



Catalyst 2960 スイッチ ソフトウェア コンフィギュ レーション ガイド

Catalyst 2960 Switch Software Configuration Guide

Cisco IOS Release 12.2(52)SE 2009 年 9 月

Text Part Number: OL-8603-07-J

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

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。 米国サイト掲載ドキュメントとの差異が生じる場合があるため、 正式な内容については米国サイトのドキュメントを参照ください。 また、契約等の記述については、弊社販売パートナー、または、 弊社担当者にご確認ください。

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

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

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

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

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

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

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

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

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド Copyright © 2004–2009 Cisco Systems, Inc. All rights reserved.

Copyright © 2004–2010, シスコシステムズ合同会社. All rights reserved.



CONTENTS

はじめに xxxv

対象読者	xxxv		
目的	xxxv		
表記法	xxxvi		
関連資料	xxxvi		
マニュア	ルの入手方	法およびテクニカル サポート	xxxvii

CHAPTER 1

概要 1-1

	機能 1-1	
	使用および導入を簡素化する機能 1-2	
	パフォーマンス向上機能 1-3	
	管理オプション 1-5	
	管理の簡易性に関する機能 1-5	
	アベイラビリティおよび冗長性に関する機能 1-8	
	VLAN 機能 1-9	
	セキュリティ機能 1-10	
	QoS および CoS 機能 1-13	
	レイヤ 3 機能 1-15	
	Power over Ethernet の機能 1-15	
	モニタ機能 1-15	
	スイッチ初期設定後のデフォルト値 1-16	
	ネットワークの構成例 1-19	
	スイッチを使用する場合の設計概念 1-19	
	スイッチを使用した中小規模のネットワーク Catalyst 2960 スイッチ 1-:	22
	長距離広帯域トランスポートの構成 1-24	
	次の作業 1-24	
CHAPTER 2	 CLIの使用方法 2-1	
	コマンド モードの概要 2-1	
	ヘルプ システムの概要 2-3	
	コマンドの省略形 2-4	
	コマンドの no 形式および default 形式の概要 2-4	
	CLI のエラー メッセージ 2-5	

CHAPTER 3

コンフィギュレーション ロギングの使用方法 2-5 コマンド履歴の使用方法 2-6 コマンド履歴バッファ サイズの変更 2-6 コマンドの呼び出し 2-6 コマンド履歴機能のディセーブル化 2-7 編集機能の使用方法 2-7 編集機能のイネーブル化およびディセーブル化 2-7 キーストロークによるコマンドの編集 2-7 画面幅よりも長いコマンドラインの編集 2-9 show および more コマンド出力の検索およびフィルタリング 2-10 CLI のアクセス方法 2-11 コンソール接続または Telnet による CLI アクセス 2-11 スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て 3-1 起動プロセスの概要 3-2 スイッチ情報の割り当て 3-3 デフォルトのスイッチ情報 3-3 DHCP ベースの自動設定の概要 3-4 DHCP クライアントの要求プロセス 3-4 DHCP ベースの自動設定およびイメージ アップデートの概要 3-5 DHCP 自動設定 3-6 DHCP 自動イメージ アップデート 3-6 制限事項と制約事項 3-6 DHCP ベースの自動設定の設定 3-7 DHCP サーバ設定時の注意事項 3-7 TFTP サーバの設定 3-8 DNS の設定 3-8 リレー デバイスの設定 3-9 コンフィギュレーション ファイルの入手方法 3-10 構成例 3-11 DHCP 自動設定機能およびイメージ アップデート機能 3-12 DHCP 自動設定(コンフィギュレーション ファイルだけ)の設定 3-13 DHCP 自動イメージ アップデート (コンフィギュレーション ファイルおよびイメー ジ)の設定 3-14 クライアントの設定 3-15 手動でのスイッチ情報の割り当て 3-16 実行コンフィギュレーションの確認および保存 3-17 スタートアップ コンフィギュレーションの変更 3-18 起動のデフォルト設定 3-18

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

	コンフィギュレーション ファイルの自動ダウンロード 3-18	
	システム コンフィギュレーションを読み書きするためのファイル名の指定	3-19
	手動で起動する場合 3-19	
	特定のソフトウェア イメージを起動する場合 3-20	
	環境変数の制御 3-21	
	ソフトウェア イメージ リロードのスケジュール設定 3-23	
	リロードのスケジュール設定 3-23	
	リロード スケジュール情報の表示 3-24	
CHAPTER 4	 Cisco IOS Configuration Engine の設定 4-1	
	Cisco Configuration Engine ソフトウェアの概要 4-1	
	コンフィギュレーション サービス 4-2	
	イベント サービス 4-3	
	NSM 4-3	
	CNS ID およびデバイスのホスト名に関する重要事項 4-3	
	ConfigID 4-4	
	DeviceID 4-4	
	ホスト名および DeviceID 4-4	
	ホスト名、DeviceID、ConfigID の使用方法 4-5	
	Cisco IOS エージェントの概要 4-5	
	初期設定 4-5	
	差分(部分)設定 4-6	
	同期設定 4-6	
	Cisco IOS エージェントの設定 4-6	
	自動 CNS 設定のイネーブル化 4-7	
	CNS イベント エージェントのイネーブル化 4-7	
	Cisco IOS CNS エージェントのイネーブル化 4-9	
	初期設定のイネーブル化 4-9	
	部分設定のイネーブル化 4-13	
	CNS 設定の表示 4-14	
CHAPTER 5	 スイッチのクラスタ化 5-1	
	スイッチ クラスタの概要 5-2	
	クラスタ コマンド スイッチの特性 5-3	
	スタンバイ クラスタ コマンド スイッチの特性 5-4	
	候補スイッチおよびクラスタ メンバー スイッチの特性 5-4	
	スイッチ クラスタのプランニング 5-5	
	クラスタ候補およびクラスタ メンバーの自動検出 5-5	
	CDP ホップを使用しての検出 5-6	

L

CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出 5-6 異なる VLAN からの検出 5-7 異なる管理 VLAN からの検出 5-9 新しくインストールしたスイッチの検出 5-10 HSRP およびスタンバイ クラスタ コマンド スイッチ 5-11 仮想 IP アドレス 5-12 クラスタ スタンバイ グループに関する他の考慮事項 5-12 クラスタ設定の自動復旧 5-13 IP アドレス 5-14 ホスト名 5-14 パスワード 5-15 SNMP コミュニティ ストリング 5-15 TACACS+ および RADIUS 5-15 LRE プロファイル 5-16 CLI によるスイッチ クラスタの管理 5-16 Catalyst1900 および Catalyst2820 の CLI に関する考慮事項 5-16 SNMP によるスイッチ クラスタの管理 5-17

CHAPTER 6 スイッチの管理

6-1

システム日時の管理 6-1 システム クロックの概要 6-2 NTP の概要 6-2 NTP の設定 6-4 NTP のデフォルト設定 6-4 NTP 認証の設定 6-5 NTP アソシエーションの設定 6-6 NTP ブロードキャスト サービスの設定 6-7 NTP アクセス制限の設定 6-8 NTP パケット用の送信元 IP アドレスの設定 6-11 NTP 設定の表示 6-11 手動での日時の設定 6-12 システム クロックの設定 6-12 日時設定の表示 6-13 タイム ゾーンの設定 6-13 夏時間の設定 6-14 システム名およびプロンプトの設定 6-16 デフォルトのシステム名およびプロンプトの設定 6-16 システム名の設定 6-16 DNS の概要 6-17

Contents

DNS のデフォルト設定 6-17 DNS の設定 6-18 DNS の設定の表示 6-19 バナーの作成 6-19 バナーのデフォルト設定 6-19 MoTD ログイン バナーの設定 6-20 ログイン バナーの設定 6-21 MAC アドレス テーブルの管理 6-22 アドレス テーブルの作成 6-23 MAC アドレスおよび VLAN 6-23 MAC アドレス テーブルのデフォルト設定 6-23 アドレス エージング タイムの変更 6-24 ダイナミック アドレス エントリの削除 6-24 MAC アドレス変更通知トラップの設定 6-25 MAC アドレス移動通知トラップの設定 6-27 MAC しきい値通知トラップの設定 6-28 スタティック アドレス エントリの追加および削除 6-30 ユニキャスト MAC アドレス フィルタリングの設定 6-31 VLAN の MAC アドレス学習のディセーブル化 6-32 アドレス テーブル エントリの表示 6-33 ARP テーブルの管理 6-34

 CHAPTER 7
 SDM テンプレートの設定
 7-1

 SDM テンプレートの概要
 7-1

 スイッチ SDM テンプレートの設定
 7-2

 デフォルトの SDM テンプレート
 7-2

 SDM テンプレートの設定時の注意事項
 SDM テンプレートの設定
 7-3

 SDM テンプレートの表示
 7-3

______ CHAPTER 8 スイッチ ベース認証の設定 8-1

スイッチへの不正アクセスの防止 8-1	
特権 EXEC コマンドへのアクセスの保護 8-2	
デフォルトのパスワードおよび権限レベル設定 8-2	
スタティック イネーブル パスワードの設定または変更 8-3	
暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護	8-4
パスワード回復のディセーブル化 8-5	
端末回線に対する Telnet パスワードの設定 8-6	
ユーザ名とパスワードのペアの設定 8-7	

7-2

複数の権限レベルの設定 8-8 8-8 コマンドの権限レベルの設定 回線に対するデフォルトの権限レベルの変更 8-10 権限レベルへのログインおよび終了 8-10 TACACS+ によるスイッチ アクセスの制御 8-11 TACACS+の概要 8-11 TACACS+の動作 8-13 TACACS+の設定 8-14 TACACS+ のデフォルト設定 8-14 TACACS+ サーバ ホストの特定および認証鍵の設定 8-14 TACACS+ ログイン認証の設定 8-15 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設 定 8-17 TACACS+ アカウンティングの起動 8-18 TACACS+ 設定の表示 8-19 RADIUS によるスイッチ アクセスの制御 8-19 RADIUS の概要 8-19 RADIUS の動作 8-21 RADIUS Change of Authorization 8-21 概要 8-21 Change-of-Authorization 要求 8-22 CoA 要求応答コード 8-23 CoA 要求コマンド 8-25 RADIUS の設定 8-27 RADIUS のデフォルト設定 8-28 RADIUS サーバ ホストの識別 8-28 RADIUS ログイン認証の設定 8-30 AAA サーバ グループの定義 8-32 ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の 設定 8-34 RADIUS アカウンティングの起動 8-35 すべての RADIUS サーバの設定 8-36 ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定 8-36 ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定 8-38 スイッチ上での CoA の設定 8-39 CoA 機能のモニタリングおよびトラブルシューティング 8-40 RADIUS サーバ ロードバランシングの設定 8-40 RADIUS の設定の表示 8-40 スイッチのローカル認証および許可の設定 8-40 SSH のためのスイッチの設定 8-42

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

SSH の概要 8-42 SSH サーバ、統合クライアント、およびサポートされているバージョン 8-42 制限事項 8-43 SSH の設定 8-43 設定時の注意事項 8-43 スイッチで SSH を実行するためのセットアップ 8-44 SSH サーバの設定 8-45 SSH の設定およびステータスの表示 8-46 SSL HTTP のためのスイッチの設定 8-46 セキュア HTTP サーバおよびクライアントの概要 8-47 CA の信頼点 8-47 CipherSuite 8-48 セキュア HTTP サーバおよびクライアントの設定 8-49 SSL のデフォルト設定 8-49 SSL の設定時の注意事項 8-49 CAの信頼点の設定 8-50 セキュア HTTP サーバの設定 8-51 セキュア HTTP クライアントの設定 8-53 セキュア HTTP サーバおよびクライアントのステータスの表示 8-53 SCP のためのスイッチの設定 8-54 Secure Copy に関する情報 8-54 IEEE 802.1x ポートベース認証の設定 9-1 IEEE 802.1x ポートベース認証の概要 9-1 デバイスの役割 9-3 認証プロセス 9-4 認証の開始およびメッセージ交換 9-6 認証マネージャ 9-8 Port-Based 認証方法 9-8 ユーザ単位 ACL および Filter-Id 9-9 認証マネージャ CLI コマンド 9-10 許可ステートおよび無許可ステートのポート 9-11 802.1x のホスト モード 9-12 マルチドメイン認証 9-13 802.1x 複数認証モード 9-14 MAC Move 9-15 802.1x アカウンティング 9-15 802.1x アカウンティング アトリビュート値ペア 9-15 802.1x 準備状態チェック 9-17

CHAPTER 9

VLAN 割り当てを使用した 802.1x 認証 9-17 ユーザ単位 ACL を使用した 802.1x 認証の使用 9-19 ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 9-20 リダイレクト URL の Cisco Secure ACS およびアトリビュート値ペア 9-20 ダウンロード可能な ACL の Cisco Secure ACS およびアトリビュート値ペア 9-21 VLAN ID ベース MAC 認証 9-21 ゲスト VLAN を使用した 802.1x 認証 9-22 制限付き VLAN を使用した 802.1x 認証 9-23 アクセス不能認証バイパスによる 802.1x 認証 9-24 複数認証ポートのサポート 9-24 認証結果 9-24 機能の相互作用 9-25 音声 VLAN ポートを使用した 802.1x 認証 9-25 ポート セキュリティを使用した 802.1x 認証 9-26 Wake-on-LAN を使用した 802.1x 認証 9-27 MAC 認証バイパスによる 802.1x 認証 9-28 802.1x ユーザ ディストリビューション 9-29 802.1x ユーザ ディストリビューションの設定時の注意事項 9-29 Network Admission Control レイヤ2802.1x 検証 9-29 柔軟な認証の順序設定 9-30 Open1x 認証 9-30 音声認識 802.1x セキュリティの使用 9-31 Network Edge Access Topology (NEAT) を使用した 802.1x サプリカントおよび認 証者 9-31 注意事項 9-32 ACL および RADIUS Filter-Id アトリビュートを使用した IEEE 802.1x 認証の使 用 9-33 802.1x 認証の設定 9-33 802.1x 認証のデフォルト設定 9-34 802.1x 認証設定時の注意事項 9-35 802.1x 認証 9-35 VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパ ス 9-36 MAC 認証バイパス 9-37 ポートあたりのデバイスの最大数 9-37 802.1x 準備状態チェックの設定 9-38 音声認識 802.1x セキュリティの設定 9-39 802.1x 違反モードの設定 9-40 802.1x 認証の設定 9-41 スイッチおよび RADIUS サーバ間の通信の設定 9-43

Contents

ホスト モードの設定 9-44 定期的な再認証の設定 9-45 ポートに接続するクライアントの手動での再認証 9-46 待機時間の変更 9-47 スイッチからクライアントへの再送信時間の変更 9-48 スイッチからクライアントへのフレーム再送信回数の設定 9-49 再認証回数の設定 9-50 MAC Move のイネーブル化 9-51 802.1x アカウンティングの設定 9-51 ゲスト VLAN の設定 9-52 制限付き VLAN の設定 9-53 アクセス不能認証バイパス機能の設定 9-55 WoL を使用した 802.1x 認証の設定 9-57 MAC 認証バイパスの設定 9-58 802.1x ユーザ ディストリビューションの設定 9-59 NAC レイヤ 2 802.1x 検証の設定 9-60 NEAT での認証者およびサプリカント スイッチの設定 9-61 ASP での NEAT の設定 9-62 ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定 9-63 ダウンロード可能な ACL の設定 9-63 ダウンロード ポリシーの設定 9-63 VLAN ID ベース MAC 認証の設定 9-65 柔軟な認証の順序設定 9-66 Open1x の設定 9-66 ポート上での 802.1x 認証のディセーブル化 9-67 802.1x 認証設定のデフォルト値へのリセット 9-68 802.1x の統計情報およびステータスの表示 9-68 Web ベース認証の設定 10-1

OL-8603-07-J

CHAPTER 10

ゲートウェイ IP 10-8 ACL 10-8 コンテキストベース アクセス コントロール 10-8 802.1x 認証 10-8 EtherChannel 10-8 Web ベース認証の設定 10-9 デフォルトの Web ベース認証の設定 10-9 Web ベース認証の設定に関する注意事項と制約事項 10-9 Web ベース認証の設定タスク リスト 10-10 認証ルールとインターフェイスの設定 10-10 AAA 認証の設定 10-11 スイッチから RADIUS サーバへの通信のコンフィギュレーション 10-12 HTTP サーバの設定 10-13 認証プロキシ Web ページのカスタマイズ 10-14 成功ログインに対するリダイレクション URL の指定 10-15 AAA 失敗ポリシーの設定 10-16 Web ベース認証パラメータの設定 10-16 Web 認証ローカル バナーの設定 10-17 Web ベース認証キャッシュ エントリの削除 10-17 Web ベース認証ステータスの表示 10-18

снартев 11 インターフェイス特性の設定 11-1

インターフェイス タイプの概要 11-1 ポートベースの VLAN 11-2 スイッチ ポート **11-2** アクセス ポート 11-3 トランク ポート 11-3 EtherChannel ポート グループ 11-4 デュアルパーパス アップリンク ポート 11-4 Power over Ethernet (PoE) # #11-5 サポート対象のプロトコルおよび規格 11-5 受電装置の検出および初期電力割り当て 11-6 電力管理モード 11-7 電力モニタリングおよび電力ポリシング 11-8 インターフェイスの接続 11-10 インターフェイス コンフィギュレーション モードの使用方法 11-11 インターフェイスの設定手順 11-11 インターフェイス範囲の設定 11-12 インターフェイス レンジ マクロの設定および使用方法 11-14

	VLAN の概要 13-2	
CHAPTER 13	VLAN の設定 13-1	
	Auto SmartPort マクロおよびスタティック SmartPort マクロの表示	12-21
	スタティック SmartPort マクロの適用 12-19	
	スタティック SmartPort 設定時の注意事項 12-18	
	スタティック SmartPort のデフォルト設定 12-18	
	スタティック SmartPort マクロの設定 12-18	
	Auto SmartPort ユーザ定義マクロの設定 12-16	
	Auto Sinditron 祖み込みマクロ オラジョブの設定 12-10 ユーザ定義のイベント トリガーの作成 12-13	
	Auto SmartPort マクロの水統性の設定 12-9	
	Auto SmartPort の MAC アドレス クループの設定 12-8	
	Auto SmartPort のデフォルト パラメータ値の設定 12-6	
	Auto SmartPort のイネーブル化 12-6	
	Auto SmartPort 設定時の注意事項 12-5	
	Auto SmartPort のデフォルト設定 12-4	
	Auto SmartPort の設定 12-3	
	Auto SmartPort および Cisco Medianet 12-3	
	Auto SmartPort マクロおよびスタティック SmartPort マクロの概要	12-2
CHAPTER 12	 Auto SmartPort マクロの設定 12-1	
	インターフェイスのシャットダウンおよび再起動 11-33	
	インターフェイスおよびカウンタのクリアとリセット 11-32	
	インターフェイス ステータスのモニタ 11-31	
	インターフェイスのモニタおよびメンテナンス 11-31	
	システム MTU の設定 11-30	
	インターフェイスに関する記述の追加 11-29	
	電カポリシングの設定 11-28	
	PoE ポートに接続された装置のパワー バジェット 11-26	
	PoE ポートの電力管理モードの設定 11-24	
	インターフェイスでの Auto-MDIX の設定 11-23	
	IEEE 802.3x フロー制御の設定 11-22	11 20
	座皮とりェッレックス ここれの設定時の左急事項 こう インターフェイス速度およびデュプレックス パラメータの設定	11-20
	す ファーフェイス 座皮 および フェフレ ファス こ 「FO 設定 II-15 速度とデュプレックス モードの設定時の注音車項 11-19	
) エアルハーハス アッフリンツ ホードのラインの設定 II-1/ インターフェイス連度なとびデュプレックス モードの設定 11-10	
	イーザネット インダーフェイスのテフォルト設定 11-16 デュアルパーパス アップリンク ポートのタイプの設定 11-17	
	イーサネットインダーフェイスの設定 11-16 イーサネットノンターフェイスのデフェルト語会 44.40	
	イーサネット インターフェイスの設定 11.16	

