#)
 - オブジェクト トラッキング [44-7](#)
 - 概要 [42-2](#)
 - クラスタ グループにバインド [42-13](#)
 - クラスタ スタンバイ グループの考慮事項 [6-12](#)
 - クラスタ設定の自動復旧 [6-13](#)
 - コマンドスイッチの冗長構成 [1-1, 1-8](#)
 - スイッチ スタックの考慮事項 [42-5](#)
 - 設定 [42-5](#)
 - タイマー [42-11](#)
 - 注意事項 [42-6](#)
 - 定義 [42-1](#)
 - デフォルト設定 [42-6](#)
 - トラッキング [42-9](#)
 - 認証ストリング [42-11](#)
 - プライオリティ [42-8](#)
 - モニタリング [42-14](#)
 - ルーティングの冗長構成 [1-14](#)
 - 「クラスタ」、「クラスタ スタンバイ グループ」、および「スタンバイ コマンドスイッチ」も参照
- HTTP over SSL
 - 「HTTPS」を参照
- HTTPS [9-51](#)
 - 自己署名証明書 [9-52](#)
 - 設定 [9-55](#)

- I**
- IBPG [38-47](#)
 - ICMP
 - IPv6 [39-4](#)
 - time-to-live-exceeded メッセージ [49-19](#)
 - traceroute [49-19](#)
 - サポート [1-15](#)
 - 到達不能および ACL [35-22](#)
 - 到達不能メッセージ [35-20](#)
 - 到達不能メッセージおよび IPv6 [41-5](#)
 - リダイレクト メッセージ [38-13](#)
 - ICMP ping
 - 概要 [49-15](#)
 - 実行 [49-16](#)
 - ICMP Router Discovery Protocol
 - 「IRDP」を参照
 - ICMPv6 [39-4](#)
 - ICMP エコー動作
 - IP SLA [43-11](#)
 - 設定 [43-12](#)
 - IDS 装置
 - 入力 RSPAN [30-23](#)
 - 入力 SPAN [30-15](#)
 - IEEE 802.1
 - 「MSTP」を参照
 - IEEE 802.1D
 - 「STP」を参照
 - IEEE 802.1p [16-1](#)
 - IEEE 802.1Q
 - カプセル化 [14-15](#)
 - 設定時の制限事項 [14-18](#)
 - その他の機能を含むトンネル ポート [18-6](#)
 - タグなしトラフィック用のネイティブ VLAN [14-23](#)
 - トランク ポート [12-4](#)
 - トンネリング
 - 説明 [18-2](#)
 - 他の機能との互換性 [18-6](#)
 - デフォルト [18-4](#)
 - IEEE 802.1w
 - 「RSTP」を参照
 - IEEE 802.1x
 - 「ポートベースの認証」を参照
 - IEEE 802.3ad
 - 「EtherChannel」を参照
 - IEEE 802.3af
 - 「PoE」を参照
 - IEEE 802.3X フロー制御 [12-22](#)
 - ifIndex 値、SNMP [33-6](#)
 - IFS [1-7](#)
 - IGMP
 - Join メッセージ [25-3](#)
 - 概要 [46-3](#)
 - キャッシュ エントリの削除 [46-66](#)
 - クエリー [25-4](#)
 - グループの表示 [46-66](#)
 - グループへのアクセスの制御 [46-43](#)
 - 高速スイッチング [46-47](#)
 - サポート [1-5](#)
 - サポートされているバージョン [25-3](#)
 - スイッチの設定
 - グループのメンバー [46-42](#)
 - スタティックに接続されたメンバー [46-47](#)
 - 脱退処理、イネーブル化 [25-11, 40-9](#)
 - 脱退タイマーの設定
 - イネーブル化 [25-12](#)
 - 説明 [25-6](#)
 - デフォルト設定 [46-42](#)
 - バージョン 1
 - 説明 [46-3](#)
 - バージョン 2 への変更 [46-44](#)
 - バージョン 2
 - クエリー タイムアウト [46-46](#)
 - グループのプルーニング [46-46](#)
 - 最大クエリー応答時間 [46-46](#)
 - 説明 [46-4](#)
 - バージョン 1 への変更 [46-44](#)

- フラッディングしたマルチキャスト トラフィック
 - インターフェイスでディセーブル **25-14**
 - クエリー送信要求 **25-13**
 - グローバル Leave **25-13**
 - 時間の制御 **25-13**
 - フラッディング モードからの回復 **25-13**
- ホストクエリー インターバル、変更 **46-45**
- マルチキャスト グループからの脱退 **25-5**
- マルチキャスト グループへの加入 **25-3**
- マルチキャストの到達可能性 **46-42**
- レポート抑制
 - 説明 **25-6**
 - ディセーブル化 **25-16, 40-11**
- IGMP グループ
 - 最大数の設定 **25-28**
 - フィルタリングの設定 **25-29**
- IGMP スヌーピング
 - VLAN コンフィギュレーション **25-8**
 - アドレス エイリアス **25-2**
 - イネーブル化およびディセーブル化 **25-8, 40-7**
 - クエリア
 - 設定 **25-14**
 - 設定時の注意事項 **25-14**
 - グローバル コンフィギュレーション **25-8**
 - サポート **1-5**
 - サポートされているバージョン **25-3**
 - スイッチ スタック内 **25-7**
 - スタック変更 **25-7**
 - 設定 **25-7**
 - 即時脱退 **25-6**
 - 定義 **25-2**
 - デフォルト設定 **25-7, 40-6**
 - 方法 **25-9**
 - モニタリング **25-16, 40-12**
- IGMP スロットリング
 - 設定 **25-29**
 - 説明 **25-25**
 - デフォルト設定 **25-26**
 - 表示 **25-30**
- IGMP 即時脱退
 - イネーブル化 **25-11**
 - 設定時の注意事項 **25-12**
 - 説明 **25-6**
- IGMP フィルタリング
 - サポート **1-5**
 - 設定 **25-26**
 - 説明 **25-25**
 - デフォルト設定 **25-26**
 - モニタリング **25-30**
- IGMP プロファイル
 - コンフィギュレーション モード **25-26**
 - 設定 **25-26**
 - 適用 **25-27**
- IGMP ヘルパー **1-5, 46-7**
- IGP **38-27**
- interfaces range macro コマンド **12-15**
- interface コマンド **12-12 ~ 12-13**
- Interior Gateway Protocol (内部ゲートウェイ プロトコル)
 - 「IGP」を参照
- Internal BGP
 - 「IBGP」を参照
- Internet Control Message Protocol (インターネット制御メッセージプロトコル)
 - 「ICMP」を参照
- Internet Group Management Protocol
 - 「IGMP」を参照
- Internet Protocol バージョン 6
 - 「IPv6」を参照
- Inter-Switch Link (スイッチ間リンク)
 - 「ISL」を参照
- Intrusion Detection System (侵入検知システム)
 - 「IDS 装置」を参照
- IOS シェル
 - 「Auto Smartport マクロ」も参照
- IP ACL
 - QoS の分類 **36-7**
 - 暗黙の拒否 **35-10, 35-15**

- 名前付き **35-15**
- 未定義 **35-21**
- 無視マスク **35-10**
- ip cef distributed コマンド **38-96**
- ip igmp profile コマンド **25-26**
- IP Phone
 - QoS **16-1**
 - QoS によるポートセキュリティの確保 **36-39**
 - QoS 用信頼境界機能 **36-39**
 - 自動分類およびキューイング **36-20**
 - 設定 **16-5**
- IP precedence **36-2**
- IP precedence/DSCP マップ、QoS **36-63**
- IP Service Level Agreements (IP サービス レベル契約)
 - 「IP SLA」を参照
- IP SLA
 - ICMP エコー動作 **43-11**
 - SNMP のサポート **43-2**
 - UDP ジッタ動作 **43-9**
 - 応答側
 - イネーブル化 **43-8**
 - 説明 **43-4**
 - 応答時間 **43-4**
 - オブジェクト トラッキング **44-9**
 - オブジェクト トラッキングの設定 **44-9**
 - コントロール プロトコル **43-4**
 - サポートされるメトリック **43-2**
 - しきい値モニタリング **43-6**
 - スケジューリング **43-5**
 - 設定時の注意事項 **43-6**
 - 定義 **43-1**
 - デフォルト設定 **43-6**
 - 動作 **43-3**
 - 到達可能性トラッキング **44-9**
 - トラック オブジェクト モニタリング エージェント、設定 **44-11**
 - トラック ステート **44-9**
 - ネットワーク パフォーマンスの測定 **43-3**
 - 複数動作のスケジューリング **43-5**
 - モニタリング **43-13**
 - 利点 **43-2**
- IP traceroute
 - 概要 **49-18**
 - 実行 **49-19**
- IPv4 ACL
 - インターフェイスへの適用 **35-20**
 - 拡張、作成 **35-11**
 - 名前付き **35-15**
 - 標準、作成 **35-10**
- IPv4 および IPv6
 - デュアル プロトコル スタック **39-6**
- IPv6
 - ACL
 - 一致条件 **41-3**
 - サポート対象 **41-3**
 - 制限事項 **41-3**
 - 表示 **41-9**
 - ポート **41-2**
 - 優先 **41-2**
 - ルータ **41-2**
 - CEFv6 **39-20**
 - Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 **39-7**
 - EIGRP IPv6 コマンド **39-7**
 - ルータ ID **39-7**
 - ICMP **39-4**
 - OSPF **39-7**
 - SDM テンプレート **8-2, 40-1, 41-1**
 - アドレス **39-2**
 - アドレス形式 **39-2**
 - アドレスの割り当て **39-12**
 - アプリケーション **39-5**
 - 機能制限 **39-9**
 - 近接ディスカバリ **39-4**
 - サポートされない機能 **39-9**
 - サポートされる機能 **39-3**
 - 自動設定 **39-5**
 - スイッチ スタック **39-10**

- スイッチの制限 [39-9](#)
- スタック マスター機能 [39-10](#)
- スタティック ルートの概要 [39-7](#)
- スタティック ルートの設定 [39-21](#)
- ステートレス自動設定 [39-5](#)
- 定義 [39-1](#)
- デフォルト設定 [39-11](#)
- デフォルト ルータ プリファレンス (DRP) [39-5](#)
- 転送 [39-12](#)
- パス MTU ディスカバリ [39-4](#)
- モニタリング [39-28](#)
- IPv6 HSRP
 - 設定 [39-26](#)
 - 注意事項 [39-25](#)
- IPv6 トラフィック、フィルタリング [41-4](#)
- IPv6 による SNMP および Syslog [39-8](#)
- IP アドレス
 - 128 ビット [39-2](#)
 - IPv6 [39-2](#)
 - IP ルーティング [38-6](#)
 - MAC アドレスとの相互作用 [38-10](#)
 - クラス [38-7](#)
 - クラスタ アクセス [6-2](#)
 - 検出 [7-32](#)
 - 候補またはメンバー [6-4, 6-14](#)
 - コマンド スイッチ [6-3, 6-12, 6-14](#)
 - 冗長クラスタ [6-12](#)
 - スタンバイ コマンド スイッチ [6-12, 6-14](#)
 - デフォルト設定 [38-6](#)
 - モニタリング [38-20](#)
 - 「IP 情報」も参照
- IP サービス イメージ [1-1](#)
- IP サービス レベル、分析 [43-1](#)
- IP 指定ブロードキャスト [38-16](#)
- IP 情報
 - デフォルト設定 [3-3](#)
 - 割り当て
 - DHCP ベースの自動設定の使用 [3-4](#)
 - 手動 [3-16](#)
- IP ソース ガード
 - 802.1x [23-20](#)
 - DHCP スヌーピング [23-17](#)
 - EtherChannels [23-20](#)
 - TCAM エントリ [23-20](#)
 - VRF [23-20](#)
 - イネーブル化 [23-21, 23-22](#)
 - スタティック バインディング
 - 削除 [23-21](#)
 - 追加 [23-21, 23-22](#)
 - スタティック ホスト [23-22](#)
 - 設定時の注意事項 [23-20](#)
 - 説明 [23-17](#)
 - 送信元 IP アドレス フィルタリング [23-18](#)
 - 送信元 IP および MAC アドレス フィルタリング [23-18](#)
 - ディセーブル化 [23-21](#)
 - デフォルト設定 [23-20](#)
 - トランク インターフェイス [23-20](#)
 - バインディング設定
 - 自動 [23-18](#)
 - 手動 [23-18](#)
 - バインディング テーブル [23-18](#)
 - 表示
 - アクティブな IP または MAC バインディング [23-27](#)
 - 設定 [23-27](#)
 - バインディング [23-27](#)
 - フィルタリング
 - 送信元 IP アドレス [23-18](#)
 - 送信元 IP および MAC アドレス [23-18](#)
 - プライベート VLAN [23-20](#)
 - プロビジョニングされたスイッチ [23-20](#)
 - ポート セキュリティ [23-20](#)
 - ルーテッド ポート [23-20](#)
- IP ブロードキャスト アドレス [38-18](#)
- IP プロトコル
 - ACL [35-12](#)
 - ルーティング [1-14](#)

- IP ベース イメージ [1-1](#)
- IP マルチキャスト ルーティング
 - IGMP スヌーピング [25-2](#)
 - MBONE
 - sdr キャッシュ エントリの削除 [46-66](#)
 - sdr キャッシュ エントリの存在期間の制限 [46-50](#)
 - sdr キャッシュの表示 [46-67](#)
 - sdr リスナー サポート機能のイネーブル化 [46-49](#)
 - Session Directory (sdr) ツール、説明 [46-49](#)
 - アドバタイズされる DVMRP ルートの制限 [46-61](#)
 - 会議セッション アナウンスメント用の SAP パケット [46-49](#)
 - 説明 [46-49](#)
 - PIMv1 および PIMv2 の相互運用性 [46-12](#)
 - Reverse Path Forwarding (RPF) チェック [46-8](#)
 - RP
 - PIMv2 BSR の設定 [46-33](#)
 - 自動 RP および BSR の使用法 [46-37](#)
 - 自動 RP の設定 [46-28](#)
 - 手動での割り当て [46-27](#)
 - マッピング情報のモニタ [46-38](#)
 - アドレス
 - すべてのホスト [46-3](#)
 - すべてのマルチキャスト ルータ [46-3](#)
 - ホスト グループ アドレス範囲 [46-3](#)
 - イネーブル化
 - PIM モード [46-15](#)
 - マルチキャスト転送 [46-14](#)
 - 管理の有効範囲付き境界、説明 [46-50](#)
 - グループ /RP マッピング
 - BSR [46-7](#)
 - 自動 RP [46-7](#)
 - シスコの実装機能 [46-2](#)
 - 自動 RP
 - BSR による使用法 [46-37](#)
 - 概要 [46-7](#)
 - 既存の SM クラウドへの追加 [46-29](#)
 - キャッシュのクリア [46-66](#)
 - 候補 RP スプーフィングの禁止 [46-31](#)
 - 新規インターネットワークでの設定 [46-29](#)
 - 設定時の注意事項 [46-13](#)
 - 着信 RP アナウンスメント メッセージのフィルタリング [46-31](#)
 - 問題のある RP への Join メッセージの送信禁止 [46-31](#)
 - 利点 [46-28](#)
 - スタッキング
 - スタック マスター機能 [46-11](#)
 - スタック メンバーの機能 [46-11](#)
 - 設定
 - IP マルチキャスト境界 [46-50](#)
 - 基本的なマルチキャストルーティング [46-14](#)
 - デフォルト設定 [46-12](#)
 - 統計情報、システムおよびネットワークの表示 [46-66](#)
 - ブートストラップ ルータ
 - IP マルチキャスト境界の定義 [46-34](#)
 - PIM ドメイン境界の定義 [46-33](#)
 - 概要 [46-7](#)
 - 候補 BSR の設定 [46-35](#)
 - 候補 RP の設定 [46-36](#)
 - 自動 RP による使用法 [46-37](#)
 - 設定時の注意事項 [46-13](#)
 - プロトコルの動作 [46-2](#)
 - マルチキャスト転送、説明 [46-8](#)
 - モニタリング
 - パケット速度および損失情報 [46-67](#)
 - パスのトレース [46-67](#)
 - ピアリング デバイス [46-67](#)
 - ルーティング テーブル
 - 削除 [46-66](#)
 - 表示 [46-66](#)
 - 「CGMP」も参照
 - 「DVMRP」も参照
 - 「IGMP」も参照
 - 「PIM」も参照
- IP ユニキャスト ルーティング

- ARP [38-10](#)
- EtherChannel レイヤ 3 インターフェイス [38-5](#)
- IGP [38-27](#)
- IPv6 [39-3](#)
- IP アドレス指定
 - クラス [38-7](#)
 - 設定 [38-6](#)
- IRDP [38-14](#)
- MAC アドレスと IP アドレス [38-10](#)
- SVI を使用 [38-5](#)
- UDP [38-17](#)
- VLAN 間 [38-2](#)
- アドレス解決 [38-10](#)
- イネーブル化 [38-20](#)
- 管理距離 [38-98, 38-109](#)
- 逆アドレス解決 [38-10](#)
- クラスレス ルーティング [38-8](#)
- 再配信 [38-99](#)
- サブネット ゼロ [38-8](#)
- サブネット マスク [38-7](#)
- 指定ブロードキャスト [38-16](#)
- スーパーネット [38-8](#)
- スタティック ルーティング [38-3](#)
- スタティック ルートの設定 [38-97](#)
- 設定手順 [38-6](#)
- ダイナミック ルーティング [38-3](#)
- ディセーブル化 [38-21](#)
- デフォルト
 - アドレス指定の設定 [38-6](#)
 - ゲートウェイ [38-13](#)
 - ネットワーク [38-98](#)
 - ルーティング [38-3](#)
 - ルート [38-98](#)
- 認証鍵 [38-110](#)
- パッシブ インターフェイス [38-107](#)
- ブロードキャスト
 - アドレス [38-18](#)
 - ストーム [38-15](#)
 - パケット [38-15](#)
 - フラッディング [38-18](#)
- プロキシ ARP [38-10](#)
- プロトコル
 - ダイナミック [38-3](#)
 - ディスタンス ベクタ [38-3](#)
 - リンクステート [38-3](#)
- ルーテッド ポート [38-5](#)
- レイヤ 3 インターフェイス [38-5](#)
- レイヤ 3 インターフェイスへの IP アドレスの割り当て [38-7](#)
- 「BGP」も参照
- 「EIGRP」も参照
- 「OSPF」も参照
- 「RIP」も参照
- IP ルーティング
 - イネーブル化 [38-20](#)
 - インターフェイスの接続 [12-11](#)
 - ディセーブル化 [38-21](#)
- IP ルート、モニタ [38-111](#)
- IRDP
 - サポート [1-15](#)
 - 設定 [38-14](#)
 - 定義 [38-14](#)
- IS-IS
 - show コマンド [38-79](#)
 - アドレス [38-70](#)
 - エリア ルーティング [38-70](#)
 - システム ルーティング [38-70](#)
 - デフォルト設定 [38-71](#)
 - モニタリング [38-79](#)
- ISL
 - IEEE 802.1 トンネリングによるトランキング [18-5](#)
 - IPv6 [39-3](#)
 - カプセル化 [1-9, 14-15](#)
 - トランク ポート [12-4](#)
- ISO CLNS
 - clear コマンド [38-79](#)
 - NET [38-69](#)
 - NSAP [38-69](#)

OSI 規格 [38-69](#)
 ダイナミック ルーティング プロトコル [38-69](#)
 モニタリング [38-79](#)

ISO IGRP

エリア ルーティング [38-70](#)
 システム ルーティング [38-70](#)

J

Join メッセージ、IGMP [25-3](#)

K

KDC

説明 [9-41](#)
 「Kerberos」も参照

Kerberos

KDC [9-41](#)
 TGT [9-42](#)
 暗号化ソフトウェア イメージ [9-40](#)
 サーバ [9-42](#)
 サポート [1-12](#)
 証明書 [9-41](#)
 信頼できるサードパーティとしてのスイッチ [9-41](#)
 設定 [9-44](#)
 設定例 [9-40](#)
 説明 [9-41](#)
 チケット [9-41](#)
 動作 [9-43](#)
 認証
 KDC [9-43](#)
 境界スイッチ [9-43](#)
 ネットワーク サービス [9-44](#)
 用語 [9-41](#)
 レルム [9-42](#)

Key Distribution Center (鍵発行局)

「KDC」を参照

L

l2protocol-tunnel コマンド [18-13](#)

LACP

「EtherChannel」を参照
 レイヤ 2 プロトコル トンネリング [18-9](#)

LDAP [4-2](#)

LED、スイッチ

『Hardware Installation Guide』を参照

Lightweight Directory Access Protocol

「LDAP」を参照

Link Layer Discovery Protocol

「CDP」を参照

Link State Advertisement (LSA) [38-33](#)

LLDP

イネーブル化 [28-6](#)
 概要 [28-1](#)
 サポートされる TLV [28-2](#)
 スイッチ スタックの考慮事項 [28-2](#)
 設定 [28-5](#)
 デフォルト設定 [28-5](#)
 特性 [28-6](#)
 タイマーおよびホールドタイム、設定 [28-6](#)
 モニタおよびメンテナンス [28-11](#)

LLDP-MED

概要 [28-1, 28-2](#)
 サポートされる TLV [28-2](#)
 設定
 TLV [28-7](#)
 手順 [28-5](#)
 モニタおよびメンテナンス [28-11](#)

LLDP Media Endpoint Discovery

「LLDP-MED」を参照

Long-Reach Ethernet (LRE) テクノロジー [1-22, 1-29](#)

LRE プロファイル、スイッチ クラスタの考慮事項 [6-17](#)

- ## M
- MAB
 - 「MAC 認証バイパス」を参照
 - MAB エージング タイマー [1-10](#)
 - MAB 無活動タイマー
 - デフォルト設定 [10-34](#)
 - 範囲 [10-37](#)
 - MAC/PHY コンフィギュレーション ステータス TLV [28-2](#)
 - MAC アドレス
 - ACL [35-28](#)
 - IP アドレスとの相互作用 [38-10](#)
 - IP 送信元バインディングテーブルでの表示 [23-27](#)
 - VLAN でのラーニングのディセーブル化 [7-31](#)
 - VLAN の関連 [7-21](#)
 - アドレス テーブルの作成 [7-21](#)
 - エージング タイム [7-22](#)
 - 検出 [7-32](#)
 - スタティック
 - 許可 [7-30, 7-31](#)
 - 削除 [7-29](#)
 - 追加 [7-29](#)
 - 特性 [7-28](#)
 - 廃棄 [7-30](#)
 - ダイナミック
 - 削除 [7-23](#)
 - ラーニング [7-21](#)
 - デフォルト設定 [7-22](#)
 - 表示 [7-32](#)
 - MAC アドレス通知、サポート [1-16](#)
 - MAC アドレス テーブル移動更新
 - 設定 [22-12](#)
 - 設定時の注意事項 [22-9](#)
 - 説明 [22-6](#)
 - デフォルト設定 [22-8](#)
 - モニタリング [22-14](#)
 - MAC アドレスと VLAN のマッピング [14-27](#)
 - MAC アドレス ラーニング [1-7](#)
 - MAC アドレス ラーニング、VLAN でのディセーブル化 [7-31](#)
 - MAC 拡張アクセス リスト
 - QoS の設定 [36-46](#)
 - QoS の分類 [36-5](#)
 - 作成 [35-28](#)
 - 定義 [35-28](#)
 - レイヤ 2 インターフェイスへの適用 [35-30](#)
 - MAC 認証バイパス [10-36](#)
 - 「MAB」を参照
 - 概要 [10-16](#)
 - 設定 [10-56](#)
 - maximum-paths コマンド [38-56, 38-97](#)
 - MDA
 - 設定時の注意事項 [10-12 ~ 10-13](#)
 - 説明 [1-11, 10-12](#)
 - 認証プロセスの例外 [10-5](#)
 - Medianet
 - 「Auto Smartport マクロ」を参照
 - MHSRP [42-4](#)
 - MIB
 - FTP によるファイルへのアクセス [B-4](#)
 - SNMP との相互作用 [33-4](#)
 - 概要 [33-1](#)
 - サポート対象 [B-1](#)
 - ファイルの位置 [B-4](#)
 - Mini-Point-of-Presence
 - 「POP」を参照
 - MSDP
 - DM 領域
 - SA メッセージの送信 [47-16](#)
 - 発信元アドレスの設定 [47-17](#)
 - MSDP 接続および統計情報のクリア [47-18](#)
 - SA メッセージ
 - TTL によるデータの制限 [47-13](#)
 - アドバタイズされる送信元の制限 [47-9](#)
 - キャッシュ エントリのクリア [47-18](#)
 - キャッシング [47-6](#)
 - 着信のフィルタリング [47-14](#)

- 定義 [47-2](#)
- ピアからのフィルタリング [47-10](#)
- ピアへのフィルタリング [47-12](#)
- モニタリング [47-18](#)
- 概要 [47-1](#)
- 加入遅延、定義 [47-6](#)
- サポート [1-15](#)
- 送信元情報の制御
 - スイッチから発信 [47-8](#)
 - スイッチで受信 [47-13](#)
 - スイッチで転送 [47-11](#)
- デフォルト設定 [47-4](#)
- 発信元アドレス、変更 [47-17](#)
- ピア
 - シャットダウン [47-16](#)
 - 送信元情報の要求 [47-8](#)
 - デフォルトの設定 [47-4](#)
 - ピアリング関係、概要 [47-1](#)
 - モニタリング [47-18](#)
- ピア RPF フラッドイング [47-2](#)
- フィルタリング
 - 着信 SA メッセージ [47-14](#)
 - ピアからの SA 要求メッセージ [47-10](#)
 - ピアへの SA メッセージ [47-12](#)
- メッシュ グループ
 - 設定 [47-15](#)
 - 定義 [47-15](#)
- 利点 [47-3](#)
- MSTP
 - BPDU ガード
 - イネーブル化 [21-13](#)
 - 説明 [21-2](#)
 - BPDU フィルタリング
 - イネーブル化 [21-15](#)
 - 説明 [21-3](#)
 - CIST、説明 [20-3](#)
 - CIST リージョナルルート [20-3, 20-5](#)
 - CIST ルート [20-5](#)
 - CST
 - 定義 [20-3](#)
 - リージョン間の動作 [20-4](#)
- EtherChannel ガード
 - イネーブル化 [21-17](#)
 - 説明 [21-10](#)
- IEEE 802.1
 - 実装 [20-7](#)
 - ポートの役割名の変更 [20-7](#)
 - 用語 [20-5](#)
- IEEE 802.1D STP との相互運用性
 - 移行プロセスの再起動 [20-27](#)
 - 説明 [20-9](#)
- IST
 - 定義 [20-3](#)
 - マスター [20-3](#)
 - リージョン内の動作 [20-3](#)
- MST リージョン
 - CIST [20-3](#)
 - IST [20-3](#)
 - サポートされるスパニング ツリー インスタンス [20-2](#)
 - 設定 [20-17](#)
 - 説明 [20-2](#)
 - ホップ カウント メカニズム [20-6](#)
- PortFast
 - イネーブル化 [21-12](#)
 - 説明 [21-2](#)
- PortFast 対応ポートのシャットダウン [21-2](#)
- VLAN と MST インスタンスのマッピング [20-18](#)
- インターフェイス ステート、ブロッキングからフォワードイング [21-2](#)
- オプション機能のデフォルト設定 [21-12](#)
- 概要 [20-2](#)
- 拡張システム ID
 - 異常動作 [20-19](#)
 - セカンダリ ルート スイッチへの影響 [20-20](#)
 - ルート スイッチへの影響 [20-19](#)
- 境界ポート
 - 設定時の注意事項 [20-17](#)

説明 **20-6**

サポートされるインスタンス **19-11**

サポートされるオプション機能 **1-9**

スタックの変更、作用 **20-9**

ステータスの表示 **20-28**

ステータス、表示 **20-28**

設定

hello タイム **20-24**

MST リージョン **20-17**

高速コンバージェンス用リンク タイプ **20-26**

最大エージング タイム **20-25**

最大ホップ カウント **20-26**

スイッチ プライオリティ **20-23**

セカンダリ ルート スイッチ **20-20**

転送遅延時間 **20-25**

ネイバー タイプ **20-27**

パス コスト **20-22**

ポート プライオリティ **20-21**

ルート スイッチ **20-19**

設定時の注意事項 **20-16, 21-12**

デフォルト設定 **20-16**

モード間の相互運用性と下位互換性 **19-11**

モードのイネーブル化 **20-17**

ルート ガード

イネーブル化 **21-18**

説明 **21-10**

ルート スイッチ

異常動作 **20-19**

拡張システム ID の影響 **20-19**

設定 **20-19**

ルート スイッチとしての選択防止 **21-10**

ループ ガード

イネーブル化 **21-19**

説明 **21-11**

multiauth

アクセス不能認証バイパスのサポート **10-23**

Multicast Source Discovery Protocol

「MSDP」を参照

Multicast VLAN Registration (マルチキャスト VLAN レジストレーション)

「MVR」を参照

Multiple HSRP

「MHSRP」を参照

MVR

IGMPv3 **25-21**

アドレス エイリアス **25-21**

アプリケーション例 **25-19**

インターフェイスの設定 **25-23**

グローバル パラメータの設定 **25-21**

サポート **1-5**

スイッチ スタック内 **25-20**

設定時の注意事項 **25-21**

説明 **25-18**

デフォルト設定 **25-20**

マルチキャスト TV アプリケーション **25-19**

モード **25-22**

モニタリング **25-24**

N

NAC

AAA ダウン ポリシー **1-12**

RADIUS サーバを使用した IEEE 802.1X 検証 **10-58**

RADIUS サーバを使用する IEEE 802.1X 認証 **10-58**

アクセス不能認証バイパス **1-12, 10-53**

クリティカル認証 **10-23, 10-53**

レイヤ 2 IEEE 802.1X 検証 **10-28, 10-58**

レイヤ 2 IEEE 802.1x 検証 **1-12**

レイヤ 2 IP 検証 **1-12**

Namespace Mapper

「NSM」を参照

NEAT

概要 **10-30**

設定 **10-59**

Network Admission Control (ネットワーク アドミッション制御)

- NAC
 - Network Assistant
 - イメージファイルのダウンロード [1-3](#)
 - ウィザード [1-3](#)
 - ガイドモード [1-2](#)
 - 管理オプション [1-2](#)
 - スイッチ スタックの管理 [5-2, 5-16](#)
 - スイッチのアップグレード [C-25](#)
 - 説明 [1-6](#)
 - 利点 [1-2](#)
 - Network Edge Access Topology
 - 「NEAT」を参照
 - Network Time Protocol
 - 「NTP」を参照
 - no switchport コマンド [12-5](#)
 - Not-So-Stubby-Area
 - 「NSSA」を参照
 - no コマンド [2-4](#)
 - NSAP、ISO IGRP アドレス [38-70](#)
 - NSF 認識
 - IS-IS [38-72](#)
 - NSM [4-3](#)
 - NSSA、OSPF [38-33](#)
 - NTP
 - アクセスの制限
 - アクセス グループの作成 [7-9](#)
 - インターフェイスごとの NTP サービスのディセーブル化 [7-10](#)
 - アソシエーション
 - サーバ [7-6](#)
 - 定義 [7-2](#)
 - 認証 [7-5](#)
 - ピア [7-6](#)
 - ブロードキャスト メッセージのイネーブル化 [7-7](#)
 - 概要 [7-2](#)
 - サポート [1-7](#)
 - ストラタム [7-2](#)
 - 設定の表示 [7-11](#)
 - 送信元 IP アドレス、設定 [7-10](#)
 - タイム
 - サービス [7-2](#)
 - 同期化 [7-2](#)
 - デバイスの同期化 [7-6](#)
 - デフォルト設定 [7-4](#)
-
- ## O
- Open1x
 - 設定 [10-64](#)
 - Open1x 認証
 - 概要 [10-29](#)
 - Open Shortest Path First
 - 「OSPF」を参照
 - OSPF
 - IPv6 [39-7](#)
 - LSA グループ同期設定 [38-36](#)
 - インターフェイス パラメータ、設定 [38-32](#)
 - エリア パラメータ、設定 [38-33](#)
 - 仮想リンク [38-35](#)
 - サポート [1-15](#)
 - 設定 [38-31](#)
 - 説明 [38-27](#)
 - デフォルト設定
 - 設定 [38-29](#)
 - メトリック [38-35](#)
 - ルート [38-35](#)
 - モニタリング [38-37](#)
 - ルータ ID [38-37](#)
 - ルート サマライズ [38-34](#)
-
- ## P
- PAGP
 - 「EtherChannel」を参照
 - レイヤ 2 プロトコル トンネリング [18-9](#)
 - PBR
 - PBR の高速スイッチング [38-106](#)

- イネーブル化 [38-105](#)
- 定義 [38-103](#)
- ローカル PBR [38-107](#)
- PC (パッシブ クラスタ コマンド スイッチ) [6-11](#)
- PE/CE ルーティング、設定 [38-89](#)
- Per-VLAN Spanning-Tree plus
 - 「PVST+」を参照
- PE デバイス [38-81](#)
- PIM
 - dense (稠密) モード
 - RPF チェック [46-9](#)
 - 概要 [46-5](#)
 - ランデブー ポイント (RP)、説明 [46-5](#)
 - sparse (希薄) モード
 - Join メッセージおよび共有ツリー [46-5](#)
 - Prune メッセージ [46-5](#)
 - RPF チェック [46-9](#)
 - 概要 [46-5](#)
 - SPT、使用の延期 [46-40](#)
 - 概要 [46-4](#)
 - 共有ツリーおよび送信元ツリー、概要 [46-38](#)
 - サポート [1-15](#)
 - スタブ ルーティング
 - イネーブル化 [46-25](#)
 - 概要 [46-5](#)
 - 設定時の注意事項 [46-25](#)
 - 表示 [46-67](#)
 - デフォルト設定 [46-12](#)
 - ネイバーの表示 [46-67](#)
 - バージョン
 - v2 の改善点 [46-4](#)
 - 相互運用性 [46-12](#)
 - 相互運用性に関するトラブルシューティング [46-38](#)
 - モードのイネーブル化 [46-15](#)
 - ルータクエリー メッセージ インターバル、変更 [46-41](#)
- PIM/DVMRP、スヌーピング方法 [25-9](#)
- ping
 - 概要 [49-15](#)
 - 実行 [49-16](#)
 - 文字出力の説明 [49-16](#)
- PoE
 - CDP の電力ネゴシエーション拡張機能 [12-8](#)
 - IEEE 電力分類レベル [12-9](#)
 - 固定モード [12-10](#)
 - サポートされるデバイス [12-8](#)
 - サポート対象の標準 [12-8](#)
 - シスコのインテリジェント電力管理 [12-8](#)
 - 自動モード [12-10](#)
 - 受電装置検出および初期電力割り当て [12-9](#)
 - 設定 [12-24](#)
 - 低電力モードで動作する高電力デバイス [12-8](#)
 - 電力管理モード [12-10](#)
 - 電力消費 [12-25](#)
 - 電力消費を含む CDP、説明 [12-8](#)
 - 電力をネゴシエーションする CDP、説明 [12-8](#)
 - トラブルシューティング [49-13](#)
 - パワー バジレット [12-25](#)
- Policy-Based Routing (ポリシーベース ルーティング)
 - 「PBR」を参照
- POP [1-28](#)
- PortFast
 - イネーブル化 [21-12](#)
 - サポート [1-9](#)
 - 説明 [21-2](#)
 - モード、スパニング ツリー [14-29](#)
- Power over Ethernet
 - 「PoE」を参照
- Protocol-Independent Multicast Protocol
 - 「PIM」を参照
- PVST+
 - IEEE 802.1Q トランクの相互運用性 [19-12](#)
 - サポートされるインスタンス [19-11](#)
 - 説明 [19-10](#)