L

サポートされる VLAN 13-3 VLAN ポート メンバシップ モード 13-4 標準範囲 VLAN の設定 13-5 トークンリング VLAN 13-6 標準範囲 VLAN 設定時の注意事項 13-6 標準範囲 VLAN の設定 13-7 イーサネット VLAN のデフォルト設定 13-8 イーサネット VLAN の作成または変更 13-8 VLAN の削除 13-10 VLAN へのスタティック アクセス ポートの割り当て 13-10 拡張範囲 VLAN の設定 13-11 VLAN のデフォルト設定 13-12 拡張範囲 VLAN 設定時の注意事項 13-12 拡張範囲 VLAN の作成 13-12 VLAN の表示 13-14 VLAN トランクの設定 13-14 トランキングの概要 13-14 IEEE 802.1Qの設定に関する考慮事項 13-15 レイヤ2イーサネット インターフェイス VLAN のデフォルト設定 13-16 トランク ポートとしてのイーサネット インターフェイスの設定 13-16 他の機能との相互作用 13-16 トランク ポートの設定 13-17 トランクでの許可 VLAN の定義 13-18 プルーニング適格リストの変更 13-19 タグなしトラフィック用ネイティブ VLAN の設定 13-20 トランク ポートの負荷分散の設定 13-21 STP ポート プライオリティによる負荷分散 13-21 STP パス コストによる負荷分散 13-23 VMPS の設定 13-24 VMPS の概要 13-25 ダイナミックアクセス ポート VLAN メンバシップ 13-25 VMPS クライアントのデフォルト設定 13-26 VMPS 設定時の注意事項 13-26 VMPS クライアントの設定 13-27 VMPS の IP アドレスの入力 13-27 VMPS クライアント上のダイナミックアクセス ポートの設定 13-28 VLAN メンバシップの再確認 13-28 再確認インターバルの変更 13-29 再試行回数の変更 13-29

VMPS のモニタ 13-30 ダイナミックアクセス ポート VLAN メンバシップのトラブルシューティング 13-30 VMPS の設定例 13-31 CHAPTER 14 VTP の設定 14-1 VTP の概要 14-1 VTP ドメイン 14-2 VTP モード 14-3 VTP アドバタイズ 14-4 VTP バージョン 2 14-4 VTP バージョン3 14-5 14-6 VTP プルーニング VTP の設定 14-8 VTP のデフォルト設定 14-8 VTP 設定時の注意事項 14-8 ドメイン名 14-9 パスワード 14-9 VTP バージョン 14-10 設定要件 14-11 VTP モードの設定 14-11 VTP バージョン 3 のパスワードの設定 14-13 VTP バージョン 3 のプライマリ サーバの設定 14-14 VTP バージョンのイネーブル化 14-14 VTP プルーニングのイネーブル化 14-16 ポート単位の VTP の設定 14-16 VTP ドメインへの VTP クライアント スイッチの追加 14-17 VTP のモニタ 14-18

CHAPTER 15 音声 VLAN の設定

音声 VLAN の概要 15-1	
Cisco IP Phone の音声トラフィック 15-2	
Cisco IP Phone のデータ トラフィック 15-3	
音声 VLAN の設定 15-3	
音声 VLAN のデフォルト設定 15-3	
音声 VLAN 設定時の注意事項 15-4	
Cisco7960 IP Phone に接続するポートの設定	15-5
Cisco IP Phone の音声トラフィックの設定	15-6
着信データ フレームのプライオリティ設定	15-7
音声 VLAN の表示 15-8	

15-1

STP の設定 CHAPTER 16 16-1 スパニング ツリー機能の概要 16-2 STP の概要 16-2 スパニング ツリー トポロジと BPDU 16-3 ブリッジ ID、スイッチ プライオリティ、および拡張システム ID 16-4 スパニング ツリー インターフェイス ステート 16-5 ブロッキング ステート 16-7 リスニング ステート 16-7 ラーニング ステート 16-7 フォワーディング ステート 16-8 ディセーブル ステート 16-8 スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み 16-8 スパニング ツリーおよび冗長接続 16-9 スパニング ツリー アドレスの管理 16-10 接続を維持するためのエージング タイムの短縮 16-10 スパニング ツリー モードおよびプロトコル 16-10 サポートされるスパニング ツリー インスタンス 16-11 スパニング ツリーの相互運用性と下位互換性 16-12 STP および IEEE 802.1Q トランク 16-12 スパニング ツリー機能の設定 16-13 スパニング ツリー機能のデフォルト設定 16-13 スパニング ツリー設定時の注意事項 16-14 スパニング ツリー モードの変更 16-15 スパニング ツリーのディセーブル化 16-16 ルート スイッチの設定 16-16 セカンダリ ルート スイッチの設定 16-18 ポート プライオリティの設定 16-19 パス コストの設定 16-20 VLAN のスイッチ プライオリティの設定 16-21 スパニング ツリー タイマーの設定 16-22 Hello タイムの設定 16-22 VLAN の転送遅延時間の設定 16-23 VLAN の最大エージング タイムの設定 16-23 転送保留カウントの設定 16-24 スパニング ツリー ステータスの表示 16-25

снартев 17 MSTP の設定 17-1

MSTPの概要 17-2 MST リージョン 17-2

```
IST、CIST、および CST 17-2
    MST リージョン内の動作
                       17-3
    MST リージョン間の動作
                       17-4
    IEEE 802.1s の用語
                   17-5
  ホップ カウント 17-6
  境界ポート 17-6
  IEEE 802.1s の実装
               17-7
    ポートの役割名の変更
                   17-7
    レガシー スイッチと標準スイッチの相互運用
                                  17-7
    単一方向リンクの失敗の検出
                         17-8
  IEEE 802.1D STP との相互運用性
                          17-9
RSTP の概要
           17-9
  ポートの役割およびアクティブ トポロジ
                             17-9
  高速コンバージェンス
                  17-10
  ポートの役割の同期化
                  17-12
  BPDU のフォーマットおよびプロセス
                            17-13
    優位 BPDU 情報の処理
                     17-13
    下位 BPDU 情報の処理
                     17-14
  トポロジの変更
             17-14
MSTP 機能の設定
              17-15
  MSTP のデフォルト設定
                    17-15
  MSTP 設定時の注意事項
                    17-16
  MST リージョンの設定および MSTP のイネーブル化
                                     17-16
  ルート スイッチの設定
                 17-18
  セカンダリ ルート スイッチの設定
                          17-20
  ポート プライオリティの設定
                      17-21
  パス コストの設定
               17-22
  スイッチ プライオリティの設定
                        17-23
  Hello タイムの設定
               17-24
  転送遅延時間の設定
                 17-24
  最大エージング タイムの設定
                       17-25
  最大ホップ カウントの設定
                     17-25
  リンク タイプの指定による高速移行の保証
                              17-26
  ネイバ タイプの指定
                17-27
  プロトコル移行プロセスの再起動
                       17-27
MST コンフィギュレーションおよびステータスの表示
                                   17-28
```

______ CHAPTER 18 オプションのスパニング ツリー機能の設定 18-1

オプションのスパニング ツリー機能の概要 18-1

PortFast の概要 18-2 BPDU ガードの概要 18-3 BPDU フィルタリングの概要 18-3 UplinkFast の概要 18-4 BackboneFast の概要 18-6 EtherChannel ガードの概要 18-8 ルート ガードの概要 18-8 ループ ガードの概要 18-10 オプションのスパニング ツリー機能の設定 18-10 オプションのスパニング ツリー機能のデフォルト設定 18-11 オプションのスパニング ツリー設定時の注意事項 18-11 PortFast のイネーブル化 18-11 BPDU ガードのイネーブル化 18-12 BPDU フィルタリングのイネーブル化 18-14 冗長リンク用 UplinkFast のイネーブル化 18-15 BackboneFast のイネーブル化 18-16 EtherChannel ガードのイネーブル化 18-16 ルート ガードのイネーブル化 18-17 ループ ガードのイネーブル化 18-18 スパニング ツリー ステータスの表示 18-19 Flex Link および MAC アドレス テーブル移動更新機能の設定 19-1 Flex Link および MAC アドレス テーブル移動更新機能の概要 19-1 Flex Link 19-2 VLAN Flex Link ロード バランシングおよびサポート 19-3

Flex Link マルチキャスト高速コンバージェンス 19-3 その他の Flex Link ポートを mrouter ポートとして学習 19-4 IGMP レポートの生成 19-4 IGMP レポートのリーク 19-4 設定例 19-5 MAC アドレス テーブル移動更新 19-7 Flex Link および MAC アドレス テーブル移動更新機能の設定 19-8 デフォルト設定 19-9 設定時の注意事項 19-9 Flex Link の設定 19-10 Flex Link の VLAN ロード バランシングの設定 19-12 MAC アドレス テーブル移動更新機能の設定 19-14

Flex Link および MAC アドレス テーブル移動更新のモニタ 19-16

CHAPTER 19

CHAPTER 20	 DHCP 機能 および IP ソース ガード機能の設定 20-1	
	DHCP スヌーピングの概要 20-2	
	DHCP サーバ 20-2	
	DHCP リレー エージェント 20-2	
	DHCP スヌーピング 20-3	
	Option 82 データ挿入 20-4	
	DHCP スヌーピング バインディング データベース 20-7	
	DHCP スヌーピングの設定 20-8	
	DHCP スヌーピングのデフォルト設定 20-9	
	DHCP スヌーピング設定時の注意事項 20-9	
	DHCP リレー エージェントの設定 20-11	
	DHCP スヌーピングおよび Option 82 のイネーブル化 20-11	
	Cisco IOS DHCP サーバ データベースのイネーブル化 20-13	
	DHCP スヌーピング バインディング データベース エージェントのイネーブル化	20-13
	DHCP スヌーピング情報の表示 20-15	
	IP ソース ガードの概要 20-15	
	送信元 IP アドレスのフィルタリング 20-16	
	送信元 IP アドレスおよび MAC アドレスのフィルタリング 20-16	
	スタティック ホスト用 IP ソース ガード 20-17	
	IP ソース ガードの設定 20-18	
	デフォルトの IP ソース ガード設定 20-18	
	IP ソース ガード設定時の注意事項 20-18	
	IP ソース ガードのイネーブル化 20-19	
	スタティック ホスト用 IP ソース ガードの設定 20-20	
	レイヤ2アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定	20-20
	IP ソース ガード情報の表示 20-24	
	DHCP サーバ ポートベースのアドレス割り当ての概要 20-24	
	DHCP サーバ ポートベースのアドレス割り当ての設定 20-25	
	ポートベースのアドレス テーブルのデフォルト設定 20-25	
	ポートベースのアドレス割り当て設定時の注意事項 20-25	
	DHCP サーバ ポートベースのアドレス割り当てのイネーブル化 20-25	
	DHCP サーバ ポートベースのアドレス割り当ての表示 20-28	
CHAPTER 21	 ダイナミック ARP インスペクションの設定 21-1	
	ダイナミック ARP インスペクションの概要 21-2	
	インターフェイスの信頼状態とネットワーク セキュリティ 21-3	
	ARP パケットのレート制限 21-5	
	ARP ACL および DHCP スヌーピング エントリの相対的な優先順位 21-5	

L

廃棄されたパケットのロギング 21-5 ダイナミック ARP インスペクションの設定 21-6 ダイナミック ARP インスペクションのデフォルト設定 21-6 ダイナミック ARP インスペクション設定時の注意事項 21-7 DHCP 環境でのダイナミック ARP インスペクションの設定 21-8 非 DHCP 環境での ARP ACL の設定 21-10 着信 ARP パケットのレート制限 21-12 確認検査の実行 21-14 ログ バッファの設定 21-15 ダイナミック ARP インスペクション情報の表示 21-17 CHAPTER 22 IGMP スヌーピングおよび MVR の設定 22-1 IGMP スヌーピングの概要 22-2 IGMP バージョン 22-3 マルチキャスト グループへの加入 22-3 マルチキャスト グループからの脱退 22-5 即時脱退 22-6 IGMP 脱退タイマーの設定 22-6 IGMP レポート抑制 22-6 IGMP スヌーピングの設定 22-7 IGMP スヌーピングのデフォルト設定 22-7 IGMP スヌーピングのイネーブル化およびディセーブル化 22-8 スヌーピング方法の設定 22-9 マルチキャスト ルータ ポートの設定 22-10 グループに加入するホストの静的な設定 22-11 IGMP 即時脱退のイネーブル化 22-11 IGMP 脱退タイマーの設定 22-12 TCN 関連のコマンドの設定 22-13 TCN イベント後のマルチキャスト フラッディング時間の制御 22-13 フラッディング モードからの回復 22-14 TCN イベント中のマルチキャスト フラッディングのディセーブル化 22-14 IGMP スヌーピング クエリアの設定 22-15 IGMP レポート抑制のディセーブル化 22-17 IGMP スヌーピング情報の表示 22-18 MVR の概要 22-19 マルチキャスト TV アプリケーションで MVR を使用する場合 22-20 MVR の設定 22-22 MVR のデフォルト設定 22-22 MVR 設定時の注意事項および制限事項 22-23

	MVR 情報の表示 22-26	
	IGMP フィルタリングおよびスロットリングの設定 22-27	
	IGMP フィルタリンクおよび IGMP スロットリングのテフォルト設定	22-28
	IGMP ブロファイルの設定 22-28	
	IGMP ブロファイルの適用 22-29	
	IGMP クルーフの最大数の設定 22-30	
	IGMP スロットリング アグジョンの設定 22-31	
	IGMP フィルタリングおよび IGMP スロットリング設定の表示 22-32	
CHAPTER 23	 ポート単位のトラフィック制御の設定 23-1	
	ストーム制御の設定 23-1	
	ストーム制御の概要 23-1	
	ストーム制御のデフォルト設定 23-3	
	ストーム制御およびしきい値レベルの設定 23-3	
	小さいフレームの着信レートの設定 23-6	
	保護ポートの設定 23-7	
	保護ポートのデフォルト設定 23-7	
	保護ポート設定時の注意事項 23-7	
	保護ポートの設定 23-7	
	ポート ブロッキングの設定 23-8	
	ポート ブロッキングのデフォルト設定 23-8	
	インターフェイスでのフラッディング トラフィックのブロッキング	23-8
	ポート セキュリティの設定 23-9	
	ポート セキュリティの概要 23-10	
	セキュア MAC アドレス 23-10	
	セキュリティ違反 23-11	
	ポート セキュリティのデフォルト設定 23-12	
	ポート セキュリティの設定時の注意事項 23-12	
	ポート セキュリティのイネーブル化および設定 23-13	
	ポート セキュリティ エージングのイネーブル化および設定 23-18	
	ポート単位のトラフィック制御設定の表示 23-20	
24		

CHAPTER 24 UDLD の設定 24-1 UDLD の概要 24-1 動作モード 24-2 単一方向の検出方法 24-3

I

UDLD の設定 24-4
UDLD のデフォルト設定 24-4
設定時の注意事項 24-5
UDLD のグローバルなイネーブル化 24-5
インターフェイス上での UDLD のイネーブル化 24-6
UDLD によってディセーブル化されたインターフェイスのリセット 24-7
UDLD ステータスの表示 24-7

CHAPTER 25	 CDPの設定 25-1
	CDP の概要 25-1
	CDPの設定 25-2
	CDP のデフォルト設定 25-2
	CDP の特性の設定 25-2
	CDP のディセーブル化およびイネーブル化 25-3
	インターフェイス上での CDP のディセーブル化およびイネーブル化 25-4
	CDP のモニタおよびメンテナンス 25-5
CHAPTER 26	 LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 26-1
	LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要 26-2
	LLDP 26-2
	LLDP-MED 26-3
	ワイヤード ロケーション サービス 26-4
	LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 26-5
	デフォルト LLDP 設定 26-6
	設定時の注意事項 26-6
	LLDP のイネーブル化 26-7
	LLDP 特性の設定 26-8
	LLDP-MED TLV の設定 26-9
	Network-Policy TLV の設定 26-9
	ロケーション TLV およびワイヤード ロケーション サービスの設定 26-11
	LLDP、LLDP-MED、およびワイヤード ロケーション サービスのモニタリングおよびメン テナンス 26-13
27	
CHAPTER Z/	

SPAN および RSPAN の概要 27-1 ローカル SPAN 27-2 リモート SPAN 27-3 SPAN と RSPAN の概念および用語 27-4 SPAN セッション 27-4

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

モニタ対象トラフィック 27-5 送信元ポート 27-6 送信元 VLAN 27-6 VLAN フィルタリング 27-7 宛先ポート 27-7 RSPAN VLAN 27-8 SPAN および RSPAN と他の機能の相互作用 27-9 SPAN および RSPAN の設定 27-10 SPAN および RSPAN のデフォルト設定 27-10 ローカル SPAN の設定 27-10 SPAN 設定時の注意事項 27-10 ローカル SPAN セッションの作成 27-11 ローカル SPAN セッションの作成および着信トラフィックの設定 27-14 フィルタリングする VLAN の指定 27-16 RSPAN の設定 27-17 RSPAN 設定時の注意事項 27-17 RSPAN VLAN としての VLAN の設定 27-18 RSPAN 送信元セッションの作成 27-19 RSPAN 宛先セッションの作成 27-20 RSPAN 宛先セッションの作成および着信トラフィックの設定 27-21 フィルタリングする VLAN の指定 27-23 SPAN および RSPAN のステータス表示 27-24

CHAPTER 28	 RMON の設定 28-1	
	RMON の概要 28-1	
	RMON の設定 28-3	
	RMON のデフォルト設定 28-3	
	RMON アラームおよびイベントの設定 28-3	
	インターフェイス上でのグループ履歴統計情報の収集 28-5	
	インターフェイス上でのイーサネット グループ統計情報の収集 28-0	3
	RMON ステータスの表示 28-7	
CHAPTER 29	 システム メッセージ ロギングの設定 29-1	
	システム メッセージ ロギングの概要 29-2	
	システム メッセージ ロギングの設定 29-2	
	システム ログ メッセージのフォーマット 29-3	
	システム メッセージ ロギングのデフォルト設定 29-4	
	メッセージ ロギングのディセーブル化 29-4	
	メッセージ表示宛先デバイスの設定 29-5	