Q

QoS

IP Phone

検出および信頼設定 **36-20, 36-39**

自動分類およびキューイング **36-20**

MQC コマンド **36-1**

QoS ラベル、定義 **36-4**

暗黙の拒否 **36-7**

概要 **36-2**

書き換え **36-20**

基本モデル **36-4**

キュー

SRR、説明 **36-14**

WTD、説明 **36-13**

位置 **36-13**

出力キューの特性の設定 **36-72**

入力キューの特性の設定 **36-68**

ハイ プライオリティ (緊急) **36-19, 36-79**

クラス マップ

設定 **36-47**

表示 **36-80**

グローバルなイネーブル化 **36-36**

サポート **1-13**

自動 QoS

VoIP 用のイネーブル化 **36-27**

実行コンフィギュレーションへの影響 **36-26**

出力キューのデフォルト **36-21**

初期設定の表示 **36-30**

生成コマンドの表示 **36-28**

生成コマンドのリスト **36-22**

設定およびデフォルトの表示 **36-30**

設定時の注意事項 **36-26**

設定例 **36-29**

説明 **36-20**

ディセーブル化 **36-28**

トラフィックの分類 **36-21**

入力キューのデフォルト **36-21**

出力インターフェイスの帯域幅の制限 **36-79**

出力キュー

DSCP または CoS 値のマッピング **36-75**

SRR の共有重みの設定 **36-78**

SRR のシェーピング重みの設定 **36-76**

WTD しきい値の設定 **36-73**

WTD、説明 **36-19**

しきい値マップの表示 **36-76**

スケジューリング、説明 **36-4**

説明 **36-4**

バッファ スペースの割り当て **36-73**

バッファ割り当て方式、説明 **36-18**

フローチャート **36-17**

信頼状態

信頼性のあるデバイス **36-39**

説明 **36-5**

ドメイン内 **36-37**

別のドメインとの境界 **36-41**

設定

DSCP マップ **36-62**

IP 拡張 ACL **36-45**

IP 標準 ACL **36-44**

MAC ACL **36-46**

自動 QoS **36-20**

集約ポリサー **36-60**

出力キューの特性 **36-72**

信頼境界機能 **36-39**

デフォルトのポート CoS 値 **36-39**

透過的な DSCP **36-41**

ドメイン内のポートの信頼状態 **36-37**

入力キューの特性 **36-68**

別のドメインとの境界の DSCP 信頼状態 **36-41**

ポリシー マップ、階層型 **36-53**

設定時の注意事項

自動 QoS **36-26**

標準 QoS **36-34**

デフォルトの自動設定 **36-21**

デフォルトの標準設定 **36-31**

透過的な DSCP **36-41**

- 統計情報の表示 [36-80](#)
 - 入力キュー
 - DSCP または CoS 値のマッピング [36-68](#)
 - SRR の共有重みの設定 [36-70](#)
 - WTD しきい値の設定 [36-68](#)
 - WTD、説明 [36-16](#)
 - しきい値マップの表示 [36-69](#)
 - スケジューリング、説明 [36-4](#)
 - 説明 [36-4](#)
 - 帯域幅の割り当て [36-70](#)
 - バッファおよび帯域幅の割り当て、説明 [36-16](#)
 - バッファ スペースの割り当て [36-70](#)
 - プライオリティ キュー、説明 [36-16](#)
 - プライオリティ キューの設定 [36-71](#)
 - フローチャート [36-15](#)
 - パケットの変更 [36-20](#)
 - フローチャート
 - 出力のキューイングおよびスケジューリング [36-17](#)
 - 入力キューイングおよびスケジューリング [36-15](#)
 - 分類 [36-6](#)
 - ポリシングおよびマーキング [36-10](#)
 - 分類
 - DSCP の信頼状態、説明 [36-5](#)
 - IP ACL、説明 [36-5, 36-7](#)
 - IP precedence の信頼状態、説明 [36-5](#)
 - IP トラフィックのオプション [36-5](#)
 - MAC ACL、説明 [36-5, 36-7](#)
 - クラス マップ、説明 [36-7](#)
 - 信頼性のある CoS 値、説明 [36-5](#)
 - 定義 [36-4](#)
 - 転送処理 [36-3](#)
 - 透過的な DSCP、説明 [36-41](#)
 - 非 IP トラフィックのオプション [36-5](#)
 - フレームおよびパケット [36-3](#)
 - フローチャート [36-6](#)
 - ポリシー マップ、説明 [36-7](#)
 - ポリサー
 - 数 [36-35](#)
 - 設定 [36-52, 36-57, 36-60](#)
 - 説明 [36-8](#)
 - タイプ [36-9](#)
 - 表示 [36-80](#)
 - ポリシー、インターフェイスへの結合 [36-9](#)
 - ポリシー マップ
 - SVI の階層 [36-53](#)
 - 階層 [36-8](#)
 - 特性 [36-49](#)
 - 表示 [36-81](#)
 - 物理ポートの非階層型 [36-49](#)
 - ポリシング
 - 説明 [36-4, 36-8](#)
 - トークン バケット アルゴリズム [36-9](#)
 - マーキング、説明 [36-4, 36-8](#)
 - マークダウン アクション [36-52, 36-57](#)
 - マッピング テーブル
 - CoS/DSCP [36-62](#)
 - DSCP/CoS [36-65](#)
 - DSCP/DSCP 変換 [36-66](#)
 - IP precedence/DSCP [36-63](#)
 - タイプ [36-12](#)
 - 表示 [36-80](#)
 - ポリシング済み DSCP [36-64](#)
- Quality of Service
「QoS」を参照
-
- ## R
- ### RADIUS
- AAA サーバ グループの定義 [9-32](#)
 - アトリビュート
 - ベンダー固有 [9-36](#)
 - ベンダー独自 [9-38](#)
 - 概要 [9-18](#)
 - クラスタ内 [6-17](#)
 - サーバの識別 [9-28](#)
 - サーバ ロード バランシング [9-40](#)

- サポート **1-12**
- 推奨するネットワーク環境 **9-19**
- 設定
 - アカウントिंग **9-35**
 - 許可 **9-34**
 - 通信、グローバル **9-28, 9-36**
 - 通信、サーバ単位 **9-28**
 - 認証 **9-30**
 - 複数の UDP ポート **9-28**
- 設定の表示 **9-40**
- デフォルト設定 **9-28**
- 動作 **9-20**
- 方式リスト、定義 **9-27**
- ユーザがアクセスしたサービスのトラッキング **9-35**
- ユーザへのサービスの制限 **9-34**
- RADIUS Change of Authorization (CoA) **9-20**
- Rapid Per-VLAN Spanning-Tree plus
 - 「Rapid PVST+」を参照
- Rapid PVST+
 - IEEE 802.1Q トランクの相互運用性 **19-12**
 - サポートされるインスタンス **19-11**
 - 説明 **19-10**
- Rapid Spanning Tree Protocol
 - 「RSTP」を参照
- RARP **38-10**
- rcommand コマンド **6-17**
- RCP
 - イメージファイル
 - アップロード **C-40**
 - サーバの準備 **C-36**
 - ダウンロード **C-38**
 - 古いイメージの削除 **C-39**
 - コンフィギュレーション ファイル
 - アップロード **C-19**
 - 概要 **C-17**
 - サーバの準備 **C-17**
 - ダウンロード **C-18**
- Remote Authentication Dial-In User Service
 - 「RADIUS」を参照
- Remote Copy Protocol
 - 「RCP」を参照
- Remote Network Monitoring
 - 「RMON」を参照
- Reverse Address Resolution Protocol (逆アドレス解決プロトコル)
 - 「RARP」を参照
- RFC
 - 1058、RIP **38-21**
 - 1112、IP マルチキャストおよび IGMP **25-2**
 - 1157、SNMPv1 **33-2**
 - 1163、BGP **38-47**
 - 1166、IP アドレス **38-7**
 - 1253、OSPF **38-27**
 - 1267、BGP **38-47**
 - 1305、NTP **7-2**
 - 1587、NSSA **38-28**
 - 1757、RMON **31-2**
 - 1771、BGP **38-47**
 - 1901、SNMPv2C **33-2**
 - 1902 ~ 1907、SNMPv2 **33-2**
 - 2236、IP マルチキャストおよび IGMP **25-2**
 - 2273 ~ 2275、SNMPv3 **33-2**
- RFC 5176 準拠性 **9-22**
- RIP
 - IPv6 **39-7**
 - アドバタイズメント **38-22**
 - サポート **1-14**
 - サマリー アドレス **38-25**
 - スプリット ホライズン **38-25**
 - 設定 **38-23**
 - 説明 **38-22**
 - デフォルト設定 **38-22**
 - 認証 **38-25**
 - ホップ カウント **38-22**
- RMON
 - アラームおよびイベントのイネーブル化 **31-3**
 - 概要 **31-1**

サポート **1-16**

サポート対象グループ **31-2**

ステータスの表示 **31-6**

デフォルト設定 **31-3**

統計情報

- イーサネット グループの収集 **31-6**
- グループ履歴の収集 **31-5**

route-map コマンド **38-106**

Routing Information Protocol

- 「RIP」を参照

RPS

- 「Cisco Redundant Power System 2300」を参照

RPS 2300

- 「Cisco Redundant Power System 2300」を参照

RSPAN

- VLAN ベース **30-7**
- 宛先ポート **30-8**
- 概要 **1-16, 30-1**
- 受信トラフィック **30-5**
- スイッチ スタック **30-2**
- スタック変更 **30-10**
- ステータスの表示 **30-26**
- セッション

 - SPAN 送信元トラフィックの特定の VLAN への制限 **30-25**
 - 作成 **30-19**
 - 着信トラフィックのイネーブル化 **30-23**
 - 定義 **30-4**
 - モニタ対象ポートの指定 **30-19**

- セッション限度 **30-11**
- 設定時の注意事項 **30-18**
- 送信トラフィック **30-6**
- 送信元ポート **30-6**
- 他の機能との相互作用 **30-9**
- 定義 **30-3**
- デフォルト設定 **30-11**
- 特性 **30-9**
- モニタ側ポート **30-8**
- モニタ対象ポート **30-6**

RSTP

BPDU

- 処理 **20-14**
- フォーマット **20-13**

IEEE 802.1D STP との相互運用性

- 移行プロセスの再起動 **20-27**
- 説明 **20-9**
- トポロジの変更 **20-14**

「MSTP」も参照

- アクティブ トポロジ **20-10**

概要 **20-10**

高速コンバージェンス

- エッジ ポートおよび PortFast **20-11**
- クロススタック高速コンバージェンス **20-12**
- 説明 **20-11**
- ポイントツーポイント リンク **20-11, 20-26**
- ルート ポート **20-11**
- 指定スイッチ、定義 **20-10**
- 指定ポート、定義 **20-10**
- 提案 / 合意ハンドシェイク プロセス **20-11**
- ポートの役割

 - 説明 **20-10**
 - 同期 **20-12**

- ルート ポート、定義 **20-10**

S

SCP

- SSH **9-57**
- 設定 **9-58**

「SCP」を参照

SC (スタンバイ クラスタ コマンド スイッチ) **6-11**

SDM

- スイッチ スタックの考慮事項 **5-9**
- テンプレート

 - 数 **8-1**
 - 設定 **8-6**

SDM テンプレート **41-4**

- アグリゲータ **8-1**

- 設定 [8-5](#)
- 設定時の注意事項 [8-5](#)
- タイプ [8-1](#)
- デスクトップ [8-1](#)
- デュアル IPv4/IPv6 [8-2](#)
- SDM 不一致モード [5-9, 8-4](#)
- Secure Copy Protocol
- Secure Shell (セキュア シェル)
 - 「SSH」を参照
- Secure Socket Layer
 - 「SSL」を参照
- set-request 動作 [33-4](#)
- SFP
 - ステータスのモニタリング [12-35, 49-15](#)
 - ステータス、表示 [49-15](#)
 - セキュリティおよび ID [49-14](#)
 - 番号付け [12-13](#)
- Shaped Round Robin (シェイプド ラウンド ロビン)
 - 「SRR」を参照
- show access-lists hardware counters コマンド [35-22](#)
- show cdp traffic コマンド [27-5](#)
- show cluster members コマンド [6-17](#)
- show configuration コマンド [12-27](#)
- show forward コマンド [49-23](#)
- show interfaces switchport [22-4](#)
- show interfaces コマンド [12-21, 12-27](#)
- show l2protocol コマンド [18-14, 18-16, 18-17](#)
- show lldp traffic コマンド [28-11](#)
- show platform forward コマンド [49-23](#)
- show running-config コマンド
 - ACL の表示 [35-20, 35-21, 35-33, 35-35](#)
 - インターフェイスの記述 [12-27](#)
- show および more コマンド出力、フィルタリング [2-10](#)
- shutdown コマンド、インターフェイス上 [12-36](#)
- Simple Network Management Protocol (簡易ネットワーク管理プロトコル)
 - 「SNMP」を参照
- Small Form-factor Pluggable (SFP) モジュール
 - 「SFP」を参照
- SmartPort マクロ
 - グローバル パラメータ値の適用 [13-18](#)
 - シスコのデフォルト マクロの適用 [13-18](#)
 - 設定時の注意事項 [13-17](#)
 - 定義 [13-1](#)
 - デフォルト設定 [13-17](#)
 - トレース [13-17](#)
 - 表示 [13-20](#)
 - 「Auto Smartport マクロ」も参照
- SNAP [27-1](#)
- SNMP
 - CPU しきい値通知の設定 [33-17](#)
 - ifIndex 値 [33-6](#)
 - IP SLA [43-2](#)
 - MIB
 - 位置 [B-4](#)
 - サポート対象 [B-1](#)
 - MIB 変数のアクセス [33-4](#)
 - NMS に送信される Syslog メッセージの制限 [32-10](#)
 - TFTP サーバによるアクセスの制限 [33-18](#)
 - エージェント
 - 説明 [33-4](#)
 - ディセーブル化 [33-8](#)
 - エンジン ID [33-7](#)
 - 概要 [33-1, 33-4](#)
 - クラスタ内 [6-15](#)
 - クラスタの管理 [6-18](#)
 - グループ [33-7, 33-10](#)
 - コミュニティ ストリング
 - 概要 [33-4](#)
 - クラスタ スイッチ用 [33-4](#)
 - 設定 [33-8](#)
 - サポートされているバージョン [33-2](#)
 - システム コンタクトおよびロケーション [33-17](#)
 - 情報
 - trap キーワード [33-13](#)
 - イネーブル化 [33-16](#)
 - 説明 [33-5](#)

- ディセーブル化 [33-16](#)
- トラップとの相違 [33-5](#)
- ステータス、表示 [33-20](#)
- セキュリティ レベル [33-3](#)
- 設定例 [33-19](#)
- 帯域内管理 [1-7](#)
- 通知 [33-5](#)
- デフォルト設定 [33-7](#)
- トラップ
 - MACアドレス通知のイネーブル化 [7-23, 7-25, 7-27](#)
 - イネーブル化 [33-13](#)
 - 概要 [33-1, 33-4](#)
 - 情報との相違 [33-5](#)
 - 説明 [33-3, 33-5](#)
 - タイプ [33-13](#)
 - ディセーブル化 [33-16](#)
 - トラップ マネージャ、設定 [33-14](#)
 - 認証レベル [33-11](#)
 - ホスト [33-7](#)
 - マネージャ機能 [1-6, 33-3](#)
 - ユーザ [33-7, 33-10](#)
- SNMPv1 [33-2](#)
- SNMPv2C [33-2](#)
- SNMPv3 [33-2](#)
- Source-Specific Multicast
 - 「SSM」を参照
- SPAN
 - VLAN ベース [30-7](#)
 - 宛先ポート [30-8](#)
 - 概要 [1-16, 30-1](#)
 - 受信トラフィック [30-5](#)
 - スタック変更 [30-10](#)
 - ステータスの表示 [30-26](#)
 - セッション
 - SPAN 送信元トラフィックの特定の VLAN への制限 [30-17](#)
 - 宛先ポートの削除 [30-14](#)
 - 作成 [30-12](#)
 - 着信トラフィックのイネーブル化 [30-15](#)
 - 定義 [30-4](#)
 - 入力転送の設定 [30-16, 30-24](#)
 - モニタ対象ポートの指定 [30-12](#)
 - セッション限度 [30-11](#)
 - 設定時の注意事項 [30-11](#)
 - 送信トラフィック [30-6](#)
 - 送信元ポート [30-6](#)
 - 他の機能との相互作用 [30-9](#)
 - デフォルト設定 [30-11](#)
 - ポート、制約 [26-12](#)
 - モニタ側ポート [30-8](#)
 - モニタ対象ポート [30-6](#)
- Spanning Tree Protocol (スパニング ツリー プロトコル)
 - 「STP」を参照
- SPAN トラフィック [30-5](#)
- SRR
 - 共有モード [36-14](#)
 - サポート [1-14](#)
 - シェーピング モード [36-14](#)
 - 設定
 - 出力キューでのシェーピング重み [36-76](#)
 - 出力キューの共有重み [36-78](#)
 - 入力キューの共有重み [36-70](#)
 - 説明 [36-14](#)
- SSH
 - 暗号化ソフトウェア イメージ [9-46](#)
 - 暗号化方式 [9-47](#)
 - スイッチ スタックの考慮事項 [5-16, 9-47](#)
 - 設定 [9-48](#)
 - 説明 [1-7, 9-46](#)
 - ユーザ認証方式、サポートされている [9-47](#)
- SSL
 - 暗号化ソフトウェア イメージ [9-51](#)
 - セキュア HTTP クライアントの設定 [9-56](#)
 - セキュア HTTP サーバの設定 [9-55](#)
 - 設定時の注意事項 [9-54](#)
 - 説明 [9-51](#)
 - モニタリング [9-57](#)

- SSM
- CGMP の制限事項 [46-18](#)
 - IGMPv3 [46-16](#)
 - IGMPv3 ホスト シグナリング [46-17](#)
 - IGMP スヌーピング [46-18](#)
 - IP アドレスの範囲 [46-16](#)
 - PIM [46-16](#)
 - アドレス管理の制約事項 [46-18](#)
 - インターネット標準マルチキャストとの違い [46-16](#)
 - コンポーネント [46-16](#)
 - ステート管理の制限事項 [46-18](#)
 - 設定 [46-15, 46-18](#)
 - 設定時の注意事項 [46-17](#)
 - 動作 [46-17](#)
 - モニタリング [46-18](#)
- SSM マッピング [46-19](#)
- DNS ベース [46-21, 46-23](#)
 - 概要 [46-20](#)
 - スタティック [46-20, 46-22](#)
 - スタティック トラフィック フォワーディング [46-23](#)
 - 制約事項 [46-20](#)
 - 設定 [46-19, 46-22](#)
 - 設定時の注意事項 [46-19](#)
 - モニタリング [46-24](#)
- StackWise テクノロジー、Cisco [1-3](#)
- 「スタック、スイッチ」も参照
- standby ip コマンド [42-7](#)
- STP
- BackboneFast
 - イネーブル化 [21-17](#)
 - 説明 [21-7](#)
 - ディセーブル化 [21-17](#)
 - BPDU ガード
 - イネーブル化 [21-13](#)
 - 説明 [21-2](#)
 - ディセーブル化 [21-14](#)
 - BPDU フィルタリング
 - イネーブル化 [21-15](#)
 - 説明 [21-3](#)
 - ディセーブル化 [21-15](#)
 - BPDU メッセージ交換 [19-3](#)
 - EtherChannel ガード
 - イネーブル化 [21-17](#)
 - 説明 [21-10](#)
 - ディセーブル化 [21-18](#)
 - IEEE 802.1Q トランクに関する制限事項 [19-12](#)
 - IEEE 802.1D およびブリッジ ID [19-5](#)
 - IEEE 802.1D およびマルチキャストアドレス [19-9](#)
 - IEEE 802.1t および VLAN ID [19-5](#)
 - PortFast
 - イネーブル化 [21-12](#)
 - 説明 [21-2](#)
 - PortFast 対応ポートのシャットダウン [21-2](#)
 - UplinkFast
 - イネーブル化 [21-16](#)
 - 説明 [21-3](#)
 - VLAN ブリッジ [19-12](#)
 - インターフェイス ステート
 - 概要 [19-5](#)
 - ディセーブル [19-8](#)
 - 転送 [19-6, 19-8](#)
 - ブロッキング [19-7](#)
 - ラーニング [19-7](#)
 - リスニング [19-7](#)
 - インターフェイス ステート、ブロッキングからフォワーディング [21-2](#)
 - オプション機能のデフォルト設定 [21-12](#)
 - 下位 BPDU [19-3](#)
 - 概要 [19-2](#)
 - カウンタ、クリア [19-25](#)
 - 拡張システム ID
 - 異常動作 [19-17](#)
 - 概要 [19-5](#)
 - セカンダリ ルート スイッチへの影響 [19-18](#)
 - ルート スイッチへの影響 [19-17](#)
 - 間接リンク障害の検出 [21-8](#)

- クロススタック UplinkFast
 - イネーブル化 [21-17](#)
 - 説明 [21-5](#)
- サポートされるインスタンス [19-11](#)
- サポートされるオプション機能 [1-9](#)
- サポートされる機能 [1-8](#)
- サポートされるプロトコル [19-10](#)
- サポートされるモード [19-10](#)
- 指定スイッチ、定義 [19-4](#)
- 指定ポート、定義 [19-4](#)
- 冗長接続 [19-9](#)
- スイッチスタックでのルートポートの選択 [19-4](#)
- スタックの変更、作用 [19-12](#)
- ステータスの表示 [19-25](#)
- ステータス、表示 [19-25](#)
- 設定
 - hello タイム [19-23](#)
 - 最大エージング タイム [19-24](#)
 - スイッチ プライオリティ [19-22](#)
 - スパニング ツリー モード [19-15](#)
 - セカンダリ ルート スイッチ [19-18](#)
 - 転送遅延時間 [19-24](#)
 - 転送保留カウント [19-25](#)
 - パス コスト [19-21](#)
 - ポート プライオリティ [19-19](#)
 - ルート スイッチ [19-17](#)
- 設定時の注意事項 [19-14, 21-12](#)
- タイマー、説明 [19-23](#)
- ディセーブル化 [19-16](#)
- デフォルト設定 [19-13](#)
- パス コスト [14-26](#)
- 負荷分散
 - 概要 [14-23](#)
 - パス コストの使用 [14-26](#)
 - ポート プライオリティの使用 [14-24](#)
- ポート プライオリティ [14-25](#)
- マルチキャスト アドレス、作用 [19-9](#)
- モード間の相互運用性と下位互換性 [19-11](#)
- 優位 BPDU [19-3](#)
- ルート ガード
 - イネーブル化 [21-18](#)
 - 説明 [21-10](#)
- ルート スイッチ
 - 異常動作 [19-17](#)
 - 拡張システム ID の影響 [19-5, 19-17](#)
 - 設定 [19-17](#)
 - 選択 [19-3](#)
- ルート スイッチとしての選択防止 [21-10](#)
- ルート ポート選択の高速化 [21-4](#)
- ルート ポート、定義 [19-4](#)
- ループ ガード
 - イネーブル化 [21-19](#)
 - 説明 [21-11](#)
- レイヤ 2 プロトコル トンネリング [18-8](#)
- SunNet Manager [1-6](#)
- SVI
 - IP ユニキャスト ルーティング [38-5](#)
 - VLAN 間のルーティング [14-2](#)
 - VLAN の接続 [12-11](#)
 - 定義 [12-5](#)
 - ルータ ACL [35-4](#)
- SVI Autostate Exclude
 - 設定 [12-29](#)
 - 定義 [12-6](#)
- SVI リンク ステート [12-6](#)
- Switch Database Management
 - 「SDM」を参照
- Switched Port Analyzer (スイッチド ポート アナライザ)
 - 「SPAN」を参照
- switchport backup interface [22-4, 22-5](#)
- switchport block multicast コマンド [26-8](#)
- switchport block unicast コマンド [26-8](#)
- switchport mode dot1q-tunnel コマンド [18-7](#)
- switchport protected コマンド [26-7](#)
- switchport コマンド [12-18](#)
- Switch Virtual Interface (スイッチ仮想インターフェイス)
 - 「SVI」を参照

- syslog
「システム メッセージ ロギング」を参照
-
- ## T
- TACACS+
- アカウントティング、定義 **9-12**
 - 概要 **9-10**
 - 許可、定義 **9-12**
 - クラスタ内 **6-17**
 - サーバの識別 **9-13**
 - サポート **1-12**
 - 設定
 - アカウントティング **9-17**
 - 許可 **9-16**
 - 認証鍵 **9-13**
 - ログイン認証 **9-14**
 - 設定の表示 **9-18**
 - デフォルト設定 **9-13**
 - 動作 **9-12**
 - 認証、定義 **9-11**
 - ユーザがアクセスしたサービスのトラッキング **9-17**
 - ユーザへのサービスの制限 **9-16**
- tar ファイル
- イメージ ファイル形式 **C-26**
 - 作成 **C-6**
 - 抽出 **C-8**
 - 内容の表示 **C-7**
- TCL スクリプト、組み込みイベント マネージャへの登録および定義 **34-7**
- TDR **1-17**
- Telnet
- 管理インターフェイスのアクセス **2-11**
 - 接続数 **1-7**
 - パスワードの設定 **9-6**
- Terminal Access Controller Access Control System Plus
「TACACS+」を参照
- TFTP
- イメージ ファイル
 - アップロード **C-30**
 - サーバの準備 **C-28**
 - 削除 **C-30**
 - ダウンロード **C-28**
 - コンフィギュレーション ファイル
 - アップロード **C-13**
 - サーバの準備 **C-11**
 - ダウンロード **C-12**
 - サーバによるアクセスの制限 **33-18**
 - 自動設定の場合 **3-8**
 - ベース ディレクトリのコンフィギュレーション ファイル **3-8**
- TFTP サーバ **1-6**
- Time Domain Reflector
「TDR」を参照
- time-range コマンド **35-17**
- TLV
- LLDP **28-2**
 - LLDP-MED **28-2**
 - 定義 **28-2**
- ToS **1-13**
- traceroute コマンド **49-19**
「IP traceroute」も参照
- traceroute、レイヤ 2
- 1 ポートに複数のデバイス **49-18**
 - ARP **49-18**
 - CDP **49-17**
 - IP アドレスおよびサブネット **49-18**
 - MAC アドレスおよび VLAN **49-17**
 - 使用時の注意事項 **49-17**
 - 説明 **49-17**
 - ブロードキャスト トラフィック **49-17**
 - マルチキャスト トラフィック **49-17**
 - ユニキャスト トラフィック **49-17**
- trusted (信頼性のある) ポート ステート
- IP Phone 用ポート セキュリティの確保 **36-39**
 - QoS ドメイン間 **36-41**
 - QoS ドメイン内 **36-37**

サポート [1-13](#)
 分類オプション [36-5](#)
 Type of Service (サービス タイプ)
 「ToS」を参照

U

UDLD

イネーブル化
 インターフェイスごと [29-6](#)
 グローバル [29-5](#)
 インターフェイスのリセット [29-6](#)
 エコーによる検出メカニズム [29-3](#)
 概要 [29-1](#)
 サポート [1-8](#)
 ステータス、表示 [29-7](#)
 設定時の注意事項 [29-4](#)
 ディセーブル化
 インターフェイスごと [29-6](#)
 グローバル [29-5](#)
 光ファイバ インターフェイス [29-5](#)
 デフォルト設定 [29-4](#)
 ネイバー データベース [29-2](#)
 リンク検出メカニズム [29-1](#)
 レイヤ 2 プロトコル トンネリング [18-10](#)
 UDLD によってディセーブルにされたインターフェイス
 のリセット [29-6](#)
 UDP ジッタ、設定 [43-9](#)
 UDP ジッタ動作、IP SLA [43-9](#)
 UDP、設定 [38-17](#)
 UniDirectional Link Detection (単一方向リンク検出) プ
 ロトコル
 「UDLD」を参照

UNIX Syslog サーバ

サポートされるファシリティ [32-14](#)
 デーモンの設定 [32-13](#)
 メッセージ ロギングの設定 [32-13](#)

UplinkFast

イネーブル化 [21-16](#)

サポート [1-9](#)
 説明 [21-3](#)
 ディセーブル化 [21-16](#)

User Datagram Protocol (ユーザ データグラム プロトコ ル)

「UDP」を参照

V

Virtual Private Network (バーチャル プライベート ネット ワーク)

「VPN」を参照

VLAN

ID 1006 ~ 4094 の設定 [14-11](#)
 RSPAN による送信元トラフィックの制限 [30-25](#)
 SPAN による送信元トラフィックの制限 [30-17](#)
 STP および IEEE 802.1Q トランク [19-12](#)
 SVI による接続 [12-11](#)
 VLAN データベースへの追加 [14-8](#)
 VLAN ブリッジ STP [19-12, 48-2](#)
 VTP モード [15-3](#)
 間のトラフィック [14-2](#)
 拡張範囲 [14-1, 14-11](#)
 機能 [1-9](#)
 サービスプロバイダー ネットワーク内のカスタマー
 番号 [18-3](#)
 削除 [14-9](#)
 作成 [14-9](#)
 サポートされている数 [1-9](#)
 サポート対象 [14-3](#)
 図 [14-2](#)
 スイッチ スタック内 [14-7](#)
 スタティック アクセス ポート [14-10](#)
 スパニングツリー インスタンス [14-3, 14-7, 14-12](#)
 設定 [14-1](#)
 設定時の注意事項、拡張範囲 VLAN [14-11](#)
 設定時の注意事項、標準範囲 VLAN [14-6](#)
 説明 [12-2, 14-1](#)
 ダイナミック アドレスのエージング タイム [19-10](#)
 追加 [14-8](#)

- デフォルト設定 [14-8](#)
- トークンリング [14-6](#)
- トランクでの許可 [14-21](#)
- 内部 [14-12](#)
- ネイティブ、設定 [14-23](#)
- パラメータ [14-5](#)
- 表示 [14-15](#)
- 標準範囲 [14-1, 14-5](#)
- 変更 [14-8](#)
- ポート メンバシップ モード [14-3](#)
- マルチキャスト [25-18](#)
- VLAN 1、トランク ポートでのディセーブル化 [14-21](#)
- VLAN 1 の最小化 [14-21](#)
- VLAN ACL
 - 「VLAN マップ」を参照
 - vlan.dat ファイル [14-5](#)
 - vlan dot1q tag native コマンド [18-5](#)
 - VLAN ID、検出 [7-32](#)
 - VLAN Query Protocol
 - 「VQP」を参照
 - VLAN Trunking Protocol (VLAN トランキング プロトコル)
 - 「VTP」を参照
 - VLAN 間ルーティング [1-15, 38-2](#)
 - VLAN 管理ドメイン [15-2](#)
 - vlan グローバル コンフィギュレーション コマンド [14-7](#)
 - VLAN コンフィギュレーション
 - 起動時 [14-7](#)
 - 保存 [14-7](#)
 - VLAN コンフィギュレーション モード [2-2](#)
 - VLAN データベース
 - VTP [15-1](#)
 - 格納された VLAN [14-5](#)
 - スタートアップ コンフィギュレーション ファイル [14-7](#)
 - 保存された VLAN コンフィギュレーション [14-7](#)
 - VLAN トランク [14-15](#)
 - VLAN フィルタリング、SPAN [30-7](#)
 - VLAN マップ
 - ACL および VLAN マップの例 [35-33](#)
 - 一般的な使用法 [35-36](#)
 - サーバへのアクセス拒否例 [35-37](#)
 - 削除 [35-35](#)
 - 作成 [35-33](#)
 - サポート [1-11](#)
 - 設定 [35-31](#)
 - 設定時の注意事項 [35-32](#)
 - 定義 [35-2](#)
 - 適用 [35-35](#)
 - パケットの拒否および許可 [35-33](#)
 - 表示 [35-43](#)
 - ワイヤリング クローゼットの設定例 [35-36](#)
 - VLAN マップ エントリ、順序 [35-32](#)
 - VLAN マネジメント ポリシー サーバ
 - 「VMPS」を参照
 - VLAN メンバシップ
 - 確認 [14-31](#)
 - モード [14-3](#)
 - VLAN リンク ステータス [12-6](#)
 - VLAN ロード バランシング、Flex Link [22-3](#)
 - 設定時の注意事項 [22-8](#)
 - VLAN 割り当て応答、VMPS [14-28](#)
 - VMPS
 - MAC アドレスと VLAN のマッピング [14-27](#)
 - 管理 [14-32](#)
 - サーバ アドレスの入力 [14-30](#)
 - 再確認インターバル、変更 [14-31](#)
 - 再試行回数、変更 [14-32](#)
 - 設定時の注意事項 [14-29](#)
 - 設定例 [14-33](#)
 - 説明 [14-27](#)
 - ダイナミック ポート メンバシップ
 - 再確認 [14-31](#)
 - 説明 [14-28](#)
 - トラブルシューティング [14-33](#)
 - デフォルト設定 [14-29](#)
 - メンバシップの再確認 [14-31](#)
 - モニタリング [14-32](#)

- Voice-over-IP [16-1](#)
- VPN
 - サービス プロバイダ ネットワーク [38-80](#)
 - 転送 [38-82](#)
 - ルーティングの設定 [38-89](#)
 - ルート [38-81](#)
- VQP [1-9, 14-27](#)
- VRF
 - 定義 [38-82](#)
 - テーブル [38-80](#)
- VRF テーブル
 - 「VRF」を参照 [38-80](#)
- VRF 認識サービス
 - ARP [38-86](#)
 - ftp [38-88](#)
 - HSRP [38-87](#)
 - ping [38-86](#)
 - SNMP [38-86](#)
 - syslog [38-87](#)
 - tftp [38-88](#)
 - traceroute [38-88](#)
 - 設定 [38-85](#)
- VTP
 - アドバタイズメント [14-19, 15-4](#)
 - 拡張範囲 VLAN [14-3, 15-2](#)
 - クライアント モード、設定 [15-13](#)
 - コンフィギュレーション リビジョン番号
 - 注意事項 [15-17](#)
 - リセット [15-18](#)
 - サーバ モード、設定 [15-12, 15-15](#)
 - サポート [1-10](#)
 - 使用 [15-1](#)
 - 整合性検査 [15-5](#)
 - 設定
 - 注意事項 [15-9](#)
 - 保存 [15-9](#)
 - 要件 [15-11](#)
 - 設定要件 [15-11](#)
 - 説明 [15-1](#)
 - デフォルト設定 [15-9](#)
 - 透過モード、設定 [15-12](#)
 - 統計情報 [15-19](#)
 - トークン リングのサポート [15-5](#)
 - ドメイン [15-2](#)
 - ドメインへのクライアントの追加 [15-17](#)
 - ドメイン名 [15-10](#)
 - バージョン
 - イネーブル化 [15-15](#)
 - バージョン 1 [15-5](#)
 - バージョン 2
 - 概要 [15-5](#)
 - 設定時の注意事項 [15-10](#)
 - バージョン 3
 - 概要 [15-5](#)
 - バージョン、注意事項 [15-10](#)
 - パスワード [15-10](#)
 - 標準範囲 VLAN [14-3, 15-2](#)
 - プルーニング
 - イネーブル化 [15-16](#)
 - 概要 [15-6](#)
 - サポート [1-10](#)
 - ディセーブル化 [15-17](#)
 - 例 [15-7](#)
 - プルーニング適格リスト、変更 [14-22](#)
 - モード
 - 移行 [15-3](#)
 - オフ [15-4](#)
 - クライアント [15-3](#)
 - サーバ [15-3](#)
 - 透過 [15-4](#)
 - モニタリング [15-19](#)
 - レイヤ 2 プロトコル トンネリング [18-8](#)

W

WCCP

- MD5 セキュリティ [45-3](#)
- イネーブル化 [45-7](#)