ログ メッセージの同期化 29-6 ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 29-8 ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 29-8 メッセージ重大度の定義 29-9 履歴テーブルおよび SNMP に送信される Syslog メッセージの制限 29-11 設定変更ロガーのイネーブル化 29-11 UNIX Syslog サーバの設定 29-13 UNIX Syslog デーモンへのログ メッセージ 29-13 UNIX システム ロギング ファシリティの設定 29-14 ロギング設定の表示 29-15

CHAPTER 30 SNMP の設定 30-1

SNMP の概要 30-1 SNMP バージョン 30-2 SNMP マネージャ機能 30-3 SNMP エージェント機能 30-4 SNMP コミュニティ ストリング 30-4 SNMP を使用して MIB 変数にアクセスする方法 30-5 SNMP 通知 30-5 SNMP ifIndex MIB オブジェクト値 30-6 SNMP の設定 30-6 SNMP のデフォルト設定 30-7 SNMP 設定時の注意事項 30-7 SNMP エージェントのディセーブル化 30-8 コミュニティ ストリングの設定 30-9 SNMP グループおよびユーザの設定 30-10 SNMP 通知の設定 30-13 CPU しきい値通知のタイプと値の設定 30-17 エージェント コンタクトおよびロケーションの設定 30-17 SNMP を通して使用する TFTP サーバの制限 30-18 SNMP の例 30-19 SNMP ステータスの表示 30-20

CHAPTER **31**

ACL によるネットワーク セキュリティの設定 31-21 ACL の概要 31-22 ポート ACL 31-23 フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処 理 31-24 IPv4 ACL の設定 31-25

	標準 IPv4 ACL および拡張 IPv4 ACL の作成 31-26
	アクセス リスト番号 31-26
	番号付き標準 ACL の作成 31-27
	番号付き拡張 ACL の作成 31-29
	ACL 内の ACE の並べ替え 31-33
	名前付き標準 ACL および名前付き拡張 ACL の作成 31-33
	ACL での時間範囲の使用 31-35
	ACL へのコメントの挿入 31-37
	端末回線への IPv4 ACL の適用 31-37
	インターフェイスへの IPv4 ACL の適用 31-38
	ハードウェアおよびソフトウェアによる IP ACL の処理 31-39
	ACL のトラブルシューティング 31-40
	IPv4 ACL の設定例 31-41
	番号付き ACL 31-41
	拡張 ACL 31-41
	名前付き ACL 31-42
	IP ACL に適用される時間範囲 31-42
	コメント付きの IP ACL エントリ 31-42
	名前付き MAC 拡張 ACL の作成 31-43
	レイヤ 2 インターフェイスへの MAC ACL の適用 31-45
	IPv4 ACL の設定の表示 31-46
CHAPTER 32	Cisco IOS IP SLA 動作の設定 32-1
	Cisco IOS IP SLA の概要 32-2
	Cisco IOS IP SLA によるネットワーク パフォーマンスの測定 32-3
	IP SLA Responder と IP SLA コントロール プロトコル 32-4
	IP SLA の応答時間の計算 32-4
	IP SLA 動作の設定 32-5
	デフォルト設定 32-5
	設定時の注意事項 32-5
	IP SLA Responder の設定 32-6
	IP SLA 動作のモニタリング 32-7
CHAPTER 33	QOS の設定 33-1
	QoSの概要 33-2
	QoS の基本モデル 33-4
	分類 33-5

_現 33-5 QoSACLに基づく分類 33-8 クラス マップおよびポリシー マップに基づく分類 33-8

I

ポリシングおよびマーキング 33-9 物理ポートのポリシング 33-10 マッピング テーブル 33-12 キューイングおよびスケジューリングの概要 33-13 WTD 33-13 SRR のシェーピングおよび共有 33-14 入力キューでのキューイングおよびスケジューリング 33-15 出力キューでのキューイングおよびスケジューリング 33-17 パケットの変更 33-20 自動 QoS の設定 33-20 生成される自動 QoS 設定 33-21 コンフィギュレーションにおける自動 QoS の影響 33-26 自動 QoS 設定時の注意事項 33-26 VoIP 用自動 QoS のイネーブル化 33-27 自動 QoS 設定例 33-28 自動 QoS 情報の表示 33-30 標準 QoS の設定 33-30 標準 QoS のデフォルト設定 33-31 入力キューのデフォルト設定 33-31 出力キューのデフォルト設定 33-32 マッピング テーブルのデフォルト設定 33-33 標準 QoS 設定時の注意事項 33-33 QoS ACL の注意事項 33-33 ポリシングの注意事項 33-34 一般的な QoS の注意事項 33-34 QoS のグローバルなイネーブル化 33-35 ポートの信頼状態による分類の設定 33-35 QoS ドメイン内のポートの信頼状態の設定 33-35 インターフェイスの CoS 値の設定 33-38 ポート セキュリティを確保するための信頼境界機能の設定 33-39 DSCP 透過モードのイネーブル化 33-40 別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定 33-41 QoS ポリシーの設定 33-43 ACL によるトラフィックの分類 33-43 クラス マップによるトラフィックの分類 33-47 ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマー キング 33-49 集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング 33-54 DSCP マップの設定 33-56 CoS/DSCP マップの設定 33-56

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

IP precedence/DSCP マップの設定 33-57 ポリシング済み DSCP マップの設定 33-58 DSCP/CoS マップの設定 33-59 **DSCP/DSCP 変換マップの設定** 33-60 入力キューの特性の設定 33-62 入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設 定 33-62 入力キュー間のバッファ スペースの割り当て 33-64 入力キュー間の帯域幅の割り当て 33-65 入力プライオリティ キューの設定 33-66 出力キューの特性の設定 33-67 設定時の注意事項 33-67 出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設 定 33-68 出力キューおよび ID への DSCP または CoS 値のマッピング 33-70 出力キューでの SRR シェーピング重みの設定 33-71 出力キューでの SRR 共有重みの設定 33-72 出力緊急キューの設定 33-73 出力インターフェイスの帯域幅の制限 33-74 標準 QoS 情報の表示 33-75

CHAPTER 34

IPv6 ホスト機能の設定 34-1

IPv6の概要 34-2	
IPv6 アドレス 34-2	
サポート対象の IPv6 ホスト機能 34-3	
128 ビット幅のユニキャスト アドレス 34-3	
IPv6 用 DNS 34-4	
ICMPv6 34-4	
近接ディスカバリ 34-4	
IPv6 のステートレス自動設定および重複アドレス検出	34-4
IPv6 アプリケーション 34-4	
デュアル IPv4/IPv6 プロトコル スタック 34-5	
IPv6 のスタティック ルート 34-6	
IPv6 による SNMP および Syslog 34-6	
IPv6 による HTTP(S) 34-7	
IPv6 の設定 34-7	
IPv6 のデフォルト設定 34-7	
IPv6 アドレス指定の設定および IPv6 ホストのイネーブル化	34-8
IPv6 ICMP レート制限の設定 34-10	
IPv6 のスタティック ルートの設定 34-11	

IPv6 の表示 34-13 CHAPTER 35 IPv6 MLD スヌーピングの設定 35-1 MLD スヌーピングの概要 35-2 MLD メッセージ 35-3 MLD クエリー 35-3 マルチキャスト クライアント エージングの堅牢性 35-4 マルチキャスト ルータ検出 35-4 MLD レポート 35-4 MLD Done メッセージおよび即時脱退 35-5 TCN 処理 35-5 IPv6 MLD スヌーピングの設定 35-5 MLD スヌーピングのデフォルト設定 35-6 MLD スヌーピング設定時の注意事項 35-6 MLD スヌーピングのイネーブル化またはディセーブル化 35-7 スタティックなマルチキャスト グループの設定 35-8 マルチキャスト ルータ ポートの設定 35-9 MLD 即時脱退のイネーブル化 35-10 MLD スヌーピング クエリーの設定 35-10 MLD リスナー メッセージ抑制のディセーブル化 35-12 MLD スヌーピング情報の表示 35-13 EtherChannel およびリンクステート トラッキングの設定 CHAPTER 36 36-1 EtherChannel の概要 36-1 EtherChannel の概要 36-2 ポートチャネル インターフェイス 36-3 ポート集約プロトコル 36-4 PAgP モード 36-4 PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出 36-5 PAgP と他の機能との相互作用 36-5 LACP 36-6 LACPモード 36-6 LACP と他の機能との相互作用 36-6 EtherChannel \mathcal{O} On $\mathbf{t} - \mathbf{k}$ 36-7 ロードバランシングおよび転送方式 36-7 EtherChannel の設定 36-9 EtherChannel のデフォルト設定 36-9 EtherChannel 設定時の注意事項 36-10 レイヤ 2 EtherChannel の設定 36-11

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

EtherChannel ロードバランシングの設定 36-13	
PAgP 学習方式およびプライオリティの設定 36-1	14
LACP ホット スタンバイ ポートの設定 36-16	
LACP システム プライオリティの設定 36-16	
LACP ポート プライオリティの設定 36-17	
EtherChannel、PAgP、および LACP ステータスの表示	36-18
リンクステート トラッキングの概要 36-18	
リンクステート トラッキングの設定 36-22	
デフォルトのリンクステート トラッキングの設定	36-22
リンクステート トラッキングの設定時の注意事項	36-22
リンクステート トラッキングの設定 36-22	
リンクステート トラッキング ステータスの表示	36-23

снартев 37 トラブルシューティング 37-1

ソフトウェアで障害が発生した場合の回復 37-2 パスワードを忘れた場合の回復 37-4 パスワード回復がイネーブルになっている場合の手順 37-5 パスワード回復がディセーブルになっている場合の手順 37-7 コマンド スイッチで障害が発生した場合の回復 37-8 故障したコマンド スイッチをクラスタ メンバーと交換する場合 37-9 故障したコマンドスイッチを他のスイッチと交換する場合 37-11 クラスタ メンバー スイッチとの接続の回復 37-12 自動ネゴシエーションの不一致の防止 37-13 PoE スイッチ ポートのトラブルシューティング 37-13 電力消失によるポートの障害 37-13 不正リンク アップによるポート障害 37-14 SFP モジュールのセキュリティと識別 37-14 SFP モジュール ステータスのモニタリング 37-14 ping の使用 37-15 ping の概要 37-15 ping の実行 37-15 レイヤ 2 traceroute の使用 37-16 レイヤ 2 traceroute の概要 37-16 使用上のガイドライン 37-17 物理パスの表示 37-18 IP traceroute の使用 37-18 IP traceroute の概要 37-18

37-19

IP traceroute の実行

TDR の使用 37-20 TDR の概要 37-20 TDR の実行および結果の表示 37-20 debug コマンドの使用 37-21 特定機能に関するデバッグのイネーブル化 37-21 システム全体診断のイネーブル化 37-22 デバッグおよびエラー メッセージ出力のリダイレクト 37-22 show platform forward コマンドの使用 37-23 crashinfo ファイルの使用 37-24 基本 crashinfo ファイル 37-25 拡張 crashinfo ファイル 37-25 トラブルシューティング表 37-25 CPU 使用率に関するトラブルシューティング 37-25 CPU 使用率が高い場合に起こりうる症状 37-26 問題と原因の検証 37-26 Power over Ethernet (PoE) のトラブルシューティング 37-27 サポート対象 MIB APPENDIX A A-1 MIB の一覧 A-1 FTP による MIB ファイルへのアクセス A-3 Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメー APPENDIX **B** ジの操作 **R-1** フラッシュ ファイル システムの操作 B-2 使用可能なファイル システムの表示 B-2 デフォルト ファイル システムの設定 B-3 ファイル システムのファイルに関する情報の表示 R-4 ディレクトリの変更および作業ディレクトリの表示 B-4 ディレクトリの作成および削除 B-5 ファイルのコピー B-6 ファイルの削除 B-7 tar ファイルの作成、表示、および抽出 B-7 tar ファイルの作成 **R-8** tar ファイルの内容の表示 **B-8** tar ファイルの抽出 B-9 ファイルの内容の表示 B-10 コンフィギュレーション ファイルの操作 B-10 コンフィギュレーション ファイルの作成および使用上の注意事項 B-11 コンフィギュレーション ファイルのタイプおよび場所 **B-11**

テキスト エディタによるコンフィギュレーション ファイルの作成 B-12 TFTP によるコンフィギュレーション ファイルのコピー **B-12** TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロード の準備 **R-12** TFTP によるコンフィギュレーション ファイルのダウンロード **B-13** TFTP によるコンフィギュレーション ファイルのアップロード B-14 FTP によるコンフィギュレーション ファイルのコピー B-15 FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの 準備 B-16 FTP によるコンフィギュレーション ファイルのダウンロード B-16 FTP によるコンフィギュレーション ファイルのアップロード B-18 RCP によるコンフィギュレーション ファイルのコピー B-19 RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの 準備 B-20 RCP によるコンフィギュレーション ファイルのダウンロード B-21 RCP によるコンフィギュレーション ファイルのアップロード B-22 設定情報の消去 B-23 スタートアップ コンフィギュレーション ファイルの消去 B-23 格納されたコンフィギュレーション ファイルの削除 B-23 コンフィギュレーションの交換またはロール バック B-23 コンフィギュレーション交換およびロールバックの概要 B-23 設定時の注意事項 B-25 コンフィギュレーション アーカイブの設定 B-26 コンフィギュレーション交換またはロールバック動作の実行 B-27 ソフトウェア イメージの操作 B-28 スイッチ上のイメージの場所 B-29 サーバまたは Cisco.com 上のイメージの tar ファイル形式 B-29 TFTP によるイメージ ファイルのコピー B-30 TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-31 TFTP によるイメージ ファイルのダウンロード **B-31** TFTP によるイメージ ファイルのアップロード B-33 FTP によるイメージ ファイルのコピー B-34 FTP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-34 FTP によるイメージ ファイルのダウンロード B-35 FTP によるイメージ ファイルのアップロード B-37 RCP によるイメージ ファイルのコピー B-38 RCP によるイメージ ファイルのダウンロードまたはアップロードの準備 B-39 RCP によるイメージ ファイルのダウンロード B-40 RCP によるイメージ ファイルのアップロード B-42

APPENDIX C	Catalyst 2950 スイッチから Catalyst 2960 スイッチへのアップグレードの推奨 C-1		
	設定の互換性の問題 C-1		
	機能的な動作の非互換項目 C-6		
APPENDIX D	 Cisco IOS Release 12.2(52)SE でサポートされていないコマンド D-1		
	アクセス コントロール リスト D-2		
	サポートされていない特権 EXEC コマンド D-2		
	サポートされていないグローバル コンフィギュレーション コマンド D-2		
	サポートされていないルートマップ コンフィギュレーション コマンド D-2		
	ブート ローダ コマンド D-2		
	サポートされていないグローバル コンフィギュレーション コマンド D-2		
	debug コマンド D-3		
	サポートされていない特権 EXEC コマンド D-3		
	IGMP スヌーピング コマンド D-3		
	サポートされていないグローバル コンフィギュレーション コマンド D-3		
	インターフェイス コマンド D-3		
	サポートされていない特権 EXEC コマンド D-3		
	サポートされていないグローバル コンフィギュレーション コマンド D-3		
	サポートされていないインターフェイス コンフィギュレーション コマンド	D-3	
	MAC アドレス コマンド D-4		
	サポートされていない特権 EXEC コマンド D-4		
	サポートされていないグローバル コンフィギュレーション コマンド D-4		
	その他 D-4		
	サポートされていないユーザ EXEC コマンド D-4		
	サホートされていない特権 EXEC コマンド D-4		
	サホートされていない特権 EXEC コマント D-5		
		ט-ט ס ב	
		J-0	
	ッ小一 とられにいない ひとろ 唱方化コイント ロウ		

I

スパニングツリー D-7 サポートされていないグローバル コンフィギュレーション コマンド D-7 サポートされていないインターフェイス コンフィギュレーション コマンド D-7 VLAN D-7 サポートされていないグローバル コンフィギュレーション コマンド D-7 サポートされていない vlan-config コマンド D-7 サポートされていないユーザ EXEC コマンド D-7 サポートされていない vlan-config コマンド D-7 サポートされていない VLAN データベース コマンド D-7 VTP D-8

サポートされていない特権 EXEC コマンド D-8

INDEX

Contents

I



はじめに

対象読者

このマニュアルでは、Catalyst 2960 スイッチ(以降、スイッチと記載)を管理するネットワーキング の専門家を対象としています。Cisco IOS ソフトウェアの使用経験があり、イーサネットおよび LAN の概念や専門用語を十分理解していることが前提です。

目的

このマニュアルでは、スイッチ上で Cisco IOS ソフトウェア機能を設定するために必要な情報について 説明します。Catalyst 2960 ソフトウェアは、Access Control List (ACL; アクセス コントロール リス ト)および Quality of Service (QoS) 機能のような企業クラスのインテリジェントなサービスを提供 します。

このマニュアルでは、スイッチで使用するために作成または変更されたコマンドの使用手順を扱ってい ます。これらのコマンドの詳細は扱いません。これらのコマンドの詳細については、このリリースに対 応する『*Catalyst 2960 Switch Command Reference*』を参照してください。Cisco IOS Release 12.2 の 標準コマンドについては、Cisco.com のホームページ (**Documentation > Cisco IOS Software**) にア クセスし、Cisco IOS のマニュアル セットを参照してください。

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

このマニュアルでは、表示されるシステム メッセージまたはスイッチの設置方法については説明しま せん。詳細については、このリリースの『Catalyst 2960 Switch System Message Guide』および 『Catalyst 2960 Switch Hardware Installation Guide』を参照してください。

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

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。 コマンドの説明では、次の表記法を使用しています。

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

対話形式の例では、次の表記法を使用しています。

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

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

(注)

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



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

関連資料

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

http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html



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

- 初期設定の情報については、『Getting Started Guide』の「Using Express Setup」の章、または 『Hardware Installation Guide』にある付録の「Configuring the Switch with the CLI-Based Setup Program」を参照してください。
- デバイスマネージャの要件については、リリースノート(発注はできませんが、Cisco.comから入手できます)の「System Requirements」を参照してください。
- Network Assistant の要件については、『*Getting Started with Cisco Network Assistant*』を参照して ください(発注はできませんが、Cisco.com から入手できます)。
- クラスタの要件については、『Release Notes for Cisco Network Assistant』を参照してください(発 注はできませんが、Cisco.com から入手できます)。
- アップグレード情報を入手するには、リリースノートの「Downloading Software」を参照してください。

スイッチに関するその他の情報については、以下の資料を参照してください。

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

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

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

マニュアルの入手方法およびテクニカル サポート

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

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

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

CHAPTER

概要

この章では、Catalyst 2960 スイッチ ソフトウェアについて説明します。内容は次のとおりです。

- 「機能」(P.1-1)
- 「スイッチ初期設定後のデフォルト値」(P.1-16)
- 「ネットワークの構成例」(P.1-19)
- 「次の作業」(P.1-24)

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

機能

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

- 「使用および導入を簡素化する機能」(P.1-2)
- 「パフォーマンス向上機能」(P.1-3)
- •「管理オプション」(P.1-5)
- 「管理の簡易性に関する機能」(P.1-5)
- 「アベイラビリティおよび冗長性に関する機能」(P.1-8)
- 「VLAN 機能」(P.1-9)
- 「セキュリティ機能」(P.1-10)
- 「QoS および CoS 機能」(P.1-13)
- 「Power over Ethernet の機能」(P.1-15)
- 「モニタ機能」(P.1-15)