クライアントから受信したトラフィックのリダイレクト **45-7**

サポートされない WCCPv2 機能 **45-5**

サポートされない機能 **45-5**

設定時の注意事項 **45-6**

説明 **45-1**

ダイナミック サービス グループ **45-4**

デフォルト設定 **45-6**

転送方式 **45-3**

認証 **45-3**

ネゴシエーション **45-3**

パケットリターン方法 **45-3**

パケットリダイレクション **45-4**

パスワードの設定 **45-7**

表示 **45-10**

メッセージ交換 **45-2**

モニタおよびメンテナンス **45-10**

レイヤ 2 ヘッダーの書き換え **45-3**

Web Cache Communication Protocol

「WCCP」を参照

Web 認証 **10-16**

設定 **11-17**

説明 **1-10**

Web ベース認証

カスタマイズ可能な Web ページ **11-6**

説明 **11-1**

Web ベース認証、その他の機能の相互作用 **11-7**

Weighted Tail Drop

「WTD」を参照

WTD

サポート **1-14**

しきい値の設定

出力キューセット **36-73**

入力キュー **36-68**

説明 **36-13**

X

XMODEM プロトコル **49-2**

あ

アカウントティング

802.1x **10-49**

IEEE 802.1x **10-15**

RADIUS **9-35**

TACACS+ **9-12, 9-17**

アクセス

クラスタ、スイッチ **6-14**

コマンド スイッチ **6-12**

スイッチ クラスタ **6-14**

メンバー スイッチ **6-14**

アクセス拒否応答、VMPS **14-28**

アクセス グループ

インターフェイスへの IPv4 ACL の適用 **35-21**

レイヤ 2 **35-21**

レイヤ 3 **35-21**

アクセス コントロール エントリ (ACE) **41-3**

アクセス、スタック メンバー **5-23**

アクセス テンプレート **8-1**

アクセス不能認証バイパス **10-23**

マルチ認証ポートのサポート **10-23**

アクセス ポート

スイッチ クラスタ **6-10**

定義 **12-3**

レイヤ 2 プロトコル トンネリング **18-11**

アクセス リスト

「ACL」を参照

アクティブ トラフィック モニタリング、IP SLA **43-1**

アクティブ リンク **22-2, 22-4, 22-5, 22-6**

アクティブ ルータ **42-2**

アグリゲータ テンプレート **5-9, 8-1**

アップグレード、ソフトウェア イメージ

「ダウンロード」を参照

アップロード

イメージ ファイル

FTP の使用 **C-35**

RCP の使用 **C-40**

TFTP の使用 **C-30**

- 準備 [C-28, C-31, C-36](#)
- 理由 [C-25](#)
- コンフィギュレーション ファイル
 - FTP の使用 [C-16](#)
 - RCP の使用 [C-19](#)
 - TFTP の使用 [C-13](#)
 - 準備 [C-11, C-14, C-17](#)
 - 理由 [C-9](#)
- 宛先 IP アドレスベース転送、EtherChannel [37-9](#)
- 宛先 MAC アドレス転送、EtherChannel [37-9](#)
- 宛先アドレス
 - IPv4 ACL [35-12](#)
 - IPv6 ACL [41-6](#)
- アドバタイズメント
 - CDP [27-1](#)
 - LLDP [28-2](#)
 - RIP [38-22](#)
 - VTP [14-19, 15-3, 15-4](#)
- アトリビュート、RADIUS
 - ベンダー固有 [9-36](#)
 - ベンダー独自 [9-38](#)
- アトリビュート値ペア [10-13, 10-15, 10-19, 10-20](#)
- アドレス
 - IPv6 [39-2](#)
 - MAC アドレス テーブルの表示 [7-32](#)
 - MAC、検出 [7-32](#)
 - スタティック
 - 追加および削除 [7-28](#)
 - 定義 [7-20](#)
 - ダイナミック
 - エージング タイムの短縮 [19-10](#)
 - エージング タイムの変更 [7-22](#)
 - 削除 [7-23](#)
 - 定義 [7-20](#)
 - デフォルトのエージング タイム [19-10](#)
 - ラーニング [7-21](#)
 - マルチキャスト
 - STP アドレス管理 [19-9](#)
 - グループ アドレス範囲 [46-3](#)
 - アドレス エイリアス [25-2](#)
 - アドレス解決 [7-32, 38-10](#)
 - アプリケーション エンジン、トラフィックのリダイレクト先 [45-1](#)
 - アベイラビリティ、機能 [1-8](#)
 - アラーム、RMON [31-4](#)
 - 暗号化、CipherSuite [9-53](#)
 - 暗号化ソフトウェア イメージ
 - Kerberos [9-40](#)
 - SSH [9-46](#)
 - SSL [9-51](#)
 - スイッチ スタックの考慮事項 [5-2, 5-16, 9-47](#)
 - 暗号化、パスワード [9-4](#)
 - 安全なリモート接続 [9-46](#)

い

 - イーサネット VLAN
 - 追加 [14-8](#)
 - デフォルトおよび範囲 [14-8](#)
 - 変更 [14-8](#)
 - 一時的な自己署名証明書 [9-52](#)
 - 一般クエリー [22-5](#)
 - イネーブル シークレット パスワード [9-4](#)
 - イネーブル パスワード [9-4](#)
 - イベント、RMON [31-4](#)
 - イベント ディテクタ、組み込みイベント マネージャ [34-3](#)
 - インターフェイス
 - Auto-MDIX、設定 [12-23](#)
 - カウンタ、クリア [12-35](#)
 - 管理 [1-6](#)
 - 記述名、追加 [12-27](#)
 - 再起動 [12-36](#)
 - サポート対象 [12-12](#)
 - シャットダウン [12-36](#)
 - 情報の表示 [12-34](#)
 - ステータス [12-34](#)
 - 設定

手順	12-13
設定時の注意事項	
10 ギガビットイーサネット	12-19
デュプレックスと速度	12-20
説明	12-27
速度およびデュプレックス、設定	12-21
タイプ	12-1
デフォルト設定	12-18
範囲	12-14
番号	12-12
物理、特定	12-12
フロー制御	12-22
命名	12-27
モニタリング	12-34
レンジマクロ	12-15
インターフェイス コンフィギュレーションモード	2-3
インターフェイス タイプ	12-12

う

ウィザード	1-3
ウェイトしきい値、トラッキング リスト	44-5

え

永続的な自己署名証明書	9-52
エージング タイム	
MAC アドレス テーブル	7-22
最大	
MSTP	20-25, 20-26
STP	19-24, 19-25
短縮	
MSTP	20-25
STP	19-10, 19-24
エージング タイム、短縮	19-10
エラー メッセージ、コマンド入力時	2-5
エリア ルーティング	
IS-IS	38-70
ISO IGRP	38-70

お

応答側、IP SLA	
イネーブル化	43-8
説明	43-4
応答時間、IP SLA での測定	43-4
オブジェクト トラッキング	
HSRP	44-7
IP SLA	44-9
IP SLA、設定	44-9
モニタリング	44-13
オブジェクト トラッキングのプライマリ インターフェイス、DHCP、設定	44-11
オプション、管理	1-6
オフ モード、VTP	15-4
オフライン設定、スイッチ スタック	5-7
音声 VLAN	
Cisco 7960 IP Phone、ポート接続	16-1
IP Phone の音声トラフィック、説明	16-2
IP Phone のデータ トラフィック、説明	16-2
IP Phone への接続	16-5
音声トラフィック用のポート設定	
802.1p プライオリティ タグ付きフレーム	16-6
802.1Q フレーム	16-5
設定時の注意事項	16-3
説明	16-1
データ トラフィック用の IP Phone の設定	
着信フレームの CoS の変更	16-7
着信フレームの CoS プライオリティを信頼	16-7
デフォルト設定	16-3
表示	16-8
音声認識 802.1X セキュリティ	
ポートベースの認証	
設定	10-38
説明	10-30, 10-38
オンライン診断	
概要	50-1
テストの実行	50-3

- か**
- 階層型のポリシー マップ **36-8**
 - 設定 **36-53**
 - 設定時の注意事項 **36-34**
 - 説明 **36-11**
 - ガイド モード **1-2**
 - 外部 VLAN
 - 「音声 VLAN」を参照
 - 回復手順 **49-1**
 - 外部ネイバー、BGP **38-52**
 - カウンタ、インターフェイスのクリア **12-35**
 - 拡張 crashinfo ファイル **49-25**
 - 拡張オブジェクト トラッキング
 - DHCP プライマリ インターフェイス **44-11**
 - HSRP **44-7**
 - IP SLA **44-9**
 - IP SLA によるネットワーク モニタリング **44-11**
 - IP ルーティング ステート **44-2**
 - コマンド **44-1**
 - スタティック ルートのプライマリ インターフェイス **44-11**
 - 定義 **44-1**
 - トラッキング リスト **44-4**
 - バックアップ スタティック ルーティング **44-12**
 - ライン プロトコル ステート **44-2**
 - ルーティング ポリシー、設定 **44-12**
 - 拡張オブジェクト トラッキングのスタティック ルーティング **44-10**
 - 拡張システム ID
 - MSTP **20-19**
 - STP **19-5, 19-17**
 - 拡張範囲 VLAN
 - 作成 **14-12**
 - 設定 **14-11**
 - 設定時の注意事項 **14-11**
 - 定義 **14-1**
 - 内部 VLAN ID による作成 **14-14**
 - カスタマイズ可能な Web ページ、Web ベース認証 **11-6**
 - 仮想 IP アドレス
 - クラスタ スタンバイ グループ **6-12**
 - コマンド スイッチ **6-12**
 - 仮想スイッチおよび PAgP **37-6**
 - 仮想ルータ **42-2, 42-3**
 - 環境変数、機能 **3-22**
 - 環境変数、組み込みイベント マネージャ **34-5**
 - 間接リンク障害の検出、STP **21-8**
 - 管理 VLAN
 - 異なる管理 VLAN からの検出 **6-8**
 - スイッチ クラスタの考慮事項 **6-8**
 - 管理アクセス
 - 帯域外コンソール ポート接続 **1-7**
 - 帯域内
 - CLI セッション **1-7**
 - SNMP **1-7**
 - デバイス マネージャ **1-7**
 - ブラウザ セッション **1-7**
 - 管理アドレス TLV **28-2**
 - 管理オプション
 - CLI **2-1**
 - CNS **4-1**
 - Network Assistant **1-2**
 - 概要 **1-6**
 - クラスタ化 **1-3**
 - スタック、スイッチ **1-3**
 - 管理距離
 - OSPF **38-35**
 - 定義 **38-109**
 - ルーティング プロトコルのデフォルト **38-98**
 - 管理の簡易性に関する機能 **1-6**
-
- き**
- ギガビット モジュール
 - 「SFP」を参照 **1-22**
 - 起動
 - 起動プロセス **3-2**
 - 手動 **3-19**

- 特定のイメージ [3-20](#)
 - ブート ロード、機能 [3-2](#)
 - 機能、互換性のない [26-12](#)
 - 逆アドレス解決 [38-10](#)
 - 許可
 - RADIUS [9-34](#)
 - TACACS+ [9-12, 9-16](#)
 - 許可 VLAN リスト [14-21](#)
 - 許可できるデバイスの最大数、ポートベース認証 [10-37](#)
 - 許可ポート、IEEE 802.1X [10-10](#)
 - 緊急キュー、QoS [36-79](#)
 - 近接ディスカバリ、IPv6 [39-4](#)
 - 近接ディスカバリおよび回復、EIGRP [38-39](#)
-
- ◀
- クエリー、IGMP [25-4](#)
 - クエリー送信要求、IGMP [25-13](#)
 - 組み込みイベント マネージャ
 - 3.2 [34-6](#)
 - 組み込みイベントマネージャ
 - TCL スクリプトの登録および定義 [34-7](#)
 - アプレットの登録および定義 [34-6](#)
 - イベント ディテクタ [34-3](#)
 - 概要 [34-2](#)
 - 環境変数 [34-5](#)
 - 情報の表示 [34-8](#)
 - 設定 [34-1, 34-6](#)
 - 操作 [34-4](#)
 - ポリシー [34-5](#)
 - クライアントプロセス、トラッキング [44-1](#)
 - クライアント モード、VTP [15-3](#)
 - クラスタおよび HSRP グループのバインド [42-13](#)
 - クラスタ、スイッチ
 - LRE プロファイルの考慮事項 [6-17](#)
 - アクセス [6-14](#)
 - 管理
 - CLI の使用 [6-17](#)
 - SNMP の使用 [6-18](#)
 - 互換性 [6-5](#)
 - 自動検出 [6-5](#)
 - 自動復旧 [6-11](#)
 - 説明 [6-1](#)
 - プランニング [6-5](#)
 - プランニングの考慮事項
 - CLI [6-17](#)
 - IP アドレス [6-14](#)
 - LRE プロファイル [6-17](#)
 - RADIUS [6-17](#)
 - SNMP [6-15, 6-18](#)
 - TACACS+ [6-17](#)
 - 自動検出 [6-5](#)
 - 自動復旧 [6-11](#)
 - スイッチ スタック [6-15](#)
 - パスワード [6-15](#)
 - ホスト名 [6-14](#)
 - 利点 [1-2](#)
 - 「候補スイッチ」、「コマンドスイッチ」、「クラスタ スタンバイ グループ」、「メンバー スイッチ」、および「スタンバイ コマンド スイッチ」も参照
 - クラスタ スタンバイ グループ
 - HSRP グループ [42-13](#)
 - 仮想 IP アドレス [6-12](#)
 - 考慮事項 [6-12](#)
 - 自動復旧 [6-13](#)
 - 定義 [6-2](#)
 - 要件 [6-3](#)
 - 「HSRP」も参照
 - クラスマップ、QoS
 - 設定 [36-47](#)
 - 説明 [36-7](#)
 - 表示 [36-80](#)
 - クラスレス ルーティング [38-8](#)
 - クリア、インターフェイス [12-35](#)
 - クリティカル VLAN [10-23](#)
 - クリティカル認証、IEEE 802.1X [10-53](#)
 - グローバル Leave、IGMP [25-13](#)

- グローバル コンフィギュレーション モード **2-2**
 - クロススタック EtherChannel
 - サポート **1-8**
 - 図 **37-4**
 - 設定
 - レイヤ 2 インターフェイス **37-14**
 - レイヤ 3 物理インターフェイス **37-17**
 - 設定時の注意事項 **37-13**
 - 説明 **37-3**
 - クロススタック UplinkFast、STP
 - Fast Uplink Transition Protocol **21-6**
 - イネーブル化 **21-17**
 - 高速コンバージェンスのイベント **21-7**
 - 説明 **21-5**
 - ディセーブル化 **21-17**
 - 標準コンバージェンスのイベント **21-7**
 - クロック
 - 「システム クロック」を参照
-
- ## け
- ケーブル、単一方向リンクのモニタ **29-1**
 - ゲスト VLAN と 802.1x **10-21**
 - 権限レベル
 - 回線のデフォルトの変更 **9-9**
 - 概要 **9-2, 9-8**
 - コマンド スイッチ **6-18**
 - コマンドの設定 **9-8**
 - 終了 **9-10**
 - メンバー スイッチとの対応 **6-18**
 - ログイン **9-10**
 - 検出、クラスタ
 - 「自動検出」を参照
-
- ## こ
- 構成例、ネットワーク **1-20**
 - 高速コンバージェンス **20-11, 22-3**
 - 候補スイッチ
 - 自動検出 **6-5**
 - 定義 **6-4**
 - 要件 **6-4**
 - 「コマンド スイッチ」、「クラスタ スタンバイ グループ」、および「メンバー スイッチ」も参照
 - 互換性、機能 **26-12**
 - 互換性、ソフトウェア
 - 「スタック、スイッチ」を参照
 - コマンド
 - no 形式および default 形式 **2-4**
 - 省略 **2-4**
 - コマンド、権限レベルの設定 **9-8**
 - コマンド スイッチ
 - アクセス **6-12**
 - アクティブ (AC) **6-11**
 - 交換
 - クラスタ メンバー **49-10**
 - 別のスイッチ **49-11**
 - 冗長 **6-11**
 - スタンバイ (SC) **6-11**
 - 設定の矛盾 **49-13**
 - 定義 **6-2**
 - パスワードおよび権限レベル **6-18**
 - パッシブ (PC) **6-11**
 - 復旧
 - コマンド スイッチの障害 **6-11, 49-9**
 - メンバー スイッチとの接続 **49-13**
 - プライオリティ **6-11**
 - 要件 **6-3**
 - 「候補スイッチ」、「クラスタ スタンバイ グループ」、「メンバー スイッチ」、および「スタンバイ コマンド スイッチ」も参照
 - コマンド モード **2-1**
 - コマンドライン インターフェイス
 - 「CLI」を参照
 - コミュニティ VLAN **17-2, 17-3**
 - コミュニティ ストリング
 - SNMP **6-15**
 - 概要 **33-4**
 - クラスタ スイッチ用 **33-4**

- クラスタ内 **6-15**
 - 設定 **6-15, 33-8**
 - コミュニティ ポート **17-2**
 - コミュニティ リスト、BGP **38-62**
 - 混合ポート
 - 設定 **17-13**
 - 定義 **17-2**
 - コンソール ポート、接続 **2-11**
 - コンテンツ ルーティング テクノロジー
「WCCP」を参照
 - コントロール プロトコル、IP SLA **43-4**
 - コンフィギュレーション交換 **C-21**
 - コンフィギュレーション ファイル
 - DHCP による入手 **3-10**
 - TFTP サーバ アクセスの制限 **33-18**
 - アーカイブ **C-21**
 - アップロード
 - FTP の使用 **C-16**
 - RCP の使用 **C-19**
 - TFTP の使用 **C-13**
 - 準備 **C-11, C-14, C-17**
 - 理由 **C-9**
 - 格納されたコンフィギュレーションの削除 **C-20**
 - 交換およびロール バックの注意事項 **C-22**
 - コピー時の無効な組み合わせ **C-5**
 - 作成および使用上の注意事項 **C-10**
 - システム コンタクトおよびロケーションの情報 **33-17**
 - 実行コンフィギュレーションの交換 **C-21**
 - 実行コンフィギュレーションのロール バック **C-21, C-22**
 - スタートアップ コンフィギュレーションの消去 **C-20**
 - 説明 **C-9**
 - タイプおよび場所 **C-10**
 - ダウンロード
 - FTP の使用 **C-14**
 - RCP の使用 **C-18**
 - TFTP の使用 **C-12**
 - 自動 **3-18**
 - 準備 **C-11, C-14, C-17**
 - 理由 **C-9**
 - テキスト エディタによる作成 **C-11**
 - デフォルト名 **3-18**
 - パスワード回復をディセーブルにする場合の考慮事項 **9-5**
 - ファイル名の指定 **3-19**
 - コンフィギュレーション ロールバック **C-21**
 - コンフィギュレーション ログギング **2-5**
 - コンポーネント管理 TLV **28-3, 28-7**
-
- ## さ
- サーバ モード、VTP **15-3**
 - サービス プロバイダー ネットワーク
 - EtherChannel のレイヤ 2 プロトコル トンネリング **18-9**
 - IEEE 802.1Q トンネリング **18-2**
 - カスタマーの VLAN **18-2**
 - またがるレイヤ 2 プロトコル **18-8**
 - サービス プロバイダー ネットワーク、MSTP および RSTP **20-1**
 - 再確認インターバル、VMPS、変更 **14-31**
 - 再確認、ダイナミック VLAN メンバシップ **14-31**
 - 再試行回数、VMPS、変更 **14-32**
 - 最大エージング タイム
 - MSTP **20-25**
 - STP **19-24**
 - 最大ホップ カウント、MSTP **20-26**
 - 最適化、システム リソース **8-1**
 - 削除、VLAN **14-9**
 - サブドメイン、プライベート VLAN **17-1**
 - サブネット ゼロ **38-8**
 - サブネット マスク **38-7**
 - サポートされるポートベースの認証方式 **10-7**
-
- ## し
- シーケンスの再編集、ACL エントリ **35-15**

- シェル機能
 - 「Auto Smartport マクロ」も参照
- シェル トリガー
 - 「Auto Smartport マクロ」も参照
- 時間範囲、ACL **35-17**
- しきい値、トラフィック レベル **26-2**
- しきい値モニタリング、IP SLA **43-6**
- シスコのインテリジェント電力管理 **12-8**
- システム MTU
 - IS-IS LSP **38-74**
- システム MTU および IEEE 802.1Q トンネリング **18-6**
- システム記述 TLV **28-2**
- システム機能 TLV **28-2**
- システム クロック
 - 概要 **7-2**
 - 設定
 - 手動 **7-12**
 - タイム ゾーン **7-13**
 - 夏時間 **7-14**
 - 日時の表示 **7-12**
 - 「NTP」も参照
- システム プロンプト、デフォルト設定 **7-15, 7-16**
- システム名
 - 手動設定 **7-16**
 - デフォルト設定 **7-16**
- システム名 TLV **28-2**
- システム名
 - 「DNS」も参照
- システム メッセージ ログギング
 - level キーワード、説明 **32-10**
 - syslog ファシリティ **1-16**
- UNIX Syslog サーバ
 - サポートされるファシリティ **32-14**
 - デーモンの設定 **32-13**
 - ログギング ファシリティの設定 **32-13**
- イネーブル化 **32-5**
- エラー メッセージの重大度の定義 **32-9**
- 概要 **32-1**
- シーケンス番号、イネーブル化およびディセーブル化 **32-8**
- スタックの変更、作用 **32-2**
- 設定の表示 **32-14**
- タイム スタンプ、イネーブル化およびディセーブル化 **32-8**
- ディセーブル化 **32-4**
- デフォルト設定 **32-4**
- 表示宛先デバイスの設定 **32-5**
- ファシリティ キーワード、説明 **32-14**
- メッセージの制限 **32-10**
- メッセージのフォーマット **32-2**
- ログ メッセージの同期化 **32-6**
- システム リソース、最適化 **8-1**
- システム ルーティング
 - IS-IS **38-70**
 - ISO IGRP **38-70**
- 実行コンフィギュレーション
 - 交換 **C-21**
 - ロール バック **C-21, C-22**
- 実行コンフィギュレーション、保存 **3-17**
- 自動 QoS
 - 「QoS」を参照
- 自動 RP、説明 **46-7**
- 自動イネーブル **10-30**
- 自動検出
 - 考慮事項
 - CDP 非対応デバイス **6-6**
 - 新しいスイッチ **6-10**
 - 管理 VLAN **6-8**
 - クラスタ非対応デバイス **6-6**
 - 異なる VLAN **6-7**
 - 接続 **6-5**
 - 非候補デバイスより先 **6-8**
 - ルーテッド ポート **6-9**
 - スイッチ クラスタ **6-5**
 - 「CDP」も参照
- 自動検知、ポート速度 **1-4**
- 自動設定 **3-4**

- 自動ネゴシエーション
 - インターフェイス設定時の注意事項 **12-20**
 - デュプレックス モード **1-4**
 - 不一致 **49-13**
 - 自動復旧、クラスタ **6-11**
 - 「HSRP」も参照
 - シャットダウンしきい値、レイヤ 2 プロトコル パケッ
ト **18-11**
 - 重大度、システム メッセージの定義 **32-9**
 - 柔軟な認証の順序
 - 概要 **10-29**
 - 設定 **10-64**
 - 集約アドレス、BGP **38-65**
 - 集約可能なグローバルユニキャストアドレス **39-3**
 - 集約ポート
 - 「EtherChannel」を参照
 - 集約ポリサー **36-60**
 - 集約ポリシング **1-14**
 - 準備チェック
 - ポートベースの認証
 - 設定 **10-37**
 - 説明 **10-16, 10-37**
 - 照合
 - IPv6 ACL **41-3**
 - 照合、IPv4 ACL **35-8**
 - 冗長
 - EtherChannel **37-3**
 - HSRP **42-2**
 - STP
 - パス コスト **14-26**
 - バックボーン **19-9**
 - ポート プライオリティ **14-24**
 - マルチドロップ バックボーン **21-5**
 - 冗長電源システム
 - 「Cisco Redundant Power System 2300」を参照
 - 冗長リンクおよび UplinkFast **21-16**
 - 省略、コマンド **2-4**
 - 初期設定
 - Express Setup **1-2**
 - デフォルト **1-17**
 - 信頼境界機能、QoS **36-39**
 - 信頼性のあるタイム ソース、説明 **7-2**
 - 信頼できるトランスポート プロトコル、EIGRP **38-39**
 - 信頼点、CA **9-51**
-
- す**
- スイッチ コンソール ポート **1-7**
 - スイッチ スタック
 - Catalyst 3750G ワイヤレス LAN コントローラ スイッ
チ **A-2**
 - スイッチ スタックの自動的なアップグレード (自動アッ
プグレード) **5-11**
 - スイッチ スタックの自動的なアドバース (自動アドバ
ース) **5-12**
 - スイッチ スタックの自動的なコピー (自動コ
ピー) **5-11**
 - スイッチ スタックの自動的な抽出 (自動抽出) **5-11**
 - スイッチ ソフトウェア機能 **1-1**
 - スイッチド パケット、ACL **35-39**
 - スイッチド ポート **12-3**
 - スイッチのクラスタ化テクノロジー **6-1**
 - 「クラスタ」、「スイッチ」も参照
 - スイッチ プライオリティ
 - MSTP **20-23**
 - STP **19-22**
 - スーパーネット **38-8**
 - スケジューリング、IP SLA 動作 **43-5**
 - スケジュール、リロード **3-22**
 - スタートアップ コンフィギュレーション
 - 起動
 - 手動 **3-19**
 - 特定のイメージ **3-20**
 - 起動のデフォルト設定 **3-18**
 - クリア **C-20**
 - コンフィギュレーション ファイル
 - 自動ダウンロード **3-18**
 - ファイル名の指定 **3-19**
 - スタック、スイッチ

- CDP の考慮事項 [27-2](#)
- HSRP の考慮事項 [42-5](#)
- IPv6 [39-10](#)
- MAC アドレス [5-5, 5-19](#)
- MAC アドレスの考慮事項 [7-22](#)
- STP
 - サポートされるインスタンス [19-11](#)
 - スタック ルート スイッチの選択 [19-3](#)
 - ブリッジ ID [19-3](#)
 - ルート ポートの選択 [19-4](#)
- アップグレード [C-41](#)
- オフライン設定
 - 新しいメンバーの割り当て [5-22](#)
 - 説明 [5-7](#)
 - 割り当てられたスイッチ、定義 [5-7](#)
 - 割り当てられたスイッチの交換の影響 [5-9](#)
 - 割り当てられたスイッチの削除の影響 [5-9](#)
 - 割り当てられたスイッチの追加の影響 [5-7](#)
 - 割り当てられた設定、定義 [5-7](#)
- 管理 [5-1](#)
- 管理接続 [5-16](#)
- クラスタ内 [6-15](#)
- 互換性、ソフトウェア [5-9](#)
- 互換性のないソフトウェアおよびイメージのアップグレード [5-14, C-41](#)
- 固定 MAC アドレス タイマーのイネーブル化 [5-19](#)
- コンフィギュレーション ファイル [5-14](#)
- サポートされる MSTP インスタンス [19-11](#)
- システム全体の設定の考慮事項 [5-15](#)
- システム プロンプトの考慮事項 [7-15](#)
- システム メッセージ
 - 出力内のホスト名 [32-1](#)
 - リモート モニタ [32-2](#)
- 自動アップグレード [5-11](#)
- 自動アドバイス [5-12](#)
- 自動コピー [5-11](#)
- 自動抽出 [5-11](#)
- 障害の発生したメンバーの交換 [5-15](#)
- 情報の表示 [5-23](#)
- 情報の割り当て
 - 新しいメンバーの割り当て [5-22](#)
 - プライオリティ値 [5-21](#)
 - メンバー番号 [5-21](#)
- スタック プロトコル バージョン [5-10](#)
- 設定のシナリオ [5-17](#)
- 説明 [5-1](#)
- ソフトウェア イメージ バージョン [5-9](#)
- ソフトウェアの互換性 [5-9](#)
- デフォルト設定 [5-19](#)
- 統合 [5-3](#)
- 特定のメンバーへの CLI アクセス [5-23](#)
- バージョン不一致 (VM) モード
 - 自動アップグレードによる自動的なアップグレード [5-11](#)
 - 自動アドバイスによる手動アップグレード [5-12](#)
 - 自動抽出によるアップグレード [5-11](#)
 - 例 [5-12](#)
- バージョン不一致モード
 - 説明 [5-10](#)
- パーティション化 [5-3, 49-9](#)
- ハードウェア互換性と SDM 不一致モード [5-9](#)
- ブリッジ ID [5-5](#)
- マルチキャスト ルーティング、スタック マスターおよびメンバーの役割 [46-11](#)
- メンバーから別のメンバーへのイメージ ファイルのコピー [C-41](#)
- メンバシップ [5-3](#)
- 利点 [1-2](#)
- 割り当てられたスイッチ
 - 交換 [5-9](#)
 - 削除 [5-9](#)
 - 追加 [5-7](#)
- 「スタック マスター」および「スタック メンバー」も参照
- スタックの変更
 - 影響
 - IPv6 ルーティング [39-10](#)
- スタックの変更、作用

- 802.1x ポートベース認証 [10-11](#)
- ACL の設定 [35-7](#)
- CDP [27-2](#)
- EtherChannel [37-10](#)
- HSRP [42-5](#)
- IGMP スヌーピング [25-7](#)
- IPv6 ACL [41-4](#)
- IP ルーティング [38-4](#)
- MAC アドレス テーブル [7-22](#)
- MSTP [20-9](#)
- MVR [25-18](#)
- SDM テンプレートの選択 [8-4](#)
- SNMP [33-1](#)
- SPAN および RSPAN [30-10](#)
- STP [19-12](#)
- VLAN [14-7](#)
- VTP [15-8](#)
- クロススタック EtherChannel [37-13](#)
- システム メッセージのログ [32-2](#)
- スイッチ クラスタ [6-15](#)
- パケットのフラッディング [48-3](#)
- ポート セキュリティ [26-20](#)
- マルチキャスト ルーティング [46-11](#)
- スタック プロトコル バージョン [5-10](#)
- スタック マスター
 - IPv6 [39-10](#)
 - 「スタック、スイッチ」も参照
 - 選択 [5-4](#)
 - 定義 [5-1](#)
 - ブリッジ ID (MAC アドレス) [5-5](#)
- スタック メンバー
 - IPv6 [39-10](#)
 - 新しいメンバーの割り当て [5-22](#)
 - 交換 [5-15](#)
 - 情報の表示 [5-23](#)
 - 「スタック、スイッチ」も参照
 - 設定
 - プライオリティ値 [5-21](#)
 - メンバー番号 [5-21](#)
 - 定義 [5-1](#)
 - 特定のメンバーへの CLI アクセス [5-23](#)
 - 番号 [5-6](#)
 - プライオリティ値 [5-6](#)
 - スタック メンバー番号 [12-12](#)
 - スタティック IP ルーティング [1-15](#)
 - スタティック MAC アドレッシング [1-10](#)
 - スタティック SSM マッピング [46-20, 46-22](#)
 - スタティック VLAN メンバシップ [14-2](#)
 - スタティック アクセス ポート
 - VLAN への割り当て [14-10](#)
 - 定義 [12-3, 14-3](#)
 - スタティック アドレス
 - 「アドレス」を参照
 - スタティックトラフィック フォワーディング [46-23](#)
 - スタティック ホストの IP ポート セキュリティ
 - PVLAN ホスト ポート [23-25](#)
 - レイヤ 2 アクセス ポート [23-22](#)
 - スタティック ルーティング [38-3](#)
 - スタティック ルーティング サポート、拡張オブジェクト
トラッキング [44-10](#)
 - スタティック ルーティングのプライマリ インターフェイス、
設定 [44-11](#)
 - スタティック ルート
 - IPv6 の設定 [39-21](#)
 - 概要 [39-7](#)
 - 設定 [38-97](#)
 - スタティック ルートのプライマリ インターフェイス、
設定 [44-11](#)
 - スタブ エリア、OSPF [38-33](#)
 - スタブ ルーティング、EIGRP [38-45](#)
 - スタンバイ グループ、クラスタ
 - 「クラスタ スタンバイ グループ」および「HSRP」を
参照
 - スタンバイ コマンド スイッチ
 - 仮想 IP アドレス [6-12](#)
 - 考慮事項 [6-12](#)
 - 設定
 - 定義 [6-2](#)
 - プライオリティ [6-11](#)

要件 **6-3**
「クラスタ スタンバイ グループ」および「HSRP」も参照

スタンバイ タイマー、HSRP **42-11**

スタンバイ リンク **22-2**

スタンバイ ルータ **42-2**

スティッキー ラーニング **26-10**

ストーム制御

- サポート **1-4**
- しきい値 **26-2**
- 設定 **26-3**
- 説明 **26-1**
- ディセーブル化 **26-5**
- 表示 **26-21**

ストラタム、NTP **7-2**

スヌーピング、IGMP **25-2**

スパンニング ツリーおよびネイティブ VLAN **14-18**

スプリット ホライズン、RIP **38-25**

せ

制限、アクセス

- NTP サービス **7-8**
- RADIUS **9-18**
- TACACS+ **9-10**
- 概要 **9-1**
- パスワードおよび権限レベル **9-2**

制限付き VLAN

- IEEE 802.1x での使用 **10-22**
- 設定 **10-51**
- 説明 **10-22**

成功応答、VMPS **14-28**

整合性検査、VTP バージョン 2 **15-5**

生成、IGMP レポート **22-4**

セカンダリ VLAN **17-2**

セキュア HTTP クライアント

- 設定 **9-56**
- 表示 **9-57**

セキュア HTTP サーバ **9-51**

設定 **9-55**

表示 **9-57**

セキュア MAC アドレス

- 最大数 **26-10**
- 削除 **26-17**
- スイッチ スタック **26-20**
- タイプ **26-9**

セキュア ポート

- スイッチ スタック **26-20**
- 設定 **26-9**

セキュリティ機能 **1-10**

セキュリティ、ポート **26-9**

設計例、ネットワーク **1-20**

接続、安全なリモート **9-46**

接続された場所のサービス

- 概要 **28-3**
- 設定 **28-9**
- 表示 **28-11**
- ロケーション TLV **28-3**

接続の問題 **49-15, 49-17, 49-18**

設定時の注意事項、マルチ VRF CE **38-83**

設定、初期

- Express Setup **1-2**
- デフォルト **1-17**

設定、小さいフレームの着信レート **26-5**

設定の矛盾、メンバー スイッチとの接続の回復 **49-13**

設定変更、ロギング **32-11**

設定、保存 **3-17**

設定ロガー **32-11**

セットアップ プログラム

- 故障したコマンド スイッチの交換 **49-10, 49-11**

選択

「スタック マスター」を参照

そ

送信、IGMP レポート **22-4**

送信元 IP アドレスベース転送、EtherChannel **37-9**

送信元 MAC アドレス転送、EtherChannel **37-9**

- 送信元 / 宛先 IP アドレスベース転送、EtherChannel **37-9**
 - 送信元 / 宛先 MAC アドレス転送、EtherChannel **37-9**
 - 送信元アドレス
 - IPv4 ACL **35-12**
 - IPv6 ACL **41-6**
 - 即時脱退、IGMP **25-6**
 - イネーブル化 **40-9**
 - ソフトウェア イメージ
 - tar ファイル形式、説明 **C-26**
 - 回復手順 **49-2**
 - フラッシュ内の場所 **C-26**
 - リロードのスケジュール **3-23**
 - 「ダウンロード」および「アップロード」も参照
 - ソフトウェア障害、XMODEM による回復手順 **49-2**
 - ソフトウェアの互換性
 - 「スタック、スイッチ」を参照
-
- ## た
- ダイナミック ARP インスペクション
 - ARP ACL と DHCP スヌーピング エントリの相対的なプライオリティ **24-5**
 - ARP キャッシュ ポイズニング **24-1**
 - ARP スプーフィング攻撃 **24-1**
 - ARP パケットのレート制限
 - errdisable ステート **24-5**
 - 設定 **24-11**
 - 説明 **24-4**
 - ARP 要求、説明 **24-1**
 - DHCP スヌーピング バインディング データベース **24-2**
 - DoS 攻撃、回避 **24-11**
 - man-in-the middle 攻撃、説明 **24-2**
 - インターフェイス信頼状態 **24-3**
 - 機能 **24-2**
 - クリア
 - 統計情報 **24-15**
 - ログ バッファ **24-15**
 - 設定
 - DHCP 環境 **24-7**
 - 着信 ARP パケットのレート制限 **24-4, 24-11**
 - 非 DHCP 環境の ACL **24-9**
 - ログ バッファ **24-13**
 - 設定時の注意事項 **24-6**
 - 説明 **24-1**
 - 妥当性チェック、実行 **24-12**
 - デフォルト設定 **24-6**
 - 統計情報
 - クリア **24-15**
 - 表示 **24-15**
 - ネットワーク セキュリティ問題とインターフェイス信頼状態 **24-3**
 - 廃棄されたパケットのロギング、説明 **24-5**
 - 表示
 - ARP ACL **24-15**
 - 信頼状態とレート制限 **24-15**
 - 設定および動作状態 **24-15**
 - 統計情報 **24-15**
 - ログ バッファ **24-15**
 - レート制限を超過した場合の errdisable ステート **24-5**
 - ログ バッファ
 - クリア **24-15**
 - 設定 **24-13**
 - 表示 **24-15**
 - ダイナミック アクセス ポート
 - 設定 **14-30**
 - 定義 **12-3**
 - 特性 **14-4**
 - ダイナミック アドレス
 - 「アドレス」を参照
 - ダイナミック ポート VLAN メンバシップ
 - 再確認 **14-31**
 - 接続のタイプ **14-30**
 - 説明 **14-28**
 - トラブルシューティング **14-33**
 - ダイナミック ルーティング **38-3**
 - ISO CLNS **38-69**