使用および導入を簡素化する機能

機能

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



(注) スイッチで、LAN Lite イメージが実行されている場合、ACL を設定することはできます が、インターフェイスまたは VLAN に結合することはできません。

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

(注)

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

(注)

Network Assistant は、必ず、cisco.com/go/cna からダウンロードしてください。

- スイッチのクラスタ化テクノロジーの機能概要
 - イーサネット、ファスト イーサネット、Fast EtherChannel、Small Form-Factor Pluggable (SFP;着脱可能小型フォーム ファクタ)モジュール、ギガビット イーサネット、Gigabit EtherChannel 接続を含めて、地理的な近接にも相互接続メディアにも関係なく、複数のクラ スタ対応スイッチの設定、モニタ、認証、およびソフトウェア アップグレードをまとめて実 行できます。クラスタ対応スイッチのリストについては、リリース ノートを参照してください。
 - ー 候補スイッチの自動検出と、最大16台のスイッチからなるクラスタの作成機能。1つのIPア ドレスを使用してクラスタを管理できます。
 - 拡張検出機能により、コマンドスイッチに直接接続されていないクラスタ候補を検出できます。
- ポートで検出されたデバイスタイプに基づいてポートを動的に設定するシスコのデフォルトおよびユーザ定義の Auto SmartPort マクロ。
- ネットワークの1か所(ディレクタ)からの管理を可能にする Smart Install。Smart Install を使用して、新しく配置されたスイッチのゼロタッチイメージとコンフィギュレーションのアップグレード、およびクライアントスイッチに対するイメージとコンフィギュレーションのダウンロードを提供することができます。詳細については、『Cisco Smart Install Configuration Guide』を参照してください。
- AutoSmartPort の強化。これは、マクロの永続性、LLDP ベースのトリガ、MAC アドレスおよび OUI ベースのトリガ、リモート マクロに対するサポート、および Cisco Digital Media Player (Cisco DMP) と Cisco IP Video Surveillance Camera (Cisco IPVSC) という 2 つの新しいデバイ スタイプに基づく事項設定に対するサポートを追加します。

パフォーマンス向上機能

Cisco EnergyWise は、Power over Ethernet (PoE) エンティティのエネルギー利用を管理します。
 詳細については、Cisco.comの『Cisco EnergyWise Version 2 Configuration Guide』を参照してください。



Cisco EnergyWise を使用するには、スイッチが LAN Base イメージを実行している必要が あります。

- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーション。
 帯域幅の利用を最適化します。
- 10/100 Mbps インターフェイス、10/100/1000 Mbps インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Auto MDIX 機能により、インターフェイスが必要なケーブル接続タイプ(ストレートまたはクロス)を自動的に検出し、接続を適切に設定します。
- ハードウェアでブリッジングされるフレームの場合は最大 9000 バイト、ソフトウェアでブリッジングされるフレームの場合は最大 2000 バイトのサポート。
- すべてのポートにおける IEEE 802.3x フロー制御 (スイッチは休止フレームを送信しません)。
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps(ギガ ビット EtherChannel) または 800 Mbps (Fast EtherChannel) 全二重の帯域幅を確保。
- Port Aggregation Protocol (PAgP) および Link Aggregation Control Protocol (LACP) により、 EtherChannel リンクを自動的に作成します。

- レイヤ2パケットをギガビット回線レートで転送。
- ポート単位でのストーム制御。ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止できます。
- レイヤ2の不明なユニキャスト、マルチキャスト、およびブリッジドブロードキャストトラフィック転送に対するポートブロッキング。
- Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピング。IGMP バージョン 1、2、および 3 に対応し、マルチメディアおよびマルチキャスト トラフィックを効率的に転送できます。
- 1つのマルチキャストルータクエリーにつき1つのIGMPレポートだけをマルチキャストデバイスへ送信するIGMPレポート抑制(IGMPv1またはIGMPv2クエリーだけをサポート)
- IGMP スヌーピング クエリー サポート。IGMP 一般クエリー メッセージを定期的に生成するよう スイッチを設定します。
- IPv6 ホストは 基本的な IPv6 管理をサポートします。
- マルチキャストリスナーディスカバリ(MLD)スヌーピングは、スイッチされたネットワークで IPv6マルチキャストデータをクライアントへ効率よく配信できます。

<u>》</u> (注)

機能

IPv6 機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

 Multicast VLAN Registration (MVR)。マルチキャスト VLAN 上でマルチキャスト ストリームを 継続的に送信し、なおかつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。



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

- IGMP フィルタリング。スイッチ ポート上のホストが所属できるマルチキャスト グループ セット を管理します。
- IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定する IGMP スロットリング。
- ネットワーク終了の待ち時間を設定できる IGMP の脱退タイマー。
- Switch Database Management (SDM) テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。
- ネットワークのパフォーマンスをモニタする Cisco IOS IP Service Level Agreement (SLA; サービスレベル契約)要求パケットをシステムが予測し、これに応答できるようにする Cisco IOS IP SLA responder のサポート。
- 小さいフレームの着信しきい値。これは、小さいフレーム(64 バイト以下)が指定された伝送速度(しきい値)でインターフェイスに到着したときに、ストーム制御を回避するためのもので、設定が可能です。
- Flex Link でエラーが発生した後で、マルチキャストトラフィックのコンバージェンス時間を短縮 するための Flex Link マルチキャスト高速コンバージェンス。



Flex Link マルチキャスト高速コンバージェンスを使用するには、スイッチが LAN Base イ メージを実行している必要があります。

- サーバグループに均等にアクセスおよび認証要求を分散できるようにするための RADIUS サーバ ロードバランシング。
- CPU 生成トラフィックの QoS マーキングのサポートと、出力ネットワーク ポートへの CPU 生成 トラフィックのキュー。

管理オプション

- 組み込みデバイスマネージャ:GUIのデバイスマネージャがソフトウェアイメージに組み込まれています。このデバイスマネージャは、単体のスイッチの設定、管理に使用します。デバイスマネージャの起動については、『Getting Started Guide』を参照してください。デバイスマネージャの詳細については、スイッチのオンラインヘルプを参照してください。
- Network Assistant: Network Assistant は、Cisco.com からダウンロードできるネットワーク管理 アプリケーションです。単一のスイッチ、スイッチ クラスタ、デバイスのコミュニティの管理に 使用します。Network Assistant の詳細については、Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。
- CLI: Cisco IOS ソフトウェアは、デスクトップ スイッチングおよびマルチレイヤ スイッチング機能をサポートします。CLI にアクセスするには、スイッチのコンソール ポートに管理ステーションを直接接続するか、リモート管理ステーションから Telnet を使用します。CLI の詳細については、第2章「CLI の使用方法」を参照してください。
- SNMP: CiscoWorks 2000 LAN Management Suite (LMS) および HP OpenView などの SNMP 管理アプリケーション。HP OpenView、SunNet Manager などのプラットフォームが稼動している SNMP 対応管理ステーションから管理できます。スイッチは豊富な MIB 拡張機能および 4 つの Remote Monitoring (RMON) グループをサポートします。SNMP の詳しい使用方法については、 第 30 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine (旧称 Cisco IOS CNS エージェント): コンフィギュレーション サービスは、ネットワーク デバイスおよびサービスの導入と管理を自動化します。スイッチごと に設定変更の内容を生成してスイッチに送信し、その設定変更を適用したあと、その結果を記録す ることで初期設定および設定の更新を自動化できます。

CNS の詳細については、第4章「Cisco IOS Configuration Engine の設定」を参照してください。

管理の簡易性に関する機能

- スイッチ管理、設定ストレージ、および配信を自動化するための CNS の組み込み型エージェント。
- Dynamic Host Configuration Protocol (DHCP) によるスイッチ情報(IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System [DNS; ドメイン ネーム システム]、TFTP サーバ 名)の自動設定。
- DHCP リレーによる DHCP クライアントからの UDP ブロードキャストの転送 (IP アドレス要求 を含む)。
- DHCP サーバによる IP アドレスおよびその他の DHCP オプションの IP ホストへの自動割り当て。
- 新しいイメージの指定された設定を多数のスイッチにダウンロードするために、DHCP ベースの 自動設定およびイメージをアップデート。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにした アドレス割り当て。
- IP アドレスおよび対応するホスト名からスイッチを特定することを目的とした、ユニキャスト要求の DNS サーバへの転送、および TFTP サーバからソフトウェア アップグレードを管理することを目的とした、ユニキャスト要求の TFTP サーバへの転送。

- Address Resolution Protocol (ARP)。IP アドレスおよび対応する MAC (メディア アクセス制御) アドレスによってスイッチを特定します。
- 特定の送信元 MAC アドレスおよび宛先 MAC アドレスを持ったパケットを廃棄するユニキャスト MAC アドレス フィルタリング。
- 設定可能な MAC アドレス スケーリング。これにより、VLAN で MAC アドレス学習をディセー ブルにし、MAC アドレス テーブルのサイズを制限することができます。
- Cisco Discovery Protocol (CDP) バージョン1および2。ネットワークトポロジを検出し、ネットワーク上のスイッチと他のシスコ製デバイスとのマッピングを行います。
- Link Layer Discovery Protocol (LLDP) および LLDP Media Endpoint Discovery (LLDP-MED) によるサードパーティ製 IP 電話との相互運用性の確保。
- スイッチからエンドポイントデバイスヘロケーション情報を提供する LLDP メディア拡張 (LLDP-MED) ロケーション TLV。



機能

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

- Network Time Protocol (NTP)。すべてのスイッチに外部ソースから同じタイムスタンプを提供します。
- Cisco IOS File System (IFS)。スイッチが使用するすべてのファイルシステムに対して単一イン ターフェイスを提供します。
- ビデオなどのマルチキャストアプリケーションを最適化するために、SSM PIM プロトコルのサポート。
- マルチキャストアプリケーションのための Source Specific Multicast (SSM) マッピングは、グ ループへのソースのマッピングを提供します。これにより、リスナーはマルチキャスト ソースに 動的に接続できるようになります。また、アプリケーションへの依存性も軽減されます。
- IPv6 トランスポートを利用し、IPv6 ピアと通信し、IPv6 ルートをアドバタイズするための Enhanced Interior Gateway Routing Protocol (EIGRPIP) v6 のサポート。
- HSRP、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute および ping などの IP サービス のサポート。これにより、これらの IP サービスに VRF を認識させ、複数のルーティング インス タンスで動作できるようにします。
- スイッチの設定変更を記録して表示させるコンフィギュレーションロギング。
- 一意のデバイス ID。show inventory ユーザ EXEC コマンドで製品の ID 情報が表示されます。
- Netscape Communicator または Microsoft Internet Explorer ブラウザ セッションでデバイス マネージャを使用した帯域内管理アクセス。
- 最大 16 の Telnet 接続を同時に使用できる帯域内管理アクセス。ネットワーク上で複数の CLI ベース セッションを実行できます。
- ネットワーク上の複数の CLI セッションに対する、最大 5 つの同時暗号化 Secure Shell (SSH; セ キュア シェル) 接続の確立によって帯域内管理アクセス。
- SNMPのバージョン1、バージョン2c、およびバージョン3のgetおよびset要求による帯域内管理アクセス。
- 帯域外管理アクセス。スイッチのコンソールポートに端末を直接接続するか、またはシリアル接続とモデム経由でリモート端末に接続します。
- Secure Copy Protocol (SCP) 機能。スイッチ設定またはスイッチ イメージ ファイルをセキュアな 認証方法でコピーします (ソフトウェアの暗号化バージョンが必要)。

機能

- 設定の交換およびロールバックは、スイッチ上で一意の保存された Cisco IOS コンフィギュレーション ファイルで稼動している設定を交換します。
- Cisco IOS サポートの HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバに要求を送信す ることができます。また、Cisco IOS の HTTP サーバは、IPv4 と IPv6 の両方の HTTP クライアン トから、HTTP 要求にサービスを提供することができます。
- Simple Network and Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)を IPv6 ト ランスポート経由で設定し、IPv6 ホストが SNMP クエリーを送信し、IPv6 を実行しているデバイ スから SNMP 通知を受信できるようにすることができます。
- ホストやモバイル IP アドレスの管理など、リンク、サブネット、およびサイト アドレス指定の変 更を管理するための IPv6 ステートレス自動設定。
- VLANのMACアドレス学習をディセーブルにします。
- スイッチ ポートに IP アドレスを前もって割り当てるための DHCP サーバ ポートをベースにした アドレス割り当て。
- ワイヤードロケーションサービスは、接続されたデバイスのロケーションおよび接続のトラッキング情報を Cisco Mobility Services Engine (MSE; モビリティサービスエンジン)に送信します。

- (注) ワイヤード ロケーションを使用するには、スイッチが LAN Base イメージを実行している必要 があります。
- CPU 使用率しきい値トラップは、CPU の使用率をモニタします。

(注)

CPU 使用率を使用するには、スイッチが LAN Base イメージを実行している必要があります。

 LLDP-MED ネットワーク ポリシー プロファイルの Type Length Value (TLV; タイプ、長さ、値)。 VLAN、Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP)、 およびタギング モードの値を指定して、音声、および音声信号のプロファイルを作成するために 使用されます。



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

- DHCPDISCOVER パケットのオプション 12 フィールドにホスト名の入力をサポート。これにより 提供される同一のコンフィギュレーション ファイルは、DHCP プロトコルを使用して送信されま す。
- Option 82 DHCP フィールドのサーキット ID サブオプションについて、固定文字列ベースの フォーマットの選択肢をサポートするために、DHCP スヌーピングを強化。
- 電源ポリシー TLV 要求に基づいて、スイッチに、Power Device (PD; 受電装置) への電源の供給 を許可することにより、LLPD-MED のサポートを強化。
- Power over Ethernet (PoE) デバイスやデーモンが実行されているエンド ポイントなど、 EnergyWise エンティティの電力消費を管理する Cisco EnergyWise。

アベイラビリティおよび冗長性に関する機能

- Unidirectional Link Detection (UDLD; 単一方向リンク検出)およびアグレッシブ UDLD。光ファ イバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向 リンクを検出し、ディセーブルにします。
- IEEE 802.1D Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) による冗長バック ボーン接続およびループフリー ネットワーク。STP には次の機能があります。
 - 最大 128 のスパニング ツリー インスタンスをサポート。



■ 機能

スイッチが LAN Lite イメージを実行中の場合は、最大 64 のスパニング ツリー インスタン スをサポートできます。

- Per-VLAN Spanning-Tree Plus (PVST+) による VLAN 間でのロードバランシング。
- Rapid PVST+による、VLAN間でのロードバランシングおよびスパニングツリーインスタンスの高速コンバージェンスの実現。
- UplinkFast および BackboneFast によって、スパニングツリートポロジーの変更後に高速コン バージェンスを実行し、ギガビット アップリンクなどの冗長アップリンク間のロードバラン シングを達成。
- IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) により、VLAN をスパニング ツリー イン スタンスに分類、またデータ トラフィックおよびロードバランシング用に複数の転送パスを確保 します。また、IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) に基づいた Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) により、ルートと指定ポートをただちにフォワーディング ス テートに変更することで、スパニング ツリーの高速コンバージェンスが実現されます。
- PVST+、Rapid-PVST+、および MSTP モードで使用できるスパニング ツリーのオプション機能は 次のとおりです。
 - PortFast。ポートをブロッキングステートからフォワーディングステートへただちに変更させることによって、転送遅延を防ぎます。
 - BPDU ガード。Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)を 受信する PortFast 対応ポートをシャットダウンします。
 - BPDU フィルタリング。PortFast 対応ポートで BPDU の送受信ができなくなります。
 - ルートガード。ネットワークコア外のスイッチがスパニングツリールートになることを防ぎます。
 - ループガード。代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。
- Flex Link レイヤ2インターフェイス。基本リンク冗長のSTPに代わるものとして、互いにバック アップします。

(注)

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

 リンクステートトラッキング。接続されたホストとサーバからのアップストリームトラフィック を伝送するポートの状態をミラーリングします。また、別のシスコ製イーサネットスイッチで動 作するリンクへサーバトラフィックをフェールオーバーすることができます。



E) リンクステート トラッキングを使用するには、スイッチが LAN Base イメージを実行している 必要があります。

VLAN 機能

 最大 255 個の VLAN をサポート。適切なネットワーク リソース、トラフィック パターン、および 帯域幅を対応付けて、VLAN にユーザを割り当てることができます。



E) スイッチが LAN Lite イメージを実行中の場合は、最大 64 の VLAN をサポートできます。

- IEEE 802.1Q 規格で認められている 1 ~ 4094 の範囲で VLAN ID をサポート。
- ダイナミック VLAN メンバシップに対応する VLAN Query Protocol (VQP)。
- すべてのポート上で稼動する IEEE 802.1Q トランキング カプセル化。ネットワークの移動、追加、 変更や、ブロードキャストおよびマルチキャスト トラフィックの管理および制御、さらに、ハイ セキュリティユーザおよびネットワーク リソース別の VLAN グループの確立によるネットワーク セキュリティを実現します。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)。2 台のデバイス間の リンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタ イプ (IEEE 802.1Q) もネゴシエートします。
- VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) および VTP プルーニング。ト ラフィックのフラッディングをそのトラフィックを受信するステーションへのリンクだけに制限す ることによって、ネットワーク トラフィックを削減します。
- 音声 VLAN。Cisco IP Phone から音声トラフィック用のサブネットを作成します。
- VLAN 1 の最小化: VLAN 1 を任意の個々の VLAN トランク リンクでディセーブル化することで、スパニング ツリー ループまたはストームのリスクを軽減。この機能をイネーブルに設定すると、トランク上でユーザ トラフィックは送受信されません。スイッチの CPU は、引き続き制御プロトコル フレームの送受信を行います。
- VLAN Flex Link ロード バランシング: Spanning Tree Protocol (STP; スパニング ツリー プロト コル)を必要としないレイヤ 2 冗長性を提供。プライマリおよびバックアップ リンクとして設定 したインターフェイスのペアを使用して、VLAN ベースによるトラフィックのロード バランシン グが可能です。



VLAN Flex Link ロード バランシングを使用するには、スイッチが LAN Base イメージを実行 している必要があります。

- 制限付き VLAN (別名、認証失敗 VLAN) を使用した 802.1x 認証のサポート。
- VTP バージョン 3 のサポート。これには、VTP モードでの拡張範囲 VLAN (1006 ~ 4094 の VLAN)、拡張認証(暗号化されたパスワード、またはシークレットパスワード)、VTP、VTP プ ライマリ、セカンダリ サーバ、およびその他のデータベースの伝播、およびポートにより VTP を オンまたはオフにするオプションの設定のサポートが含まれます。

セキュリティ機能

• IP Service Level Agreement (SLA; サービス レベル契約) Responder のサポートによって、スイッ チが IP SLA アクティブ トラフィック モニタリングのターゲット デバイスとなります。

▲(注) IP SLA を使用するには、スイッチが LAN Base イメージを実行している必要があります。

• Web 認証。IEEE 802.1x 機能をサポートしないサプリカント(クライアント)に Web ブラウザを 使用して認証可能になります。

(注)

Web 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- ローカル Web 認証バナー。これにより、カスタム バナー、またはイメージ ファイルを Web 認証 ログイン画面に表示することができます。
- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証



- 管理インターフェイス(デバイス マネージャ、Network Assistant、CLI)へのパスワード保護付 きアクセス(読み取り専用および読み書きアクセス)。不正な設定変更を防止します。
- セキュリティレベル、通知、および対応するアクションを選択できる、マルチレベルセキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポートオプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションのMACアドレスを制限または特定するポートセキュリティ オプション。
- VLAN 認識ポート セキュリティ オプション。違反の発生時にポート全体をシャットダウンするのではなく、そのポート上の VLAN をシャットダウンします。
- ポート セキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP アクセス コントロール リスト (ACL) は、レイヤ2インターフェイス (ポート ACL) でのインバウンドなセキュリティ ポリシーを定義します。
- MAC 拡張 ACL。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- untrusted (信頼性のない) ホストと DHCP サーバの間の untrusted DHCP メッセージをフィルタ リングする DHCP スヌーピング。
- DHCP スヌーピング データベース、および IP ソース バインディングに基づいてトラフィックを フィルタリングすることにより、非ルーテッド インターフェイスでのトラフィックを制限する IP ソース ガード。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに 対する悪意のある攻撃を回避するためのダイナミック ARP インスペクション。



• IEEE 802.1x ポートベース認証。不正なデバイス(クライアント)によるネットワーク アクセスを

防止します。次の機能がサポートされています。

(注) MAC 認証バイパスを使用するには、スイッチが LAN Base イメージを実行している必要 があります。

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

NAC レイヤ 2 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 802.1x 検証の設 定」(P.9-60) を参照してください。



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

- 802.1X スイッチ サプリカントを持つ Network Edge Access Topology (NEAT)、CISP を使っ たホスト認証、および自動イネーブル化。これらにより、別のスイッチへのサプリカントとし て、配線クローゼットの外のスイッチが認証されます。
- 認証される前にネットワークへのアクセスをホストに許可するための、オープンアクセスを 使用した IEEE 802.1x。
- ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを使用できるように なります。
- 新しいホストを認証するときに、ポートが思考する認証メソッドの順序を設定するための柔軟な認証シーケンス。
- マルチユーザ認証。複数のホストが、802.1x 対応ポートを認証できるようになります。
- Terminal Access Controller Access Control System Plus (TACACS+)。TACACS サーバを介して ネットワーク セキュリティを管理する独自の機能です。
- Remote Authentication Dial-In User Service (RADIUS)。Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング)によってリモートユーザの身元を確認し、 リモートユーザにアクセス権を与え、リモートユーザのアクションを追跡します。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer (SSL) バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります (ソフトウェ アの暗号化バージョンが必要)。
- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証
- スタティック ホストでの IP ソース ガードのサポート
- あるセッションが認可された後でこのセッションの属性を変更するための RADIUS Change of Authorization (CoA)。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管 理者は AAA サーバから、Cisco Secure ACS などの RADIUS CoA パケットを送信し、新しいポリ シーに適用することができます。
- IEEE 802.1x User Distribution。さまざまな VLAN にわたってユーザをロードバランシングすることにより、(ユーザ グループに対して)複数の VLAN を使った配置で、ネットワークのスケーラビリティを向上させることができます。認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- Support for critical VLAN with マルチ ホスト認証を使った、重要な VLAN のサポート。これにより、ポートが複数認証用に設定され、AAA サーバが到達不能になった場合でも、重要なリソースへのアクセスができるように、このポートが重要な VLAN に配置されます。
- カスタマイズ可能な Web 認証機能強化。ローカル Web 認証で、ユーザ定義の login、success、 failure、および expire Web ページの作成ができるようになります。

- ポートホストモードを変更し、認証者のスイッチポートに標準ポート設定を適用するために Network Edge Access Topology (NEAT)をサポート。
- VLAN-ID ベースの MAC 認証。ユーザ認証のために VLAN と MAC のアドレス情報を結合して、 許可されていない VLAN からのネットワーク アクセスを阻止します。
- MAC 移動。モビリティのイネーブル化を制約することなく、ホスト(IP 電話の背後で接続されたホストを含む)が同じスイッチ内のポート間を移動できるようになります。MAC 移動では、もう1つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。
- Simple Network Management Protocol のバージョン3 (SNMPv3; 簡易ネットワーク管理プロトコルバージョン3)を使った 3DES および AES のサポート。このリリースでは、168 ビット Triple Data Encryption Standard (3DES) と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard (AES; 高度暗号化規格)暗号化アルゴリズムに対するサポートが追加されます。

QoS および CoS 機能

 auto-QoS(自動 QoS)。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。



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

- 分類
 - IP Type of Service/Differentiated Services Code Point (IP ToS/DSCP) および IEEE 802.1p CoS のポート単位でのプライオリティ設定。ミッション クリティカルなアプリケーションの パフォーマンスを保護します。



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

 IP ToS/DSCP および IEEE 802.1p CoS (サービス クラス)のフローベースのパケット分類 (MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく)によるマーキング。ネット ワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化 されたサービス レベルを可能にするとともに、ネットワーク上のミッション クリティカルな トラフィックにプライオリティを設定します。

(注)

- フローベースのパケット分類を使用するには、スイッチが LAN Base イメージを実行している必要があります。
- QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted (信頼性のある) ポート ステート (CoS、DSCP、および IP precedence)。
- – 信頼境界機能。Cisco IP Phoneの存在を検出し、受信した CoS 値を信頼して、ポート セキュ リティを確保します。

• ポリシング

機能



- 特定のトラフィックフローに対してどの程度のポート帯域幅を割り当てるかを管理する、ス イッチポート上のトラフィックポリシングポリシー。
- 階層型のポリシーマップで複数のクラスマップを作成する場合、各クラスマップを自身のポートレベル(第2レベル)ポリシーマップと関連付けることができます。第2レベルのポリシーマップは、それぞれ異なるポリサーを保有できます。
- トラフィック フローのポリシングをまとめて行う集約ポリシング。特定のアプリケーション またはトラフィック フローをあらかじめ定義された特定のレートに制限します。
- 不適合

- 帯域幅の使用制限を超過したパケットの不適合マークダウン。

- 入力キューイングおよびスケジューリング
 - ユーザトラフィック用に設定可能な2つの入力キュー(一方のキューをプライオリティ キューにできます)。
 - 輻輳回避メカニズムとしての Weighted Tail Drop (WTD)。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。

(注)

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

Shaped Round Robin (SRR; シェイプドラウンドロビン):パケットがキューからインターナルリングへ送出されるときのレートを決定するスケジューリングサービス(入力キューでサポートされる唯一のモードはシェアリング)。

(注)

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

(注) 出力キューイングを使用するには、スイッチが LAN Base イメージを実行している必要が あります。

レイヤ 3機能

 適切なルータを選択するホストの機能を向上させるための IPv6 Default Router Preference (DRP) (LAN Base イメージが必要)

Power over Ethernet の機能

- 回路に電気が流れていないことがスイッチにより検出されたときに、PoE 対応ポートから、接続された Cisco 準規格の受電装置、および IEEE 802.3af 準拠の受電装置に電力を提供することができます。
- 電力消費を伴う CDP のサポート。受電装置は、スイッチが消費している電力量を、このスイッチ に知らせます。
- Cisco インテリジェント電力管理のサポート 受電装置とスイッチは、電力消費レベルの合意に向 け、電力ネゴシエーション CDP メッセージを通じてネゴシエーションします。このネゴシエー ションにより、高性能の Cisco 受電装置が最高の電力モードで動作できるようになります。
- 自動検出およびパワーバジェット。スイッチは、パワーバジェットの維持、電力要求のモニタおよび追跡を行いながら、電力が使用可能である場合だけ電力を許可します。
- リアルタイムの消費電力をモニタする機能。スイッチは、PoE ポート単位で、総消費電力を検知し、消費電力をポリシングして、電力消費量をレポートします。

モニタ機能

- スイッチ LED によるポートレベルおよびスイッチレベルのステータス。
- MAC アドレス通知トラップおよび RADIUS アカウンティング。スイッチが学習または削除した MAC アドレスを保存することによって、ネットワーク上のユーザをトラッキングします。
- Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN)。 任意のポートまたは VLAN について、トラフィック モニタリングが可能です。
- Intrusion Detection System (IDS; 侵入検知システム) における SPAN および RSPAN のサポート。 ネットワーク セキュリティ違反をモニタ、撃退、およびレポートします。
- 組み込み RMON エージェントの4つのグループ(履歴、統計、アラーム、およびイベント)を使用して、ネットワークをモニタし、トラフィック解析を行うことができます。
- Syslog 機能。認証または許可エラー、リソースの問題、およびタイムアウト イベントに関するシ ステム メッセージを記録します。
- レイヤ 2 traceroute。パケットが送信元デバイスから宛先デバイスへ送られる物理パスを識別します。
- Time Domain Reflector (TDR)。10/100 および 10/100/1000 の銅線イーサネット ポートでケーブ ル接続の問題を診断し、解決します。
- SFP モジュール診断管理インターフェイス。SFP モジュールの物理または動作ステータスをモニタします。

スイッチ初期設定後のデフォルト値

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

(注)

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

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

- デフォルト スイッチ IP アドレス、サブネットマスク、デフォルト ゲートウェイは 0.0.0.0 です。
 詳細は、第3章「スイッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」および第20章「DHCP 機能 および IP ソース ガード機能の設定」を参照してください。
- ドメイン名はデフォルトで設定されていません。詳細は、第3章「スイッチの IP アドレスおよび デフォルト ゲートウェイの割り当て」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブルに設定されています(DHCP サーバとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。DHCP リレーエージェントはイネーブルに設定されています(DHCP リレーエージェントとして動作するデバイスが設定されていて、イネーブルの場合にのみ)。詳細は、第3章「スイッチの IP アドレスおよびデフォルトゲートウェイの割り当て」および第20章「DHCP 機能 および IP ソース ガード機能の設定」を参照してください。
- スイッチクラスタはディセーブルに設定されています。スイッチクラスタの詳細は、第5章「スイッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。
- パスワードは定義されていません。詳細は、第6章「スイッチの管理」を参照してください。
- システム名とプロンプトは Switch です。詳細は、第6章「スイッチの管理」を参照してください。
- NTP はイネーブルに設定されています。詳細は、第6章「スイッチの管理」を参照してください。
- DNS はイネーブルに設定されています。詳細は、第6章「スイッチの管理」を参照してください。
- TACACS+ はディセーブルに設定されています。詳細は、第8章「スイッチ ベース認証の設定」 を参照してください。
- RADIUS はディセーブルに設定されています。詳細は、第8章「スイッチベース認証の設定」を 参照してください。
- 標準の HTTP サーバおよび SSL HTTPS サーバは両方ともイネーブルに設定されています。詳細は、第8章「スイッチベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルに設定されています。詳細は、第9章「IEEE 802.1x ポートベース認 証の設定」を参照してください。

- ポート パラメータ
 - インターフェイス速度およびデュプレックスモードが自動ネゴシエーションに設定されています。詳細は、第11章「インターフェイス特性の設定」を参照してください。
 - Auto-MDIX はイネーブルに設定されています。詳細は、第11章「インターフェイス特性の設定」を参照してください。
 - フロー制御はディセーブルに設定されています。詳細は、第11章「インターフェイス特性の 設定」を参照してください。
 - PoE は自動ネゴシエーションに設定されています。詳細は、第11章「インターフェイス特性の設定」を参照してください。
- VLAN
 - デフォルト VLAN は VLAN 1 です。詳細は、第13章「VLAN の設定」を参照してください。
 - VLAN トランキング設定は dynamic auto (DTP) です。詳細は、第13章「VLAN の設定」 を参照してください。
 - トランクカプセル化はネゴシエーションです。詳細は、第13章「VLAN の設定」を参照して ください。
 - VTP モードはサーバです。詳細は、第14章「VTP の設定」を参照してください。
 - VTP バージョンはバージョン 1 です。詳細は、第 14 章「VTP の設定」を参照してください。
 - 音声 VLAN はディセーブルに設定されています。詳細は、第15章「音声 VLAN の設定」を 参照してください。
- STP、PVST+は VLAN 1 でイネーブルに設定されています。詳細は、第 16 章「STP の設定」を 参照してください。
- MSTP はディセーブルに設定されています。詳細は、第17章「MSTP の設定」を参照してください。
- オプションのスパニングツリー機能はディセーブルに設定されています。詳細は、第18章「オプションのスパニングツリー機能の設定」を参照してください。
- Flex Link は設定されていません。詳細は、第19章「Flex Link および MAC アドレス テーブル移 動更新機能の設定」を参照してください。



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

- DHCP スヌーピングはディセーブルに設定されています。DHCP スヌーピング情報オプションは イネーブルに設定されています。詳細は、第 20 章「DHCP 機能 および IP ソース ガード機能の設 定」を参照してください。
- IP ソース ガードはディセーブルです。詳細は、第 20 章「DHCP 機能 および IP ソース ガード機能 の設定」を参照してください。
- DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。詳細は、第 20 章 「DHCP 機能 および IP ソース ガード機能の設定」を参照してください。
- すべての VLAN 上でダイナミック ARP インスペクションがディセーブルになっています。詳細 は、第 21 章「ダイナミック ARP インスペクションの設定」を参照してください。
- IGMP スヌーピングはイネーブルに設定されています。IGMP フィルタは適用されていません。詳細は、第22章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否されます。詳細は、第 22 章「IGMP スヌーピングおよび MVR の設定」を参照してください。

- IGMP スヌーピング クエリア機能はディセーブルに設定されています。詳細は、第 22 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルに設定されています。詳細は、第 22 章「IGMP スヌーピングおよび MVR の 設定」を参照してください。



- ポートベース トラフィック
 - ブロードキャスト、マルチキャスト、およびユニキャストストーム制御はディセーブルに設定されています。詳細は、第23章「ポート単位のトラフィック制御の設定」を参照してください。
 - 保護ポートは定義されていません。詳細は、第23章「ポート単位のトラフィック制御の設定」 を参照してください。
 - ユニキャストおよびマルチキャストトラフィックフラッディングはブロックされていません。
 詳細は、第23章「ポート単位のトラフィック制御の設定」を参照してください。
 - セキュアポートは設定されていません。詳細は、第23章「ポート単位のトラフィック制御の 設定」を参照してください。
- CDP はイネーブルに設定されています。詳細は、第25章「CDP の設定」を参照してください。
- UDLD はディセーブルに設定されています。詳細は、第24章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルに設定されています。詳細は、第 27 章「SPAN および RSPAN の設定」を参照してください。



(注) RSPAN を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- RMON はディセーブルに設定されています。詳細は、第28章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルに設定され、コンソール上に表示されます。詳細は、第29章「シ ステム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルに設定されています (バージョン1)。詳細は、第 30 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細は、第 31 章「ACL によるネットワーク セキュリティの設定」 を参照してください。
- QoS はディセーブルに設定されています。詳細は、第33章「QoS の設定」を参照してください。
- EtherChannel は設定されていません。詳細は、第 36 章 「EtherChannel およびリンクステートト ラッキングの設定」を参照してください。

ネットワークの構成例

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

- 「スイッチを使用する場合の設計概念」(P.1-19)
- 「スイッチを使用した中小規模のネットワーク Catalyst 2960 スイッチ」(P.1-22)
- 「長距離広帯域トランスポートの構成」(P.1-24)

スイッチを使用する場合の設計概念

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

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

表 1-1 ネットワーク パフォーマンスの向上

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

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

表 1-2 ネットワーク サービスの提供

ネットワークに対する需要	推奨する設計方式			
マルチメディア アプリケーションに おける帯域幅の効率的な利用および	 IGMP スヌーピングを利用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 			
ミッション クリティカルなアプリ ケーションに対する帯域幅保証	 パケット分類、マーキング、スケジューリング、輻輳回避など、他の QoS メカ ニズムを使用し、適切なプライオリティ レベルを指定してトラフィックを分類 し、最大限の柔軟性を得ながら、ミッション クリティカルなユニキャスト、マ ルチキャスト、およびマルチメディア アプリケーションをサポートできるよう にします。 			
	 MVR を使用して、マルチキャスト VLAN 上でマルチキャスト ストリームを継続的に送信し、なおかつ帯域幅およびセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。 			
<i>常時オン</i> のミッション クリティカル なアプリケーションを実現するため の、ネットワークの冗長性およびア ベイラビリティに対する大きな需要	 VLAN トランク、および BackboneFast を使用して、アップリンク ポート上で トラフィックのロードバランシングを実行し、VLAN トラフィックの転送時に ポート コストが低いアップリンク ポートが選択されるようにします。 			
IP テレフォニーに対する新しい需要	• QoS を使用して、輻輳の発生時に IP テレフォニーなどのアプリケーションを優 先順位付けし、ネットワーク内で発生する遅延およびジッタを制御できるように します。			
	 1ポートあたり少なくとも2つのキューをサポートするスイッチを使用して、音声およびデータトラフィックのプライオリティをIEEE 802.1p/Qに基づくハイプライオリティまたはロープライオリティのいずれかに設定します。スイッチは、1ポートあたり少なくとも4つのキューをサポートします。 			
	 Voice VLAN ID (VVID) を使用して、音声トラフィックに別個の VLAN を用意します。 			
既存のインフラストラクチャを利用 して、自宅または会社からインター	Catalyst Long-Reach Ethernet(LRE)スイッチを使用して、既存のインフラストラ クチャ(既存の電話回線など)上で最大 15MB の IP 接続を提供します。			
ネットまたはイントラネットへデー タおよび音声を高速で伝送する需要 の増大	(注) LRE を使用するには、スイッチが LAN Base イメージを実行している必要が あります。			
	(注) LRE は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチに採用さ れているテクノロジーです。LRE については、各スイッチ固有のマニュアル セットを参照してください。			

スイッチを使用して、以下を作成できます。

 高性能ワークグループに適したコスト効率の高いギガビットツーデスクトップ(図 1-1):ネット ワークリソースへの高速アクセスを実現するには、Catalyst 29603560 スイッチをアクセスレイヤ で使用して、デスクトップにギガビットイーサネットを提供します。輻輳を回避するために、各 スイッチ上で QoS DSCP マーキングによるプライオリティ設定を使用します。ディストリビュー ションレイヤで高速 IP 転送を実現するには、アクセスレイヤのスイッチを、ルーティング機能を 備えたギガビットマルチレイヤスイッチ(Catalyst 3750 スイッチなど)またはルータに接続しま す。

最初の図は分離された高性能ワークグループです。Catalyst 2960 スイッチがディストリビュー ション レイヤの Catalyst 3750 スイッチに接続されています。2 番めの図は、ブランチ オフィスの 高性能ワークグループです。Catalyst 2960 スイッチがディストリビューション レイヤのルータに 接続されています。 この構成では、各スイッチはネットワーク リソースにアクセスするための、専用の 1 Gbps 接続を ユーザに提供します。また、SFP モジュールを使用すると、光ファイバ接続におけるメディアおよ び距離のオプションに柔軟性が提供されます。