タイム

「NTP およびシステム クロック」を参照

タイムゾーン **7-13**

ダウンロード

イメージ ファイル

CMS の使用 **1-3**

FTP の使用 **C-32**

HTTP の使用 **1-3, C-25**

RCP の使用 **C-38**

TFTP の使用 **C-28**

準備 **C-28, C-31, C-36**

デバイス マネージャまたは Network Assistant の
使用 **C-25**

古いイメージの削除 **C-30**

理由 **C-25**

コンフィギュレーション ファイル

FTP の使用 **C-14**

RCP の使用 **C-18**

TFTP の使用 **C-12**

準備 **C-11, C-14, C-17**

理由 **C-9**

ダウンロード可能な ACL **10-19, 10-20, 10-61**

タグ付きパケット

IEEE 802.1Q **18-4**

レイヤ 2 プロトコル **18-8**

脱退タイマーの設定、IGMP **25-6**

端末回線、パスワードの設定 **9-6**

ち

小さいフレームの着信レート、設定 **26-5**

つ

ツイストペア イーサネット、単一方向リンクの検
出 **29-1**

て

ディスタンス ベクタ プロトコル **38-3**

ディレクトリ

作業ディレクトリの表示 **C-4**

作成および削除 **C-4**

変更 **C-4**

デスクトップ テンプレート **5-9, 8-1**

デバイス検出プロトコル **27-1, 28-1**

デバイス マネージャ

スイッチのアップグレード **C-25**

説明 **1-2, 1-6**

帯域内管理 **1-7**

利点 **1-2**

デバッグ

エラー メッセージ出力のリダイレクト **49-22**

コマンドの使用 **49-21**

システム全体診断のイネーブル化 **49-22**

特定機能に関するイネーブル化 **49-21**

デフォルト ゲートウェイ **3-16, 38-13**

デフォルト設定

802.1x **10-34**

BGP **38-49**

CDP **27-2**

DHCP **23-9**

DHCP Option 82 **23-10**

DHCP スヌーピング **23-9**

DHCP スヌーピング バインディング データベー
ス **23-10**

DNS **7-17**

EIGRP **38-40**

EtherChannel **37-12**

Flex Link **22-8**

HSRP **42-6**

IEEE 802.1Q トンネリング **18-4**

IGMP **46-42**

IGMP スヌーピング **25-7, 40-6**

IGMP スロットリング **25-26**

IGMP フィルタリング **25-26**

- IP SLA [43-6](#)
 - IPv6 [39-11](#)
 - IP アドレス指定、IP ルーティング [38-6](#)
 - IP ソース ガード [23-20](#)
 - IP マルチキャスト ルーティング [46-12](#)
 - IS-IS [38-71](#)
 - LLDP [28-5](#)
 - MAC アドレス テーブル [7-22](#)
 - MAC アドレス テーブル移動更新 [22-8](#)
 - MSDP [47-4](#)
 - MSTP [20-16](#)
 - MVR [25-20](#)
 - NTP [7-4](#)
 - OSPF [38-29](#)
 - PIM [46-12](#)
 - RADIUS [9-28](#)
 - RIP [38-22](#)
 - RMON [31-3](#)
 - RSPAN [30-11](#)
 - SDM テンプレート [8-5](#)
 - SNMP [33-7](#)
 - SPAN [30-11](#)
 - SSL [9-53](#)
 - STP [19-13](#)
 - TACACS+ [9-13](#)
 - UDLD [29-4](#)
 - VLAN [14-8](#)
 - VLAN、レイヤ 2 イーサネット インターフェイス [14-18](#)
 - VMPS [14-29](#)
 - VTP [15-9](#)
 - WCCP [45-6](#)
 - イーサネット インターフェイス [12-18](#)
 - オプションのスパニング ツリー機能の設定 [21-12](#)
 - 音声 VLAN [16-3](#)
 - 起動 [3-18](#)
 - システム名とプロンプト [7-16](#)
 - システム メッセージ ログイング [32-4](#)
 - 自動 QoS [36-21](#)
 - 初期スイッチ情報 [3-3](#)
 - スイッチ スタック [5-19](#)
 - ダイナミック ARP インスペクション [24-6](#)
 - パケットのフラッディング [48-4](#)
 - パスワードおよび権限レベル [9-3](#)
 - バナー [7-19](#)
 - 標準 QoS [36-31](#)
 - プライベート VLAN [17-7](#)
 - マルチ VRF CE [38-82](#)
 - レイヤ 2 インターフェイス [12-18](#)
 - レイヤ 2 プロトコル トンネリング [18-11](#)
 - デフォルト設定、Web ベース認証
 - 802.1X [11-9](#)
 - デフォルトのネットワーク [38-98](#)
 - デフォルトのルート [38-98](#)
 - デフォルト ルータ プリファレンス
 - 「DRP」を参照
 - デフォルト ルーティング [38-3](#)
 - デュアル IPv4/IPv6 テンプレート [8-2, 39-6](#)
 - デュアル アクティブ検出 [37-6](#)
 - デュアル プロトコル スタック
 - IPv4 および IPv6 [39-6](#)
 - SDM テンプレートのサポート [39-6](#)
 - 電源管理 TLV [28-2, 28-7](#)
 - 転送遅延時間
 - MSTP [20-25](#)
 - STP [19-24](#)
 - 転送保留カウンタ
 - 「STP」を参照
 - 転送、ユニキャスト要求 [1-6](#)
 - 転送、ルーティングできないプロトコル [48-1](#)
 - テンプレート、SDM [8-2](#)
-
- と
- 等価コスト ルーティング [1-15, 38-97](#)
 - 透過的な DSCP [36-41](#)
 - 透過モード、VTP [15-4](#)
 - 同期化、BGP [38-52](#)

統計情報

802.1X [11-18](#)
 802.1x [10-66](#)
 CDP [27-5](#)
 IP マルチキャスト ルーティング [46-66](#)
 LLDP [28-11](#)
 LLDP-MED [28-11](#)
 NMSP [28-11](#)
 OSPF [38-37](#)
 QoS 入出力 [36-80](#)
 RMON イーサネット グループ [31-6](#)
 RMON グループ履歴 [31-5](#)
 SNMP 入出力 [33-20](#)
 VTP [15-19](#)
 インターフェイス [12-34](#)

統合ワイヤレス LAN コントローラ スイッチ
 「3750G 統合ワイヤレス LAN コントローラ スイッチ」
 を参照

到達可能性、IP SLA IP ホストのトラッキング [44-9](#)

トークンリング VLAN
 VTP のサポート [15-5](#)
 サポート [14-6](#)

独立 VLAN [17-2, 17-3](#)
 独立ポート [17-2](#)

都市ロケーション [28-3](#)
 特権 EXEC モード [2-2](#)
 ドメイン、ISO IGRP ルーティング [38-70](#)
 ドメイン名
 DNS [7-16](#)
 VTP [15-10](#)

トラッキング、IP ルーティング ステート [44-2](#)
 トラッキング、インターフェイス ライン プロトコル ステート [44-2](#)
 トラッキング オブジェクト [44-2](#)
 ウェイトしきい値 [44-5](#)
 パーセンテージしきい値 [44-6](#)
 ブール論理式 [44-4](#)

トラッキング プロセス [44-1](#)
 トラッキング リスト

設定 [44-4](#)タイプ [44-4](#)トラック ステート、IP SLA のトラッキング [44-9](#)

トラップ

MAC アドレス通知の設定 [7-23, 7-25, 7-27](#)イネーブル化 [7-23, 7-25, 7-27, 33-13](#)概要 [33-1, 33-4](#)通知タイプ [33-13](#)定義 [33-3](#)マネージャの設定 [33-13](#)トラップドア メカニズム [3-2](#)

トラフィック

非分割 [35-6](#)フラッディングのブロッキング [26-8](#)分割 [35-6](#)分割された IPv6 [41-3](#)

トラフィックの優先処理

「QoS」を参照

トラフィックの抑制 [26-2](#)トラフィック ポリシング [1-14](#)

トラブルシューティング

CiscoWorks [33-4](#)CPU 使用率 [49-26](#)debug コマンド [49-21](#)PIMv1 および PIMv2 の相互運用性の問題 [46-38](#)ping [49-15](#)SFP のセキュリティおよび ID [49-14](#)show forward コマンド [49-23](#)traceroute [49-18](#)システム メッセージ ロギング [32-1](#)障害 (クラッシュ) 情報の表示 [49-25](#)接続の問題 [49-15, 49-17, 49-18](#)単一方向リンクの検出 [29-1](#)パケット転送の設定 [49-23](#)トランキング カプセル化 [1-9](#)

トランク

DTP をサポートしないデバイス [14-16](#)ISL [14-15](#)許可 VLAN リスト [14-21](#)

設定 **14-20, 14-25, 14-26**
 タグなしトラフィック用のネイティブ
 VLAN **14-23**
 パラレル **14-26**
 負荷分散
 STP パス コストの設定 **14-26**
 STP ポート プライオリティの使用 **14-24, 14-25**
 ブルーニング適格リスト **14-22**
 トランク フェールオーバー
 「リンクステート トラッキング」を参照
 トランク ポート
 カプセル化 **14-20, 14-25, 14-26**
 設定 **14-20**
 定義 **12-4, 14-3**
 ドロップしきい値、レイヤ 2 プロトコル パケッ
 ト **18-12**
 トンネリング
 IEEE 802.1Q **18-2**
 定義 **18-1**
 レイヤ 2 プロトコル **18-8**
 トンネル ポート
 IEEE 802.1Q、設定 **18-7**
 説明 **12-4, 18-2**
 他の機能との非互換性 **18-6**
 定義 **14-4**

な

内部ネイバー、BGP **38-52**
 夏時間 **7-14**
 名前付き IPv4 ACL **35-15**

に

二重タグ パケット
 IEEE 802.1Q トンネリング **18-2**
 レイヤ 2 プロトコル トンネリング **18-11**
 認識不能な Type-Length-Value (TLV) のサポー
 ト **15-5**

認証

EIGRP **38-44**
 HSRP **42-11**
 NTP アソシエーション **7-5**
 OpenIxx **10-29**
 RADIUS
 鍵 **9-28**
 ログイン **9-30**
 TACACS+
 鍵 **9-13**
 定義 **9-11**
 ログイン **9-14**
 ローカル モードでの AAA の実装 **9-45**
 「ポートベースの認証」も参照
 認証鍵、ルーティング プロトコル **38-110**
 認証失敗 VLAN
 「制限付き VLAN」を参照
 認証の互換性、Catalyst 6000 スイッチ **10-8**
 認証マネージャ
 CLI コマンド **10-9**
 概要 **10-7**
 古い 802.1x CLI コマンドとの互換性 **10-9**

ね

ネイティブ VLAN
 IEEE 802.1Q トンネリング **18-4**
 設定 **14-23**
 デフォルト **14-23**
 ネイバー、BGP **38-63**
 ネットワーク管理
 CDP **27-1**
 RMON **31-1**
 SNMP **33-1**
 ネットワーク設計
 サービス **1-21**
 パフォーマンス **1-21**
 ネットワークの構成例
 高性能ワイヤリング クローゼット **1-23**

- コスト効率の高いワイヤリングクローゼット **1-22**
 - サーバ集約および Linux サーバクラスタ **1-24**
 - 集合住宅ネットワーク **1-28**
 - 冗長ギガビット バックボーン **1-24**
 - 大規模ネットワーク **1-27**
 - 中小規模ネットワーク **1-26**
 - 長距離、広帯域トランスポート **1-30**
 - ネットワーク サービスの提供 **1-21**
 - ネットワーク パフォーマンスの向上 **1-21**
 - ネットワーク パフォーマンス、IP SLA での測定 **43-3**
 - ネットワーク ポリシー TLV **28-2, 28-7**
-
- は**
- バージョン依存型透過モード **15-5**
 - バージョン不一致 (VM) モード
 - 自動アップグレードによる自動的なアップグレード **5-11**
 - 自動アドバイスによる手動アップグレード **5-12**
 - 自動抽出によるアップグレード **5-11**
 - バージョン不一致モード
 - 説明 **5-10**
 - パーセンテージしきい値、トラッキング リスト **44-6**
 - ハードウェア制限とレイヤ 3 インターフェイス **12-28**
 - バインディング
 - DHCP スヌーピング データベース **23-7**
 - IP ソース ガード **23-18**
 - アドレス、Cisco IOS DHCP サーバ **23-7**
 - バインディング データベース
 - DHCP スヌーピング
 - 「DHCP スヌーピング バインディング データベース」を参照
 - アドレス、DHCP サーバ
 - 「DHCP」、「Cisco IOS サーバ データベース」を参照
 - バインディング テーブル、DHCP スヌーピング
 - 「DHCP スヌーピング バインディング データベース」を参照
 - パケットの変更、QoS **36-20**
 - パス MTU ディスカバリ **39-4**
 - パス コスト
 - MSTP **20-22**
 - STP **19-21**
 - パスワード
 - VTP ドメイン **15-10**
 - 暗号化 **9-4**
 - 回復 **49-3**
 - 回復のディセーブル化 **9-5**
 - 概要 **9-1**
 - クラスタ内 **6-15**
 - セキュリティ **1-10**
 - 設定
 - Telnet **9-6**
 - イネーブル **9-3**
 - イネーブル シークレット **9-4**
 - ユーザ名 **9-7**
 - デフォルト設定 **9-3**
 - バックアップ インターフェイス
 - 「Flex Link」を参照
 - バックアップ スタティック ルーティング、設定 **44-12**
 - バックアップ リンク **22-2**
 - パッシブ インターフェイス
 - OSPF **38-35**
 - 設定 **38-107**
 - バナー
 - 設定
 - MoTD ログイン **7-19**
 - ログイン **7-20**
 - デフォルト設定 **7-19**
 - 表示されるとき **7-18**
 - パフォーマンス向上機能 **1-4**
 - パフォーマンス、ネットワークの設計 **1-21**
 - パラレル パス、ルーティング テーブル内 **38-97**
 - 範囲
 - インターフェイス **12-14**
 - マクロ **12-15**

ひ

非 IP トラフィックのフィルタリング **35-28**

ピア、BGP **38-63**

非階層型ポリシー マップ

設定時の注意事項 **36-34**

説明 **36-9**

光ファイバ、単一方向リンクの検出 **29-1**

非対称リンク、IEEE 802.1Q トンネリング **18-4**

非トランッキング モード **14-17**

標準範囲 VLAN **14-5**

設定 **14-5**

設定時の注意事項 **14-6**

定義 **14-1**

不一致、自動ネゴシエーション **49-13**

フィルタ、IP

「ACL」、「IP」を参照

フィルタリング

IPv6 トラフィック **41-4, 41-8**

show および more コマンドの出力 **2-10**

VLAN **35-31**

非 IP トラフィック **35-28**

フィルタリング、show および more コマンド出力 **2-10**

ブート ストラップ ルータ (BSR)、説明 **46-7**

ブート ローダ

アクセス **3-21**

環境変数 **3-21**

説明 **3-2**

トラップドア メカニズム **3-2**

プロンプト **3-21**

ブール論理式、トラッキング リスト **44-4**

フェールオーバーのサポート **1-8**

フォールバック ブリッジング

STP

hello BPDU インターバル **48-9**

VLAN ブリッジ STP **48-2**

VLAN ブリッジ スパニング ツリー プライオリティ **48-6**

インターフェイスでディセーブル **48-10**

インターフェイス プライオリティ **48-7**

最大アイドル時間 **48-10**

転送遅延インターバル **48-9**

パス コスト **48-7**

SVI およびルーテッド ポート **48-2**

VLAN ブリッジ STP **19-12**

インターフェイスの接続 **12-11**

概要 **48-1**

サポート **1-15**

サポートされないプロトコル **48-4**

スタックの変更、作用 **48-3**

設定時の注意事項 **48-4**

説明 **48-1**

デフォルト設定 **48-4**

ふ

ファイル

crashinfo、説明 **49-25**

tar

イメージ ファイル形式 **C-26**

作成 **C-6**

抽出 **C-8**

内容の表示 **C-7**

拡張 crashinfo

位置 **49-26**

説明 **49-26**

基本 crashinfo

位置 **49-25**

説明 **49-25**

コピー **C-5**

削除 **C-6**

内容の表示 **C-8**

ファイル システム

使用可能なファイル システムの表示 **C-2**

デフォルトの設定 **C-3**

ネットワーク ファイル システム名 **C-5**

ファイル情報の表示 **C-3**

ローカル ファイル システム名 **C-1**

- ブリッジ グループ
 - 機能 [48-2](#)
 - 削除 [48-5](#)
 - 作成 [48-4](#)
 - サポートされる数 [48-5](#)
 - 説明 [48-2](#)
 - 表示 [48-11](#)
- ブリッジ テーブル
 - クリア [48-11](#)
 - 表示 [48-11](#)
- プロトコル、サポートされない [48-4](#)
- 保護ポート [48-4](#)
- レーム転送
 - パケットの転送 [48-2](#)
 - パケットのフラッディング [48-2](#)
- 複数動作のスケジューリング、IP SLA [43-5](#)
- 物理ポート [12-3](#)
- 不適合マークダウン [1-14](#)
- プライオリティ
 - CoS の信頼 [16-7](#)
 - CoS の変更 [16-7](#)
 - HSRP [42-8](#)
- プライベート VLAN
 - IP アドレス指定 [17-3](#)
 - SDM テンプレート [17-4](#)
 - SVI [17-5](#)
 - エンドステーション アクセス [17-3](#)
 - コミュニティ VLAN [17-2, 17-3](#)
 - コミュニティ ポート [17-2](#)
 - 混合ポート [17-2](#)
 - サブドメイン [17-1](#)
 - スイッチ スタック [17-6](#)
 - セカンダリ VLAN [17-2](#)
 - 設定 [17-10](#)
 - 設定作業 [17-6](#)
 - 設定時の注意事項 [17-7, 17-9](#)
 - デフォルト設定 [17-7](#)
 - 独立 VLAN [17-2, 17-3](#)
 - 独立ポート [17-2](#)
 - トラフィック [17-5](#)
 - 複数のスイッチにまたがる [17-4](#)
 - プライマリ VLAN [17-1, 17-3](#)
 - ポート
 - コミュニティ [17-2](#)
 - 混合 [17-2](#)
 - 混合ポートの設定 [17-13](#)
 - 設定時の注意事項 [17-9](#)
 - 説明 [14-4](#)
 - 独立 [17-2](#)
 - ホスト ポートの設定 [17-12](#)
 - マッピング [17-14](#)
 - モニタリング [17-15](#)
 - 利点 [17-1](#)
 - プライベート VLAN エッジ ポート
 - 「保護ポート」を参照
 - プライマリ VLAN [17-1, 17-3](#)
 - プライマリ リンク [22-2](#)
 - フラッシュ デバイス、数 [C-1](#)
 - フラッディング トラフィック、ブロッキング [26-8](#)
 - プリエンプト遅延、デフォルト設定 [22-8](#)
 - プリエンプト、デフォルト設定 [22-8](#)
 - ブリッジ グループ
 - 「フォールバック ブリッジング」を参照
 - ブリッジド パケット、ACL [35-40](#)
 - プルーニング、VTP
 - イネーブル化
 - VTP ドメイン [15-16](#)
 - ポート上 [14-22](#)
 - 概要 [15-6](#)
 - ディセーブル化
 - VTP ドメイン [15-17](#)
 - ポート上 [14-23](#)
 - 例 [15-7](#)
 - プルーニング適格リスト
 - VLAN [15-17](#)
 - VTP プルーニング [15-6](#)
 - 変更 [14-22](#)
 - プレフィクス リスト、BGP [38-60](#)