図 1-1 高性能ワークグループ(ギガビットツーデスクトップ)

 サーバ集約(図 1-2):スイッチを使用して、サーバグループを相互接続し、ネットワークの物理 的なセキュリティと管理を一元化できます。ディストリビューション レイヤで高速 IP 転送を実現 するには、アクセス レイヤ スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続 します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えることができます。

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

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

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





スイッチを使用した中小規模のネットワーク Catalyst 2960 スイッチ

図 1-3 に、最大 500 人の社員を対象とするネットワークの構成例を示します。このネットワークでは Catalyst 2960 スイッチを使用し、2 つのルータに高速接続できるようにします。これにより、いずれ かのルータに障害が発生した場合でも、インターネット、WAN、およびミッションクリティカルな ネットワーク リソースへの接続が保証されます。スイッチは負荷分散に EtherChannel を使用していま す。

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

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

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

VLAN 間ルーティング以外に、ルータが DSCP プライオリティなどの QoS メカニズムを使用して各種 ネットワーク トラフィックに優先順位を付け、ハイ プライオリティ トラフィックを配信します。輻輳 が発生した場合、QoS がロー プライオリティ トラフィックを廃棄し、ハイ プライオリティ トラフィッ クを伝送できるようにします。 CCM は、コール処理、ルーティング、および Cisco IP Phone 機能とその設定を制御します。Cisco SoftPhone ソフトウェアを実行しているワークステーションを持つユーザは、PC からのコールを配置、 受信、および制御できます。Cisco IP Phone、CCM ソフトウェア、および Cisco SoftPhone ソフト ウェアを使用することで、テレフォニーと IP ネットワークを統合でき、IP ネットワークが音声とデー タをサポートします。

ルータは、ファイアウォール サービス、Network Address Translation (NAT; ネットワーク アドレス変換) サービス、Voice-over-IP (VoIP) ゲートウェイ サービス、WAN およびインターネット アクセス も提供します。



図 1-3 コラプスト バックボーン構成

長距離広帯域トランスポートの構成

(注)

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

図 1-4 に、8 Gbps のデータを1本の光ファイバ ケーブルで伝送する構成を示します。Catalyst 2960 ス イッチには、Coarse Wavelength-Division Multiplexer (CWDM) 光ファイバ SFP モジュールが搭載さ れています。CWDM SFP モジュールに応じて、データは 1470 ~ 1610 nm の波長で送信されます。波 長が高くなるほど、伝送できる距離が長くなります。長距離伝送用に使われる一般的な波長は 1550 nm です。

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

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



次の作業

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

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



CHAPTER 2

CLI の使用方法

この章では、Catalyst スイッチを設定するための Cisco IOS Command-Line Interface (CLI; コマンド ライン インターフェイス)とその使用方法について説明します。2960 内容は次のとおりです。

- 「コマンドモードの概要」(P.2-1)
- 「ヘルプ システムの概要」(P.2-3)
- 「コマンドの省略形」(P.2-4)
- 「コマンドの no 形式および default 形式の概要」(P.2-4)
- 「CLI のエラー メッセージ」 (P.2-5)
- 「コンフィギュレーション ロギングの使用方法」(P.2-5)
- 「コマンド履歴の使用方法」(P.2-6)
- 「編集機能の使用方法」(P.2-7)
- 「show および more コマンド出力の検索およびフィルタリング」(P.2-10)
- 「CLIのアクセス方法」(P.2-11)

コマンド モードの概要

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

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

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

コンフィギュレーション モード (グローバル、インターフェイス、およびライン)を使用して、実行 コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保 存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスする には、まずグローバル コンフィギュレーション モードを開始しなければなりません。グローバル コン フィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コン フィギュレーション モードを開始できます。 表 2-1 に、主要なコマンドモード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表の例では、ホスト名として Switch を使用しています。

表 2-1 コマンドモードの概要

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

表 2-1 コマンド モードの概要 (続き)

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コン フィギュレー ション モードで、 interface コマン ドを入力し、イ ンターフェイス を指定します。	Switch(config-if)#	終了してグローバル コンフィギュレー ション モードに戻 るには、exit を入力 します。 特権 EXEC モード に戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、イー サネットポートのパラメータ を設定します。 インターフェイスの定義につ いては、「インターフェイスコ ンフィギュレーションモード の使用方法」(P.11-11)を参照 してください。 同じパラメータを指定して複 数のインターフェイスを設定 する場合は、「インターフェイ ス 第四の設定」(P.11.12)を参
ライン コンフィギュレーション	グローバル コン フィギュレー ション モードで、 linevty または line console コマ ンドを使用して 回線を指定しま す。	Switch(config-line)#	 終了してグローバル コンフィギュレー ション モードに戻 るには、exit を入力 します。 特権 EXEC モード に戻るには、 Ctrl+Z を押すか、 end を入力します。 	照してください。 このモードを使用して、端末 回線のパラメータを設定しま す。

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

ヘルプ システムの概要

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

表 2-2 ヘルプの概要

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

表 2-2 ヘルプの概要 (続き)

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

コマンドの省略形

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

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

Switch# show conf

コマンドの no 形式および default 形式の概要

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

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

CLI のエラー メッセージ

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

表 2-3 CLI の代表的なエラー メッセージ

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

コンフィギュレーション ロギングの使用方法

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

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtconlog.html



CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用方法

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

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

コマンド履歴バッファ サイズの変更

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

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

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

指定できる範囲は0~256です。

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

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

指定できる範囲は0~256です。

コマンドの呼び出し

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

表 2-4 コマンドの呼び出し

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

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

コマンド履歴機能のディセーブル化

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

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

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

編集機能の使用方法

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

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

編集機能のイネーブル化およびディセーブル化

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

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

Switch (config-line) # no editing

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

Switch# terminal editing

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

Switch(config-line)# editing

キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集

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

表 2-5 キーストロークによるコマンドの編集 (続き)

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

表 2-5 キーストロークによるコマンドの編集 (続き)

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

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

画面幅よりも長いコマンドラインの編集

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

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

矢印キーが使用できるのは、VT100などのANSI互換端末に限られます。

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

Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# \$ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255
Switch(config)# \$t tcp 131.108.2.5 255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# \$108.2.5 255.255.0 131.108.1.20 255.255.255.0 eq 45

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

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

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

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

show および more コマンド出力の検索およびフィルタリン

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

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

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

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

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

Switch# show interfaces | include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet0/1 is up, line protocol is down GigabitEthernet0/2 is up, line protocol is up
CLI のアクセス方法

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

コンソール接続または Telnet による CLI アクセス

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

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッション によって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設 定しておく必要があります。詳細については、「端末回線に対する Telnet パスワードの設定」(P.8-6) を参照してください。

次のいずれかの方法で、スイッチとの接続を確立できます。

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

Telnet アクセスのためのスイッチ設定については、「端末回線に対する Telnet パスワードの設定」 (P.8-6)を参照してください。スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

SSH のためのスイッチ設定については、「SSH のためのスイッチの設定」(P.8-42)を参照してく ださい。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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

■ CLI のアクセス方法



CHAPTER 3

スイッチの IP アドレスおよびデフォルト ゲー トウェイの割り当て

この章では、自動および手動の各方法で、Catalyst 2960 スイッチの初期設定(たとえば、スイッチ IP アドレスの割り当てやデフォルトのゲートウェイ情報)を作成する方法について説明します。スイッチのスタートアップ コンフィギュレーションを変更する方法についても説明します。

(注)

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

この章で説明する内容は、次のとおりです。

- 「起動プロセスの概要」(P.3-2)
- 「スイッチ情報の割り当て」(P.3-3)
- 「実行コンフィギュレーションの確認および保存」(P.3-17)
- 「スタートアップ コンフィギュレーションの変更」(P.3-18)
- 「ソフトウェアイメージ リロードのスケジュール設定」(P.3-23)

起動プロセスの概要

スイッチを起動するには、『Getting Started Guide』または『Hardware Installation Guide』の手順に 従って、スイッチを設置して電源をオンにし、スイッチの初期設定(IP アドレス、サブネットマスク、 デフォルト ゲートウェイ、シークレットおよび Telnet パスワードなど)をおこなう必要があります。 通常の起動プロセスにはブートローダ ソフトウェアの動作が含まれます。ブート ローダは以下のアク ティビティを実行します。

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

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

また、OS が使用不可能になるほどの重大な障害が発生した場合は、ブート ローダはシステムにトラッ プドアからアクセスします。トラップドアからシステムへアクセスして、必要があれば、フラッシュ ファイル システムをフォーマットし、XMODEM プロトコルを使用して OS のソフトウェアイメージ を再インストールし、失われたパスワードを回復し、最終的に OS を再起動できます。詳細について は、「ソフトウェアで障害が発生した場合の回復」(P.37-2)および「パスワードを忘れた場合の回復」 (P.37-4) を参照してください。

(注)

パスワードの回復をディセーブルにできます。詳細については、「パスワード回復のディセーブル化」 (P.8-5)を参照してください。

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

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



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

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

スイッチ情報の割り当て

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

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

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

(注)

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

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

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

デフォルトのスイッチ情報

表 3-1 に、デフォルトのスイッチ情報を示します。

表 3-1 デフォルトのスイッチ情報

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

DHCP ベースの自動設定の概要

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

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

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

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

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

DHCP クライアントの要求プロセス

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

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

図 3-1 DHCP クライアント/サーパ間のメッセージ交換



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

DHCPREQUEST ブロードキャスト メッセージでは、クライアントは、提示された設定情報に対して、 DHCP サーバに正式な要求を戻します。この正式な要求はブロードキャストされるため、クライアン トから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、ク ライアントに提示した IP アドレスを再利用できます。 DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがク ライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバ ウンドされ、クライアントはサーバから受信した設定情報を使用します。スイッチの受信する情報量 は、DHCP サーバの設定方法によって異なります。詳細については、「TFTP サーバの設定」(P.3-8) を参照してください。

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

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

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

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

クライアントがデフォルトのホスト名である場合(hostname name グローバル コンフィギュレーショ ンコマンドが設定されてない、またはホスト名を削除するために no hostname グローバル コンフィ ギュレーションコマンドが入力された)は、ip address dhcp インターフェイス コンフィギュレーショ ンコマンドを入力したとき、DHCP ホスト名オプションはパケットに含まれません。この場合は、ク ライアントがインターフェイスの IP アドレスを取得しながら DCHP ホスト名オプションを DHCP と の相互作用から受信すると、クライアントはその DHCP ホスト名オプションを受け入れ、フラグを設 定して現在システムが設定されたホスト名を持っていることを示します。

DHCP ベースの自動設定およびイメージ アップデートの概要

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

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

DHCP 自動設定

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

DHCP 自動イメージ アップデート

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

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



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

DHCP サーバのようなスイッチを設定する手順については、「「DHCP ベースの自動設定の設定」 (P.3-7)」および『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP addressing and Services」 のセクションにある「Configuring DHCP」のセクションを参照してください。

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

制限事項と制約事項

制限事項を次に示します。

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



TFTP からダウンロードされたコンフィギュレーション ファイルは、実行コンフィギュレーション内の 既存コンフィギュレーションとマージされますが、write memory または

copy running-configuration startup-configuration 特権 EXEC コマンドを入力しないかぎり、 NVRAM に保存されません。ダウンロードされたコンフィギュレーションがスタートアップ コンフィ ギュレーションに保存されると、後続のシステムシステム再起動中に、この機能が実行されないことに 注意してください。

DHCP ベースの自動設定の設定

ここでは、次の設定情報について説明します。

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

DHCP サーバ設定時の注意事項

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

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

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

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

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

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

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

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

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

TFTP サーバの設定

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

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

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

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

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

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

DNS の設定

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

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

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

リレー デバイスの設定

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

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

図 3-2 では、ルータ インターフェイスを次のように設定しています。

インターフェイス 10.0.0.2 の場合

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

インターフェイス 20.0.0.1 の場合

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





コンフィギュレーション ファイルの入手方法

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

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

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

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

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

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

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

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

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

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



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

構成例



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

表 3-2 は、DHCP サーバ上の予約リースの設定例です。

表 3-2 DHCP サーバ コンフィギュレーション

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

DNS サーバ コンフィギュレーション

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

TFTP サーバ コンフィギュレーション (UNIX)

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

prompt> cd /tftpserver/work/
prompt> ls
network-confg
switcha-confg
switchb-confg

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

DHCP クライアント コンフィギュレーション

スイッチA~Dには、コンフィギュレーションファイルは存在しません。

コンフィギュレーションの説明

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

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

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

DHCP 自動設定機能およびイメージ アップデート機能

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

DHCP 自動設定(コンフィギュレーション ファイルだけ)の設定

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

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

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

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

(注)

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

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

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

```
Switch# config terminal
Switch(config) # ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config) # bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config) # option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Switch(dhcp-config) # exit
Switch(config) # tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c2960-lanbase-tar.122-46.SE.tar
Switch(config) # tftp-server flash:boot-config.text
Switch(config) # tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if) # ip address 10.10.10.1 255.255.255.0
Switch(config-if) # end
```

クライアントの設定

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

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

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

```
Switch# configure terminal
Switch(conf)# boot host dhcp
Switch(conf)# boot host retry timeout 300
Switch(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause
You to Nolonger Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file: flash:/config.text
Private Config file: flash:/private-config.text
```

Enable Break:	no
Manual Boot:	no
HELPER path-list:	
NVRAM/Config file	
buffer size:	32768
Timeout for Config	
Download:	300 seconds
Config Download	
via DHCP:	enabled (next boot: enabled)
Switch#	

(注)

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

手動でのスイッチ情報の割り当て

複数の Switched Virtual Interface (SVI) に手動で IP 情報を割り当てるには、特権 EXEC モードで次 の手順を実行します。

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

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

スイッチのシステム名の設定、特権 EXEC コマンドへのアクセスの保護、時刻および日付の設定については、第6章「スイッチの管理」を参照してください。

実行コンフィギュレーションの確認および保存

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

```
Switch# show running-config
Building configuration ...
Current configuration: 1363 bytes
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch A
1
enable secret 5 $1$ej9.$DMUvAUnZOAmvmggBEzIxE0
1
<output truncated>
interface gigabitethernet0/1
ip address 172.20.137.50 255.255.255.0
interface gigabitethernet6/0/2
mvr type source
<output truncated>
...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
no ip directed-broadcast
1
ip default-gateway 172.20.137.1 !
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
end
```

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

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

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

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

スタートアップ コンフィギュレーションの変更

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

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

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

起動のデフォルト設定

表 3-3 に、起動のデフォルト設定を示します。

表 3-3 起動のデフォルト設定

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

コンフィギュレーション ファイルの自動ダウンロード

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

システム コンフィギュレーションを読み書きするためのファイル名の指定

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	boot config-file flash:/file-url	次回の起動時に読み込むコンフィギュレーション ファイルを 指定します。
		<i>file-url</i> に、パス(ディレクトリ)およびコンフィギュレー ション ファイル名を指定します。
		ファイル名およびディレクトリ名は、大文字と小文字が区別さ れます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show boot	設定を確認します。
		boot config-file グローバル コンフィギュレーション コマンド によって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

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

手動で起動する場合

スイッチはデフォルトで自動的に起動しますが、手動で起動するように設定することもできます。 次回の起動時に手動で起動するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行 します。

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

	コマンド	目的
ステップ 4	show boot	設定を確認します。
		boot manual グローバル コンフィギュレーション コマンドに よって、MANUAL_BOOT 環境変数の設定が変更されます。
		次回、システムを再起動したときには、スイッチはブート ロー ダ モードになり、ブート ローダ モードであることが switch: プ ロンプトによって示されます。システムを起動するには、boot filesystem:Ifile-urlブート ローダ コマンドを使用します。
		 <i>filesystem</i>:には、システムボードのフラッシュデバイスを 指定する場合は flash:を使用します。
		 file-urlには、パス(ディレクトリ)および起動可能なイメージの名前を指定します。
		ファイル名およびディレクトリ名は、大文字と小文字が区別さ れます。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

特定のソフトウェア イメージを起動する場合

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

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

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

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

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

環境変数の制御

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

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

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

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

環境変数には2種類のデータが保存されます。

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

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



ブート ローダ コマンドおよび環境変数の構文および使用方法の詳細については、このリリースに対応 するコマンド リファレンスを参照してください。 表 3-4 で、代表的な環境変数の機能について説明します。

表 3-4 環境変数

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

ソフトウェア イメージ リロードのスケジュール設定

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

(注)

リロードのスケジュールは、約24日以内に設定する必要があります。

リロードのスケジュール設定

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

• reload in [hh:]mm [text]

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

• reload at hh:mm [month day | day month] [text]

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



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

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

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

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

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

Switch# reload at 19:30

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

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

Switch# reload at 02:00 jun 20

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

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

リロード スケジュール情報の表示

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

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





Cisco IOS Configuration Engine の設定

この章では、Catalyst 3560 スイッチで機能を設定する方法について説明します。

(注)

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

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

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

Cisco Configuration Engine ソフトウェアの概要

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

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

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

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



図 4-1 Configuration Engine アーキテクチャの概要

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

コンフィギュレーション サービス

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

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

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

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

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

イベント サービス

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

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

NSM

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

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

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

CNS ID およびデバイスのホスト名に関する重要事項

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

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

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

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

ConfigID

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

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

DeviceID

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

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

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

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

ホスト名および DeviceID

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

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

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

注意

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

ホスト名、DeviceID、ConfigID の使用方法

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

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

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

(注)

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

Cisco IOS エージェントの概要

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

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

初期設定

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

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

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

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



差分(部分)設定

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

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

同期設定

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

Cisco IOS エージェントの設定

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

- 「CNS イベント エージェントのイネーブル化」(P.4-7)
- •「Cisco IOS CNS エージェントのイネーブル化」(P.4-9)

自動 CNS 設定のイネーブル化

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

表 4-1 自動設定イネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定(コンフィギュレーション ファイルなし)
ディストリビューション スイッチ	• IP ヘルパーアドレス
	• DHCP リレー エージェントのイネーブル化
	 IP ルーティング (デフォルト ゲートウェイとして使用する 場合)
DHCP サーバ	• IP アドレスの割り当て
	・ TFTP サーバの IP アドレス
	 TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス
	 デフォルトゲートウェイの IP アドレス
TFTP サーバ	 スイッチと Configuration Engine との通信を可能にする CNS 設定 コマンドを含むブートストラップ コンフィギュ レーション ファイル
	 (デフォルトのホスト名の代わりに)スイッチ MAC(メ ディア アクセス制御)アドレスまたはシリアル番号のいず れかを使用して ConfigID および EventID を生成するよう に設定されたスイッチ
	 スイッチにコンフィギュレーションファイルをプッシュするように設定された CNS イベントエージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプ レートにデバイスの ConfigID がマッピングされています。

(注)