フローチャート

QoS 出力のキューイングおよびスケジューリング **36-17**

QoS 入力 of キューイングおよびスケジューリング **36-15**

QoS のポリシングおよびマーキング **36-10**

QoS 分類 **36-6**

ブロードキャスト ストーム **26-1, 38-15**

ブロードキャスト ストーム制御コマンド **26-4**

ブロードキャストのフラッディング **38-18**

ブロードキャスト パケット

指定 **38-15**

フラッディング **38-15**

プロキシ ARP

IP ルーティングがディセーブルの場合 **38-13**

設定 **38-12**

定義 **38-10**

プロキシ レポート **22-4**

ブロッキング、パケット **26-7**

プロトコル依存モジュール、EIGRP **38-39**

プロビジョニングされたスイッチと IP ソース ガード **23-20**

へ

ヘルプ、コマンドライン **2-3**

編集機能

イネーブル化およびディセーブル化 **2-7**

画面幅よりも長いコマンドライン **2-9**

使用するキーストローク **2-7**

ほ

防止、不正アクセス **9-1**

ポート

10 ギガビット イーサネット モジュール **12-7**

IEEE 802.1Q トンネル **14-4**

VLAN 割り当て **14-10**

アクセス **12-3**

スイッチ **12-3**

スタティック アクセス **14-3, 14-10**

セキュア **26-9**

ダイナミック アクセス **14-4**

トランク **14-3, 14-15**

ブロッキング **26-7**

保護 **26-6**

ルーテッド **12-5**

ポート ACL

タイプ **35-3**

定義 **35-2**

ポート VLAN ID TLV **28-2**

ポート記述 TLV **28-2**

ポートシャットダウン応答、VMPS **14-28**

ポート セキュリティ

QoS の信頼境界機能 **36-39**

イネーブル化 **26-20**

違反 **26-10**

エージング タイム **26-18**

スタック **26-20**

スティッキー ラーニング **26-10**

設定 **26-13**

説明 **26-9**

他の機能 **26-12**

デフォルト設定 **26-11**

トランク ポート **26-15**

表示 **26-21**

プライベート VLAN **26-20**

ポートチャネル

「EtherChannel」を参照

ポート プライオリティ

MSTP **20-21**

STP **19-19**

ポートブロッキング **1-4, 26-7**

ポートベース認証

ACL および RADIUS Filter-Id アトリビュート **10-31**

イネーブル化

802.1X 認証 **11-12**

- ユーザ分散
 - 概要 [10-28](#)
 - 注意事項 [10-28](#)
- ポートベースの認証
 - EAPOL-Start フレーム [10-5](#)
 - EAP-Request/Identity フレーム [10-5](#)
 - EAP-Response/Identity フレーム [10-5](#)
 - VLAN 割り当て
 - AAA 許可 [10-40](#)
 - 設定作業 [10-17](#)
 - 説明 [10-16](#)
 - 特性 [10-17](#)
 - Wake-on-LAN、説明 [10-26](#)
 - アカウントिंग [10-15](#)
 - アクセス不能認証バイパス
 - 説明 [10-23](#)
 - 注意事項 [10-36](#)
 - 音声 VLAN
 - PVID [10-24](#)
 - VVID [10-24](#)
 - 説明 [10-24](#)
 - 音声認識 802.1X セキュリティ
 - 設定 [10-38](#)
 - 説明 [10-30, 10-38](#)
 - 開始およびメッセージ交換 [10-5](#)
 - カプセル化 [10-3](#)
 - 旧版のリリースからのアップグレード [36-27](#)
 - クライアント、定義 [10-3, 11-2](#)
 - ゲスト VLAN
 - 設定時の注意事項 [10-21, 10-22](#)
 - 説明 [10-21](#)
 - 柔軟な認証の順序
 - 概要 [10-29](#)
 - 設定 [10-64](#)
 - 準備チェック
 - 設定 [10-37](#)
 - 説明 [10-16, 10-37](#)
 - スイッチ
 - RADIUS クライアント [10-3](#)
 - プロキシ [10-3, 11-2](#)
 - スイッチ サブリカント
 - 概要 [10-30](#)
 - 設定 [10-59](#)
 - スタックの変更、作用 [10-11](#)
 - 設定
 - 802.1x 認証 [10-40](#)
 - RADIUS サーバ [10-43, 11-13](#)
 - アクセス不能認証バイパス [10-53](#)
 - 違反モード [10-39 ~ 10-40](#)
 - クライアントの手動での再認証 [10-45](#)
 - ゲスト VLAN [10-50](#)
 - スイッチからクライアントへの再送信時間 [10-46](#)
 - スイッチからクライアントへのフレーム再送信回数 [10-47, 10-48](#)
 - スイッチ上の RADIUS サーバ パラメータ [10-42, 11-12](#)
 - 制限付き VLAN [10-51](#)
 - 待機時間 [10-46](#)
 - 定期的な再認証 [10-44](#)
 - ホスト モード [10-43](#)
 - 設定時の注意事項 [10-35, 11-9](#)
 - 説明 [10-1](#)
 - ダウンロード可能な ACL とリダイレクト URL
 - 概要 [10-19 ~ 10-20](#)
 - 設定 [10-61 ~ 10-63](#)
 - デバイスの役割 [10-2, 11-2](#)
 - デフォルト設定 [10-34, 11-9](#)
 - デフォルト値へのリセット [10-66](#)
 - 統計情報の表示 [10-66, 11-18](#)
 - 統計情報、表示 [10-66](#)
 - 認証サーバ
 - RADIUS サーバ [10-3](#)
 - 定義 [10-3, 11-2](#)
 - 方式リスト [10-40](#)
 - ポート
 - 音声 VLAN [10-24](#)
 - 許可および無許可 [10-10](#)

許可ステートおよび dot1x port-control コマンド **10-11**

ポートごとに許可できるデバイスの最大数 **10-37**

ポート セキュリティ

- 音声 VLAN **10-26**
- 説明 **10-25**
- 相互作用 **10-25**
- マルチホスト モード **10-12**

ホスト モード **10-12**

マジック パケット **10-26**

マルチ認証 **10-14**

ユーザ単位 ACL

- AAA 許可 **10-40**
- RADIUS サーバアトリビュート **10-18**
- 設定作業 **10-19**
- 説明 **10-18**

ポートベースの認証違反モードの設定 **10-39 ~ 10-40**

ポートベースの認証方式、サポートされる **10-7**

ポート メンバシップ モード、VLAN **14-3**

保護ポート **1-10, 26-6**

ホスト、ダイナミック ポート上の制限 **14-33**

ホスト ポート

- 種類 **17-2**
- 設定 **17-12**

ホスト名、クラスタ内 **6-14**

ポリサー

- 数 **36-35**
- 設定

 - 一致する各トラフィック クラス **36-49**
 - 複数のトラフィック クラス **36-60**

- 説明 **36-4**
- タイプ **36-9**
- 表示 **36-80**

ポリシー マップ、QoS

- SVI の階層

 - 設定 **36-53**
 - 設定時の注意事項 **36-34**
 - 説明 **36-11**

- 階層 **36-8**

- 説明 **36-7**
- 特性 **36-49**
- 表示 **36-81**
- 物理ポートの非階層型

 - 設定時の注意事項 **36-34**
 - 説明 **36-9**

ポリシング

- 階層

 - 「階層型のポリシー マップ」を参照
 - 説明 **36-4**
 - トークン バケット アルゴリズム **36-9**

ポリシング済み DSCP マップ、QoS **36-64**

ま

マーキング

- 集約ポリサーのアクション **36-60**
- 説明 **36-4, 36-8**

マクロ

- 「Auto Smartport マクロ」も参照
- 「Smartport マクロ」を参照

マジック パケット **10-26**

マッピング テーブル、QoS

- 設定

 - CoS/DSCP **36-62**
 - DSCP **36-62**
 - DSCP/CoS **36-65**
 - DSCP/DSCP 変換 **36-66**
 - IP precedence/DSCP **36-63**
 - ポリシング済み DSCP **36-64**

- 説明 **36-12**

マルチ VRF CE

- サポート **1-15**
- 設定 **38-82**
- 設定時の注意事項 **38-83**
- 設定例 **38-90**
- 定義 **38-80**
- デフォルト設定 **38-82**
- ネットワーク コンポーネント **38-82**

パケット転送処理 **38-82**
 表示 **38-94**
 モニタリング **38-94**
 マルチキャスト TV アプリケーション **25-19**
 マルチキャスト VLAN **25-18**
 マルチキャスト グループ
 加入 **25-3**
 静的加入 **25-10, 40-8**
 即時脱退 **25-6**
 脱退 **25-5**
 マルチキャスト ストーム **26-1**
 マルチキャスト ストーム制御コマンド **26-4**
 マルチキャスト パケット
 ACL **35-41**
 ブロッキング **26-8**
 マルチキャスト ルータ インターフェイス、モニ
 タ **25-17, 40-12**
 マルチキャスト ルータ ポート **22-3, 22-5**
 マルチキャスト ルータ ポート、追加 **25-10, 40-8**
 マルチドメイン認証
 「MDA」を参照
 マルチ認証 **10-14**
 マルチ認証モード
 設定 **10-43**
 「マルチ認証モード」を参照

み

ミラーリング、トラフィック解析 **30-1**

む

無許可ポート、IEEE 802.1X **10-10**
 矛盾、設定 **49-13**

め

メッセージ、ユーザに、バナーを使用 **7-18**
 メトリック、BGP 内 **38-57**

メトリック変換、ルーティング プロトコル間 **38-103**
 メトロ タグ **18-2**
 メンバー スイッチ
 管理 **6-17**
 「候補スイッチ」、「クラスタ スタンバイ グループ」、
 「スタンバイ コマンド スイッチ」も参照
 自動検出 **6-5**
 接続の回復 **49-13**
 定義 **6-2**
 パスワード **6-14**
 要件 **6-4**
 メンバシップ モード、VLAN ポート **14-3**

も

モジュール番号 **12-12**
 モニタリング
 BGP **38-68**
 CDP **27-5**
 CEF **38-96**
 EIGRP **38-46**
 Flex Link **22-14**
 HSRP **42-14**
 IEEE 802.1Q トンネリング **18-18**
 IGMP
 スヌーピング **25-16, 40-12**
 フィルタ **25-30**
 IP
 アドレス テーブル **38-20**
 マルチキャスト ルーティング **46-65**
 ルート **38-111**
 IP SLA 動作 **43-13**
 IPv4 ACL の設定 **35-42**
 IPv6 **39-28**
 IPv6 ACL 設定 **41-9**
 IS-IS **38-79**
 ISO CLNS **38-79**
 MAC アドレス テーブル移動更新 **22-14**
 MSDP ピア **47-18**

MVR [25-24](#)
 OSPF [38-37](#)
 RP マッピング情報 [46-38](#)
 SA メッセージ [47-18](#)
 SFP ステータス [12-35, 49-15](#)
 SSM マッピング [46-24](#)
 VLAN [14-15](#)
 フィルタ [35-43](#)
 マップ [35-43](#)
 VMPS [14-32](#)
 VTP [15-19](#)
 アクセス グループ [35-42](#)
 インターフェイス [12-34](#)
 オブジェクト トラッキング [44-13](#)
 機能 [1-16](#)
 スイッチ間を流れるトラフィック [31-1](#)
 速度およびデブレックス モード [12-21](#)
 単一方向リンクのケーブル [29-1](#)
 トラフィックの抑制 [26-21](#)
 トンネリング [18-18](#)
 パケットのフラッディング [48-11](#)
 プライベート VLAN [17-15](#)
 プローブによるネットワーク トラフィック解析 [30-2](#)
 ポート
 ブロッキング [26-21](#)
 保護 [26-21](#)
 マルチ VRF CE [38-94](#)
 マルチキャスト ルータ インターフェイス [25-17, 40-12](#)
 レイヤ 2 プロトコル トンネリング [18-18](#)

ゆ

ユーザ EXEC モード [2-2](#)
 ユーザ単位 ACL と Filter-Id [10-8](#)
 ユーザ名ベースの認証 [9-7](#)
 ユニキャスト MAC アドレス フィルタリング [1-6](#)
 CPU パケット [7-29](#)

 スタティック アドレスの追加 [7-30](#)
 設定時の注意事項 [7-29](#)
 説明 [7-29](#)
 ブロードキャスト MAC アドレス [7-29](#)
 マルチキャスト アドレス [7-29](#)
 ルータ MAC アドレス [7-29](#)
 ユニキャスト ストーム [26-1](#)
 ユニキャスト ストーム制御コマンド [26-4](#)
 ユニキャスト トラフィック、ブロッキング [26-8](#)

よ

予約済みアドレス、DHCP プール [23-29](#)

ら

ライン コンフィギュレーション モード [2-3](#)

り

リセット、BGP 内 [38-55](#)
 リダイレクト URL [10-19, 10-61](#)
 リモート SPAN [30-3](#)
 「RSPAN」を参照
 履歴
 コマンドの呼び出し [2-6](#)
 説明 [2-6](#)
 ディセーブル化 [2-7](#)
 バッファ サイズの変更 [2-6](#)
 履歴テーブル、Syslog メッセージの重大度および数 [32-10](#)
 リロード、ソフトウェア [3-22](#)
 リンクステート トラッキング
 設定 [37-28](#)
 説明 [37-25](#)
 リンクステート プロトコル [38-3](#)
 リンク、単一方向 [29-1](#)
 リンクに対してローカルなユニキャストアドレス [39-4](#)
 リンクの失敗、単一方向の検出 [20-8](#)

リンクの冗長性

「Flex Link」を参照

隣接テーブル、CEF **38-95**

る

ルータ ACL

タイプ **35-4**

定義 **35-2**

ルータ ID、OSPF **38-37**

ルーティング

情報の再配信 **38-99**

スタティック **38-3**

ダイナミック **38-3**

デフォルト **38-3**

ルーティング ドメイン連合、BGP **38-66**

ルーティング プロトコルの管理距離 **38-98**

ルーテッド パケット、ACL **35-41**

ルーテッド ポート

IP アドレス **12-28, 38-5**

スイッチ クラスタ **6-9**

設定 **38-5**

定義 **12-5**

ルート ガード

イネーブル化 **21-18**

サポート **1-9**

説明 **21-10**

ルート計算タイマー、OSPF **38-35**

ルート サマライズ、OSPF **38-34**

ルート スイッチ

MSTP **20-19**

STP **19-17**

ルート選択、BGP **38-56**

ルート ターゲット、VPN **38-82**

ルート ダンピング化、BGP **38-67**

ルート マップ

BGP **38-58**

Policy-Based Routing (ポリシーベース ルーティング) **38-103**

ルート リフレクタ、BGP **38-66**

ループ ガード

イネーブル化 **21-19**

サポート **1-9**

説明 **21-11**

れ

例

ネットワーク構成 **1-20**

レイヤ 2 traceroute

1 ポートに複数のデバイス **49-18**

ARP **49-18**

CDP **49-17**

IP アドレスおよびサブネット **49-18**

MAC アドレスおよび VLAN **49-17**

使用時の注意事項 **49-17**

説明 **49-17**

ブロードキャスト トラフィック **49-17**

マルチキャスト トラフィック **49-17**

ユニキャスト トラフィック **49-17**

レイヤ 2 インターフェイス、デフォルト設定 **12-18**

レイヤ 2 フレーム、CoS での分類 **36-2**

レイヤ 2 プロトコル トンネリング

EtherChannel 用の設定 **18-15**

設定 **18-10**

注意事項 **18-12**

定義 **18-8**

デフォルト設定 **18-11**

レイヤ 3 インターフェイス

IPv4 および IPv6 アドレスの割り当て **39-15**

IPv6 アドレスの割り当て **39-12**

IP アドレスの割り当て **38-7**

タイプ **38-5**

レイヤ 2 モードからの変更 **38-7, 38-87**

レイヤ 3 機能 **1-14**

レイヤ 3 パケット、分類方法 **36-2**

レポート抑制、IGMP

説明 **25-6**

ディセーブル化 [25-16, 40-11](#)

ろ

ローカル SPAN [30-2](#)

ロード バランシング [42-4](#)

ローベースのパケット分類 [1-13](#)

ログイン認証

RADIUS [9-30](#)

TACACS+ [9-14](#)

ログイン バナー [7-18](#)

ログ メッセージ

「システム メッセージ ロギング」を参照

ログ メッセージ、ACL [35-9](#)

ログ メッセージのシーケンス番号 [32-8](#)

ログ メッセージのタイム スタンプ [32-8](#)

ロケーション TLV [28-3, 28-7](#)

わ

ワイヤレス LAN コントローラ [A-1, A-3](#)

割り当て、新しいメンバー、スイッチ スタック [5-7](#)