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

CNS イベント エージェントのイネーブル化



スイッチ上で CNS イベント エージェントをイネーブルにしてから、CNS 設定 エージェントをイネー ブルにする必要があります。 スイッチ上で CNS イベント エージェントをイネーブルにするには、特権 EXEC モードで次の手順を 実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
ステップ 2	<pre>cns event {hostname ip-address} [port-number] [backup] [failover-time seconds] [keepalive seconds retry-count] [reconnect time] [source ip-address]</pre>	 イベント エージェントをイネーブルにして、ゲート ウェイ パラメータを入力します。 For {<i>hostname</i> <i>ip-address</i>}, enter either the hostname or the IP address of the event gateway.
		 (任意) port number に、イベント ゲートウェイの ポート番号を入力します。デフォルトのポート番 号は 11011 です。
		 (任意) バックアップ ゲートウェイであることを示 す場合は、backup を入力します (省略した場合 は、プライマリ ゲートウェイになります)。
		 (任意) failover-time seconds に、バックアップ ゲートウェイが確立された後にスイッチがプライ マリ ゲートウェイ ルートを待つ時間を入力しま す。
		 (任意) keepalive seconds に、スイッチがキープ アライブメッセージを送信する間隔を入力します。 retry-count に、キープアライブメッセージへの応 答がない場合に接続を終了するまでのメッセージ 送信回数を入力します。デフォルト値はいずれも C です。
		 (任意) reconnect time に、スイッチがイベント ゲートウェイに再接続しようとする前の最大時間 間隔を入力します。
		 (任意) source <i>ip-address</i> に、このデバイスの送信 元 IP アドレスを入力します。
		(注) encrypt キーワードおよび clock-timeout time キーワードは、コマンドラインのヘルプ ストリ ングに表示されますが、サポートされていません。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show cns event connections	イベントエージェントに関する情報を確認します。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存 します。

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

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

Switch(config) # cns event 10.180.1.27 keepalive 120 10

Cisco IOS CNS エージェントのイネーブル化

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

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

初期設定のイネーブル化

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns template connect name	CNS テンプレート接続コンフィギュレーション モードを開始 して、CNS 接続テンプレートの名前を指定します。
ステップ 3	cli config-text	CNS 接続テンプレートにコマンドラインを入力します。テン プレート内の各コマンドラインにこの手順を繰り返します。
ステップ 4		別の CNS 接続テンプレートを設定する場合は、手順 2 ~ 3 を 繰り返します。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]	CNS 接続コンフィギュレーション モードを開始し、CNS 接続 プロファイルの名前を指定し、プロファイル パラメータを定 義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。
		• CNS 接続プロファイルの名前を入力します。
		 (任意) retries number に、接続のリトライ回数を入力します。指定できる範囲は1~30です。デフォルト値は3です。
		 (任意) retry-interval seconds に、Configuration Engine への連続する接続の試行間隔を入力します。指定できる範 囲は1~40秒です。デフォルト値は10秒です。
		 (任意) sleep seconds に、最初の接続試行を実行するまで 待機する時間を入力します。指定できる範囲は 0 ~ 250 秒です。デフォルト値は 0 です。
		 (任意) timeout seconds に、接続が終了しようとした後に待機する時間を入力します。指定できる範囲は 10 ~ 2000 秒です。デフォルト値は 120 です。

	コマンド	目的
ステップ 7	discover {controller controller-type dlci [subinterface subinterface-number] interface [interface-type] line line-type}	CNS 接続プロファイル内のインターフェイス パラメータを入 力します。
		• controller <i>controller-type</i> に、コントローラ タイプを入力 します。
		 dlci に、アクティブな Data-Link Connection Identifier (DLCI; データリンク接続識別子)を入力します。
		(任意) subinterface <i>subinterface-number</i> に、アクティブ な DLCI の検索に使用するポイントツーポイント サブイ ンターフェイス番号を指定します。
		 interface [interface-type]に、インターフェイスのタイプ を入力します。
		• line line-type に、ライン タイプを入力します。
ステップ 8	template name [name]	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレー トを指定できます。
ステップ 9		手順 7 ~ 8 を繰り返し、CNS 接続プロファイルにさらに多く のインターフェイス パラメータと CNS 接続テンプレートを指 定します。
ステップ 10	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	hostname name	スイッチのホスト名を入力します。
ステップ 12	ip route network-number	(任意) IP アドレスが <i>network-number</i> の Configuration Engine へのスタティック ルートを確立します。
	コマンド	目的
---------	--	--
ステップ 13	cns id <i>interface num</i> {dns-reverse ipaddress mac-address} [event] [image]	(任意) Configuration Engine が使用する一意の EventID また は ConfigID を設定します。
	または cns id {hardware-serial hostname string string udi} [event] [image]	 <i>interface num</i>に、インターフェイスの種類(たとえば、 イーサネット、group-async、loopback、 virtual-template)を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレ スまたは MAC アドレスを取得するかを指定します。
		 {dns-reverse ipaddress mac-address } では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには dns-reverse を入力し、IP アドレスを使用するには ipaddress を入力し、MAC アドレスを一意の ID として使用するには mac-address を入力します。
		 (任意) ID をスイッチの識別に使用する event-id 値になる ように設定するには、event を入力します。
		 (任意) ID をスイッチの識別に使用する image-id 値にな るように設定するには、image を入力します。
		(注) event と image キーワードの両方を省略した場合は、 スイッチの識別には image-id 値が使用されます。
		 {hardware-serial hostname string string udi} で、 hardware-serial を入力してスイッチのシリアル番号を一 意の ID として設定するか、hostname (デフォルト)を 入力してスイッチのホスト名を一意の ID として選択する か、string string に任意のテキスト ストリングを一意の ID として入力するか、または udi を入力して Unique Device Identifier (UDI; 一意のデバイス ID)を一意の ID として設定します。

	コマンド	目的
ステップ 14	<pre>cns config initial {hostname ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]</pre>	Cisco IOS をイネーブルにし、初期設定を開始します。
		• For { <i>hostname</i> <i>ip-address</i> }, enter the hostname or the IP address of the configuration server.
		 (任意) port number に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は80 です。
		 (任意)設定が完了したときの設定の成功、失敗、または 警告のメッセージ用に event をイネーブルにします。
		 (任意) cns config initial グローバル コンフィギュレー ション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、no-persist を入力します。no-persist キーワードを入力しない場合、 cns config initial コマンドを使用すると、その結果の設定 が自動的に NVRAM に書き込まれます。
		 (任意) page page に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。
		 (任意)送信元 IP アドレスに使用するには、source ip-address を入力します。
		 (任意) このパラメータを使用したときの構文をチェック するには、syntax-check をイネーブルにします。
		(注) encrypt キーワード、status キーワード、url キーワー ドおよび inventory キーワードは、コマンドラインの ヘルプ ストリングに表示されますが、サポートされて いません。
ステップ 15	end	特権 EXEC モードに戻ります。
ステップ 16	show cns config connections	コンフィギュレーション エージェントに関する情報を確認し ます。
ステップ 17	show running-config	設定を確認します。

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

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

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

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

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# template ip-route
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255 11.11.11.11
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

部分設定のイネーブル化

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

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

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

CNS 設定の表示

表 4-2 特権 EXEC 表示コマンド

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



CHAPTER 5

スイッチのクラスタ化

この章では、Catalyst 2960 スイッチ クラスタの作成と管理に関する概念と手順を説明します。

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

(注)

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

この章では、Catalyst 2960 スイッチ クラスタを中心に説明します。クラスタ内に他のクラスタに対応 した Catalyst スイッチが混在している場合の注意事項や制限事項も紹介しますが、これらのスイッチ に対するクラスタ機能の詳細な説明は割愛します。特定の Catalyst プラットフォームにおけるクラス タの詳細情報は、該当するスイッチのソフトウェア コンフィギュレーション ガイドを参照してくださ い。

この章で説明する内容は、次のとおりです。

- 「スイッチ クラスタの概要」(P.5-2)
- 「スイッチ クラスタのプランニング」(P.5-5)
- 「CLI によるスイッチ クラスタの管理」(P.5-16)
- 「SNMP によるスイッチ クラスタの管理」(P.5-17)



特定のホストまたはネットワークに対してアクセスを制限する場合、ip http access-class グローバル コンフィギュレーション コマンドは使用しないことを推奨します。アクセスを制御するには、クラス タ コマンド スイッチを使用するか、または IP アドレスが設定されているインターフェイス上に Access Control List (ACL; アクセス コントロール リスト)を適用します。ACL の詳細については、 第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

スイッチ クラスタの概要

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

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

スイッチのクラスタ化には次のような利点があります。

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

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

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

表 5-1 に、クラスタ化に対応している Catalyst スイッチを示します。クラスタ コマンド スイッチにな れるスイッチおよびクラスタ メンバー スイッチにしかなれないスイッチ、さらに、それらに必要なソ フトウェア バージョンも示します。

スイッチ	Cisco IOS リリース	クラスタへの対応性
Catalyst 3750-E または Catalyst 3560-E	12.2(35)SE2 以降	メンバーまたはコマンド ス イッチ
Catalyst 3750	12.1(11)AX 以降	メンバーまたはコマンド ス イッチ
Catalyst 3560	12.1(19)EA1b 以降	メンバーまたはコマンド ス イッチ
Catalyst 3550	12.1(4)EA1 以降	メンバーまたはコマンド ス イッチ
Catalyst 2975	12.2(46)EX 以降	メンバーまたはコマンド ス イッチ
Catalyst 2970	12.1(11)AX 以降	メンバーまたはコマンド ス イッチ

表 5-1 スイッチ ソフトウェアおよびクラスタへの対応性

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

表 5-1 スイッチ ソフトウェアおよびクラスタへの対応性 (続き)

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS Release 12.2(25)FX 以降を実行している。
- IP アドレスが指定されている。
- Cisco Discovery Protocol (CDP) バージョン2がイネーブル(デフォルト)に設定されている。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバー スイッチではない。
- 管理 VLAN を介してスタンバイ クラスタ コマンド スイッチに、共通 VLAN を介してクラスタ メ ンバー スイッチに接続されている。

スタンバイ クラスタ コマンド スイッチの特性

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

- Cisco IOS 12.2(25)FX 以降を実行している。
- IP アドレスが指定されている。
- CDP バージョン2 がイネーブルに設定されている。
- 管理 VLAN を介してコマンド スイッチに接続されていて、なおかつ他のスタンバイ コマンド ス イッチに接続されている。
- 共通 VLAN を介して(クラスタ コマンド スイッチおよびスタンバイ コマンド スイッチを除く) 他のすべてのクラスタ メンバー スイッチに接続されている。
- クラスタメンバースイッチとの接続能力を維持するために、クラスタに冗長接続されている。
- 他のクラスタのコマンドスイッチまたはメンバースイッチではない。



(注) スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同タイプのスイッチ でなければなりません。たとえば、クラスタ コマンド スイッチが Catalyst 2960 スイッチの場 合は、スタンバイ クラスタ コマンド スイッチも Catalyst 2960 スイッチにする必要がありま す。スタンバイ クラスタ コマンド スイッチの要件については、他のクラスタ対応スイッチの コンフィギュレーション ガイドを参照してください。

候補スイッチおよびクラスタ メンバー スイッチの特性

*候補スイッチ*とは、クラスタ対応ですがクラスタにまだ追加されていないスイッチを意味します。クラ スタメンバー スイッチは、スイッチ クラスタにすでに追加されているスイッチです。候補スイッチま たはクラスタメンバー スイッチには必須ではありませんが、専用の IP アドレスおよびパスワードを指 定できます(「IP アドレス」(P.5-14)および「パスワード」(P.5-15)を参照してください)。

クラスタに加入する候補スイッチは、次の要件を満たしている必要があります。

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

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

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

スイッチ クラスタのプランニング

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

- 「クラスタ候補およびクラスタメンバーの自動検出」(P.5-5)
- 「HSRP およびスタンバイ クラスタ コマンド スイッチ」(P.5-11)
- 「IP アドレス」 (P.5-14)
- 「ホスト名」(P.5-14)
- 「パスワード」(P.5-15)
- 「SNMP コミュニティ ストリング」(P.5-15)
- 「TACACS+および RADIUS」(P.5-15)
- 「LRE プロファイル」(P.5-16)

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

クラスタ候補およびクラスタ メンバーの自動検出

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

(注)

クラスタ コマンド スイッチを使用してクラスタに対応したスイッチを検出する場合、クラスタ コマン ド スイッチ、クラスタ メンバー、またはクラスタ対応スイッチの CDP を無効にしないでください。 CDP の詳細については、第 25 章「CDP の設定」を参照してください。

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

- 「CDP ホップを使用しての検出」(P.5-6)
- •「CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出」(P.5-6)
- 「異なる VLAN からの検出」(P.5-7)
- 「異なる管理 VLAN からの検出」(P.5-9)
- 「新しくインストールしたスイッチの検出」(P.5-10)

CDP ホップを使用しての検出

クラスタ コマンド スイッチは CDP を使用して、クラスタ エッジから最大 7 CDP ホップ(デフォルト は3ホップ)までスイッチを検出できます。クラスタエッジは、クラスタや候補スイッチに接続して いる一番最後のクラスタ スイッチの部分を指します。たとえば、図 5-1 のクラスタ メンバー スイッチ 9と10はクラスタのエッジにあります。

図 5-1 では、クラスタ コマンド スイッチのポートに VLAN 16 と 62 が割り当てられています。CDP ホップのカウントは3です。クラスタエッジから3ホップ以内にあるので、クラスタコマンドスイッ チはスイッチ11、12、13、14を検出します。スイッチ15はクラスタエッジから4ホップ先なので検 出されません。



CDP ホップを使用しての検出 図 5-1

CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

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

図 5-2 に、サードパーティ製のハブに接続したスイッチを検出するクラスタ コマンド スイッチを示します。ただし、クラスタ コマンド スイッチは Catalyst 5000 スイッチに接続しているスイッチは検出しません。

CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出



図 5-2

異なる VLAN からの検出

クラスタ コマンド スイッチが Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 の 場合、異なる VLAN のクラスタ メンバー スイッチもクラスタに加えることができます。クラスタ メ ンバー スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。図 5-3 のクラスタ コマンド スイッチのポートには VLAN 9、16、 62 が割り当てられているため、これらの VLAN のスイッチは検出できます。VLAN 50 にあるスイッ チは検出できません。また、最初の列の VLAN 16 にあるスイッチも、クラスタ コマンド スイッチに 接続されていないため検出できません。

Catalyst 2900 XL、Catalyst 2950、および Catalyst 3500 XL のクラスタ メンバー スイッチは、それぞれの管理 VLAN を介してクラスタ コマンドスイッチに接続している必要があります。管理 VLAN からの検出については、「異なる管理 VLAN からの検出」(P.5-9)を参照してください。VLAN の詳細については、第 13 章「VLAN の設定」を参照してください。



異なる管理 VLAN からの検出

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

(注)

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

図 5-4 に示されているクラスタ コマンド スイッチおよびスタンバイ コマンド スイッチ (Catalyst 2960、Catalyst 2970、Catalyst 2975、Catalyst 3550、Catalyst 3560、Catalyst 3750 と想定 します)のポートには、VLAN 9、16、および 62 が割り当てられています。クラスタ コマンド スイッ チの管理 VLAN は VLAN 9 です。各クラスタ コマンド スイッチは、以下の例外を除き、異なる管理 VLAN のスイッチを検出します。

- スイッチ7およびスイッチ10(管理 VLAN4のスイッチ)。クラスタコマンドスイッチと共通の VLAN(VLAN62および VLAN9)に接続していないため検出されません。
- スイッチ9。自動検出は非候補デバイス(スイッチ7)より先は検出できないため、検出されません。



図 5-4 レイヤ 3 クラスタ コマンド スイッチを使用して異なる管理 VLAN から検出

新しくインストールしたスイッチの検出

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

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

図 5-5 のクラスタ コマンド スイッチは、VLAN 9 および 16 に加入しています。新しいクラスタ対応の スイッチがクラスタに加入すると、次の処理が行われます。

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



図 5-5 新しくインストールしたスイッチの検出

HSRP およびスタンバイ クラスタ コマンド スイッチ

スイッチは Hot Standby Router Protocol (HSRP) を使用しているため、スタンバイ クラスタ コマンド スイッチのグループを設定できます。 クラスタ コマンド スイッチは、すべての通信の転送と、すべて のクラスタ メンバー スイッチの設定情報を管理しているため、次のような環境設定を推奨します。

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

クラスタスタンバイ グループは、「スタンバイ クラスタ コマンド スイッチの特性」(P.5-4) で説明し ている要件を満たしたコマンド対応スイッチのグループです。クラスタごとに、1 つのクラスタスタン バイ グループのみ割り当てることができます。

クラスタ スタンバイ グループのスイッチは、HSRP プライオリティに基づいてランク付けされていま す。グループ内でプライオリティの高いスイッチは、Active Cluster Command Switch (AC; アクティ ブクラスタ コマンド スイッチ)です。グループ内で次にプライオリティの高いスイッチは、Standby Cluster Command Switch (SC; スタンバイ クラスタ コマンド スイッチ)です。クラスタ スタンバイ グループの他のスイッチは、Passive Cluster Command Switch (PC; パッシブ クラスタ コマンド ス イッチ)です。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド ス イッチ)です。アクティブ クラスタ コマンド スイッチおよびスタンバイ クラスタ コマンド スイッチ が同時にディセーブルになった場合、パッシブ クラスタ コマンド スイッチの中でプライオリティが一 番高いものがアクティブ クラスタ コマンド スイッチになります。自動検出の制限事項については、 「クラスタ設定の自動復旧」(P.5-13)を参照してください。



HSRP のスタンバイ中止間隔は、Hello タイム間隔の3倍以上必要です。デフォルトのHSRP スタンバ イ中止間隔は10秒です。デフォルトのHSRP スタンバイ hello タイム インターバルは3秒です。

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

- 「仮想 IP アドレス」(P.5-12)
- 「クラスタスタンバイグループに関する他の考慮事項」(P.5-12)
- 「クラスタ設定の自動復旧」(P.5-13)

仮想 IP アドレス

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

アクティブ クラスタ コマンド スイッチに障害が発生すると、スタンバイ クラスタ コマンド スイッチ が仮想 IP アドレスを使用して、アクティブ クラスタ コマンド スイッチになります。クラスタ スタン バイ グループのパッシブ スイッチは、それぞれ割り当てられたプライオリティを比較し、新しいスタ ンバイ クラスタ コマンド スイッチを選出します。その後、プライオリティの一番高いパッシブ スタン バイ スイッチがスタンバイ クラスタ コマンド スイッチになります。前回アクティブ クラスタ コマン ド スイッチだったスイッチが再びアクティブになると、アクティブ クラスタ コマンド スイッチの役割 を再開します。そのため、現在アクティブ クラスタ コマンド スイッチを担当しているスイッチは再び スタンバイ クラスタ コマンド スイッチになります。スイッチ クラスタの IP アドレスの詳細について は、「IP アドレス」(P.5-14) を参照してください。

クラスタ スタンバイ グループに関する他の考慮事項

次の要件も満たす必要があります。

 スタンバイ クラスタ コマンド スイッチは、クラスタ コマンド スイッチと同タイプのスイッチでな ければなりません。たとえば、クラスタ コマンド スイッチが Catalyst 2960 スイッチの場合は、ス タンバイ クラスタ コマンド スイッチも Catalyst 2960 スイッチにする必要があります。スタンバ イ クラスタ コマンド スイッチの要件については、他のクラスタ対応スイッチのコンフィギュレー ション ガイドを参照してください。

スイッチ クラスタに Catalyst 2960 スイッチがある場合、このスイッチ クラスタがクラスタ コマ ンド スイッチになります。

- クラスタごとに、1つのクラスタスタンバイグループのみ割り当てることができます。ルータ冗長スタンバイグループは複数作成できます。
- すべてのスタンバイグループメンバーはそのクラスタのメンバーである必要があります。



- (注) スタンバイ クラスタ コマンド スイッチとして割り当てることができるスイッチ数に制限は ありません。ただし、クラスタのスイッチの総数(アクティブ クラスタ コマンド スイッ チ、スタンバイ グループ メンバー、およびクラスタ メンバー スイッチを含む)は16以内 にする必要があります。
- 各スタンバイグループのメンバー(図 5-6 を参照)は、同じ VLAN を介してクラスタ コマンドス イッチに接続されている必要があります。この例のクラスタ コマンドスイッチとスタンバイ クラ スタ コマンド スイッチには Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 が該当します。各スタンバイグループのメンバーも、スイッチ クラスタと同じ VLAN を最低1つ は介在させて、冗長性を持たせながら相互接続する必要があります。

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

- 「異なる VLAN からの検出」(P.5-7)
- 「異なる管理 VLAN からの検出」(P.5-9)



スタンバイグループ メンバーとクラスタ メンバー間の VLAN 接続

クラスタ設定の自動復旧

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

自動検出には次のような制限があります。

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

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

■ スイッチ クラスタのプランニング

IP アドレス

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

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

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

IP アドレスの詳細については、第3章「スイッチの **IP** アドレスおよびデフォルト ゲートウェイの割り 当て」を参照してください。

ホスト名

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

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

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

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

パスワード

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

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

パスワードの詳細については、「スイッチへの不正アクセスの防止」(P.8-1)を参照してください。

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

SNMP コミュニティ ストリング

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

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

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

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

スイッチのコミュニティストリング数とその長さには制限がありません。SNMP およびコミュニティ ストリングの詳細については、第 30 章「SNMP の設定」を参照してください。

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

TACACS+ および RADIUS

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

TACACS+の詳細については、「TACACS+によるスイッチアクセスの制御」(P.8-11)を参照してください。RADIUSの詳細については、「RADIUS によるスイッチアクセスの制御」(P.8-19)を参照してください。

LRE プロファイル

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

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

CLI によるスイッチ クラスタの管理

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

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

switch# rcommand 3

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

Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバー スイッチの CLI にアク セスします。そのあと、Cisco IOS コマンドを通常どおりに使用できます。スイッチの Telnet セッショ ンの設定手順については、「パスワード回復のディセーブル化」(P.8-5) を参照してください。

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

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

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

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

<u>》</u> (注)

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

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

SNMP によるスイッチ クラスタの管理

スイッチの最初の起動時にセットアップ プログラムを使用して IP 情報を入力し、提示されたコンフィ ギュレーションを採用した場合、SNMP はイネーブルに設定されています。セットアップ プログラム を使用して IP 情報を入力していない場合は、SNMP はイネーブルではありません。その場合は、 「SNMP の設定」(P.30-6)の説明に従って、SNMP をイネーブルに設定します。Catalyst 1900 および Catalyst 2820 スイッチでは、SNMP はデフォルトでイネーブルに設定されています。

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



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

クラスタ メンバー スイッチに IP アドレスが割り当てられていない場合、図 5-7 に示すように、クラス タ コマンド スイッチはクラスタ メンバー スイッチからのトラップを管理ステーションにリダイレクト します。クラスタ メンバー スイッチに専用の IP アドレスおよびコミュニティ ストリングが割り当て られている場合、そのクラスタ メンバー スイッチはクラスタ コマンド スイッチを経由せず、管理ス テーションに直接トラップを送信できます。

クラスタ メンバー スイッチに専用の IP アドレスとコミュニティ ストリングが割り当てられている場合、クラスタ コマンド スイッチによるアクセスの他に、その IP アドレスとコミュニティ ストリング も使用できます。SNMP およびコミュニティ ストリングの詳細については、第 30 章「SNMP の設定」 を参照してください。



図 5-7 SNMP によるクラスタ管理

■ SNMP によるスイッチ クラスタの管理



CHAPTER 6

スイッチの管理

この章では、Catalyst 2960スイッチを管理するための1回限りの手順について説明します。 この章で説明する内容は、次のとおりです。

- 「システム日時の管理」(P.6-1)
- 「システム名およびプロンプトの設定」(P.6-16)
- 「バナーの作成」(P.6-19)
- 「MAC アドレス テーブルの管理」(P.6-22)
- 「ARP テーブルの管理」(P.6-34)

システム日時の管理

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

(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。これには、Cisco.com のホー ムページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からア クセス可能です。

ここでは、次の設定情報について説明します。

- 「システム クロックの概要」(P.6-2)
- 「NTP の概要」(P.6-2)
- 「NTP の設定」(P.6-4)
- 「手動での日時の設定」(P.6-12)

システム クロックの概要

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

システム クロックは、次のソースにより設定できます。

- NTP
- 手動設定

システム クロックは、次のサービスに時刻を提供します。

- ユーザの show コマンド
- ログおよびデバッグ メッセージ

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

システム クロックは、時刻に*信頼性がある*かどうか(つまり、信頼できると見なされるタイム ソース によって時刻が設定されているか)を常時トラッキングします。信頼性のない場合は、時刻は表示目的 でのみ使用され、再配信されません。設定情報については、「手動での日時の設定」(P.6-12)を参照し てください。

NTP の概要

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

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

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

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

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

デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確 な時刻が誤ってあるいは意図的に設定されることを防止してください。アクセスリストを使用して制 限する方式および暗号化認証メカニズムの、2種類のメカニズムを使用できます。 シスコの NTP ではストラタム 1 サービスをサポートしていないので、ラジオ クロックまたは原子時計 に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバか ら取得することを推奨します。

図 6-1 に、NTP を使用する一般的なネットワーク例を示します。スイッチA は、NTP サーバ モードで 設定したスイッチB、C、D の NTP マスターです。スイッチB、C、D とスイッチA との間にはサー バアソシエーションが設定されています。スイッチE は、アップストリーム スイッチ (スイッチB) およびダウンストリーム スイッチ (スイッチF) の NTP ピアとして設定されています。



図 6-1 一般的な NTP ネットワークの構成

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

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

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

NTP の設定

スイッチはハードウェアでサポートされるクロックを備えていないため、外部 NTP ソースが使用でき ないときに、ピアが自身を同期化するために使用する NTP マスター クロックとして機能できません。 また、スイッチは、カレンダーに対するハードウェアのサポートも備えていません。そのため、ntp update-calendar および ntp master グローバル コンフィギュレーション コマンドが使用できません。

ここでは、次の設定情報について説明します。

- 「NTP のデフォルト設定」(P.6-4)
- 「NTP 認証の設定」(P.6-5)
- 「NTP アソシエーションの設定」(P.6-6)
- 「NTP ブロードキャスト サービスの設定」(P.6-7)
- 「NTP アクセス制限の設定」(P.6-8)
- 「NTP パケット用の送信元 IP アドレスの設定」(P.6-11)
- 「NTP 設定の表示」(P.6-11)

NTP のデフォルト設定

表 6-1 に、NTP のデフォルト設定を示します。

表 6-1 NTP のデフォルト設定

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

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

NTP 認証の設定

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ntp authenticate	デフォルトではディセーブルに設定されている NTP 認証機能を イネーブルにします。
ステップ 3	ntp authentication-key number md5 value	認証鍵を定義します。デフォルトでは何も定義されていません。
		 number には、鍵の番号を指定します。指定できる範囲は1 ~ 4294967295 です。
		 md5 は、Message Digest Algorithm 5 (MD5) を使用して メッセージ認証サポートが行われるように指定します。
		 valueには、鍵に対する8文字までの任意のストリングを入力します。
		スイッチとデバイスの双方がいずれかの認証鍵を持ち、ntp trusted-key key-number コマンドによって鍵番号が指定されて いないかぎり、スイッチはデバイスと同期化しません。
ステップ 4	ntp trusted-key key-number	1 つまたは複数の鍵番号 (ステップ3 で定義したもの)を指定し ます。ピア NTP デバイスは、このスイッチと同期化するため、 このスイッチへの NTP パケット内にこの鍵番号を設定しなけれ ばなりません。
		デフォルト設定では、信頼される鍵は定義されていません。
		key-number には、ステップ3で定義された鍵を指定します。
		このコマンドは、スイッチが、信頼されていないデバイスと 誤って同期化することを防ぎます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

NTP アソシエーションの設定

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

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

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

アソシエーションの一端しか設定する必要がありません。もう一方のデバイスには自動的にアソシエー ションが設定されます。デフォルトの NTP バージョン (バージョン 3) を使用していて、同期化が発 生しない場合は、NTP のバージョン 2 を使用してください。インターネット上の多くの NTP サーバ は、バージョン 2 で稼動しています。

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

次に、NTP バージョン2を使用して、IP アドレス 172.16.22.44 のピアのクロックにシステム クロック を同期化するようにスイッチを設定する例を示します。

Switch(config)# ntp server 172.16.22.44 version 2

NTP ブロードキャスト サービスの設定

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

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

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

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

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

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

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

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

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

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

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

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

NTP アクセス制限の設定

以降で説明するように、2つのレベルで NTP アクセスを制御できます。

- 「アクセス グループの作成と基本 IP アクセス リストの割り当て」(P.6-9)
- 「特定のインターフェイスでの NTP サービスのディセーブル化」(P.6-10)

アクセス グループの作成と基本 IP アクセス リストの割り当て

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

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

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

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

複数のアクセス タイプについて送信元 IP アドレスがアクセス リストに一致する場合は、最初のタイプ が認可されます。アクセス グループが指定されなかった場合は、すべてのアクセス タイプがすべての デバイスに認可されます。いずれかのアクセス グループが指定されている場合は、指定されたアクセ ス タイプに限り認可されます。

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

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

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

特定のインターフェイスでの NTP サービスのディセーブル化

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

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

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

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

NTP パケット用の送信元 IP アドレスの設定

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

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

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

指定されたインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用 されます。送信元アドレスを特定のアソシエーションに使用する場合は、「NTP アソシエーションの設 定」(P.6-6)に説明したように、ntp peer または ntp server グローバル コンフィギュレーション コマ ンド内で source キーワードを使用します。

NTP 設定の表示

次の2つの特権 EXEC コマンドを使用して NTP 情報を表示できます。

- show ntp associations [detail]
- show ntp status



これらの表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。これには、Cisco.com のホームページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からアクセス可能 です。

手動での日時の設定

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

ここでは、次の設定情報について説明します。

- 「システム クロックの設定」(P.6-12)
- 「日時設定の表示」(P.6-13)
- 「タイム ゾーンの設定」(P.6-13)
- 「夏時間の設定」(P.6-14)

システム クロックの設定

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

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

	コマンド	目的
ステップ 1	clock set hh:mm:ss day month year	次のいずれかのフォーマットで、手動でシステム クロックを設定し
	または	ます。
	clock set hh:mm:ss month day year	 <i>hh:mm:ss</i>には、時刻を時間(24時間形式)、分、秒で指定します。指定された時刻は、設定されたタイムゾーンに基づきます。
		• <i>day</i> には、当月の日付で日を指定します。
		 <i>month</i>には、月を名前で指定します。
		• year には、年を指定します(常に4桁で指定)。

次に、システム クロックを手動で 2001 年の 7 月 23 日午後 1 時 32 分に設定する例を示します。 Switch# clock set 13:32:00 23 July 2001

日時設定の表示

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

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

show clock の表示の前にある記号は、次の意味があります。

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

タイム ゾーンの設定

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 clock timezone zone hour [minutes-offset]	clock timezone zone hours-offset [minutes-offset]	タイム ゾーンを設定します。
		スイッチは内部時刻を UTC で管理するので、このコマンドは表示目 的の場合および手動で時刻を設定した場合に限って使用します。
		 zone には、標準時間が施行されているときに表示されるタイム ゾーンの名前を入力します。デフォルトの設定は UTC です。
		• <i>hours-offset</i> には、UTC からの時差を入力します。
		• (任意) <i>minutes-offset</i> には、UTC からの分差を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

■ システム日時の管理

夏時間の設定

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

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

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

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

Switch(config) # clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
ユーザの居住地域の夏時間が定期的なパターンに従わない	(次の夏時間のイベントの正確な日時を設定
する)場合は、特権 EXEC モードで次の手順を実行します	- 0

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

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

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

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

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

システム名およびプロンプトの設定

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

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

このセクションで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Configuration Fundamentals Command Reference』および『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』を参照してください。これには、Cisco.com のホームページ (Documentation > Cisco IOS Software > 12.2 Mainline > Command References) からアクセス可能 です。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.6-16)
- 「システム名の設定」(P.6-16)
- 「DNS の概要」(P.6-17)

デフォルトのシステム名およびプロンプトの設定

デフォルトのスイッチのシステム名およびプロンプトは Switch です。

システム名の設定

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

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

システム名を設定すると、システムプロンプトとしても使用されます。

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

DNS の概要

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

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

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

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」(P.6-17)
- 「DNS の設定」(P.6-18)
- 「DNS の設定の表示」(P.6-19)

DNS のデフォルト設定

表 6-2 に、DNS のデフォルト設定を示します。

表	6-2	DNS のデフォルト	設定

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

■ システム名およびプロンプトの設定

DNS の設定

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

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

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

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

DNS の設定の表示

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

バナーの作成

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

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



このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。これには、 Cisco.com のホームページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からアクセス可能です。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」(P.6-19)
- 「MoTD ログイン バナーの設定」(P.6-20)
- 「ログインバナーの設定」(P.6-21)

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

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

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

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

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

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

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

Switch(config)#

次に、前の設定により表示されたバナーの例を示します。

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

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

User Access Verification

Password:

ログイン バナーの設定

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

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

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

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

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

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

MAC アドレス テーブルの管理

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

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

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



ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

ここでは、次の設定情報について説明します。

- 「アドレス テーブルの作成」(P.6-23)
- 「MAC アドレスおよび VLAN」(P.6-23)
- 「MAC アドレス テーブルのデフォルト設定」(P.6-23)
- 「アドレス エージング タイムの変更」(P.6-24)
- 「ダイナミック アドレス エントリの削除」(P.6-24)
- 「MAC アドレス変更通知トラップの設定」(P.6-25)
- 「MAC アドレス移動通知トラップの設定」(P.6-27)
- 「MAC しきい値通知トラップの設定」(P.6-28)
- 「スタティック アドレス エントリの追加および削除」(P.6-30)
- 「ユニキャスト MAC アドレス フィルタリングの設定」(P.6-31)
- 「VLAN の MAC アドレス学習のディセーブル化」(P.6-32)
- 「アドレス テーブル エントリの表示」(P.6-33)

アドレス テーブルの作成

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

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

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

MAC アドレスおよび VLAN

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

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

MAC アドレス テーブルのデフォルト設定

表 6-3 に、MAC アドレス テーブルのデフォルト設定を示します。

表 6-3 MAC アドレス テーブルのデフォルト設定

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

アドレス エージング タイムの変更

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

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table aging-time [0 10-1000000] [vlan vlan-id]	ダイナミック エントリが使用または更新されたあと、MAC アド レス テーブル内に保持される時間を設定します。
		指定できる範囲は 10 ~ 1000000 秒です。デフォルトは 300 秒で す。0を入力して期限切れをディセーブルにすることもできま す。スタティック アドレスは、期限切れになることもテーブル から削除されることもありません。
		<i>vlan-id</i> の有効範囲は、1~4094です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table aging-time	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

ダイナミック アドレス エントリの削除

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

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

MAC アドレス変更通知トラップの設定

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

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

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

	コマンド	目的
ステップ 5	mac address-table notification change [interval value] [history-size value]	トラップ インターバル タイムと履歴テーブルのサ イズを入力します。
		 (任意) interval value には、NMS に対して生成される各トラップ セット間の通知トラップ インターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。
		 (任意) history-size value には、MAC 通知履 歴テーブルの最大エントリ数を指定します。 指定できる範囲は 0 ~ 500 です。デフォルト は 1 です。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モード を開始し、SNMP MAC アドレス通知トラップを イネーブルにするインターフェイスを指定します。
ステップ 7	<pre>snmp trap mac-notification change {added removed}</pre>	インターフェイス上で MAC アドレス変更通知ト ラップをイネーブルにします。
		 MAC アドレスがインターフェイスに追加された場合にトラップをイネーブルにします。
		 MAC アドレスがインターフェイスから削除 された場合に MAC 通知トラップをイネーブ ルにします。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show mac address-table notification change interface	設定を確認します。
	show running-config	
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定 を保存します。

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

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

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

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

MAC アドレス移動通知トラップの設定

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2	<pre>snmp-server host host-addr {traps informs} {version</pre>	トラップ メッセージの受信側を指定します。
	{ I 2c 3 }} community-string notification-type	 <i>host-addr</i>には、NMSの名前または IP アドレスを指定します。
		 SNMP トラップをホストに送信するには、 traps (デフォルト)を指定します。SNMP 情報をホストに送信するには、informs を指 定します。
		 サポートする SNMP バージョンを指定します。informs にはバージョン 1 (デフォルト)を使用できません。
		 community-string には、通知動作時に送信するストリングを指定します。snmp-server host コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、snmp-server community コマンドを使用し、次に snmp-server host コマンドを使用することも####レニンド
		 <i>notification-type</i>には、mac-notification キー ワードを使用します。
ステップ 3	snmp-server enable traps mac-notification move	スイッチが MAC アドレス 移動通知トラップを NMS に送信できるようにします。
ステップ 4	mac address-table notification mac-move	MAC アドレス移動通知機能をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show mac address-table notification mac-move	設定を確認します。
	show running-config	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定 を保存します。

スイッチによる MAC アドレス移動通知トラップの送信をディセーブルにするには、no snmp-server enable traps mac-notification move グローバル コンフィギュレーション コマンドを使用します。 MAC アドレス変更通知機能をディセーブルにするには、no mac address-table notification mac-move グローバル コンフィギュレーション コマンドを使用します。 次に、NMS として 172.20.10.10 を指定し、スイッチによる NMS への MAC アドレス移動通知トラッ プの送信をイネーブルにし、MAC アドレス移動通知機能をイネーブルにし、あるポートから別のポー トに MAC アドレスが移動した場合にトラップをイネーブルにする例を示します。

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

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

MAC しきい値通知トラップの設定

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

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

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

	コマンド	目的
ステップ 5	mac address-table notification threshold [limit <i>percentage</i>] [interval <i>time</i>]	MAC アドレスしきい値の使用状況モニタのしき い値を入力します。
		 (任意) limit percentage に、MAC アドレス テーブルの使用率を指定します。有効値は1 ~100% です。デフォルト値は 50% です。
		 (任意) interval time に、通知の間隔を指定します。有効値は 120 秒以上です。デフォルト値は 120 秒です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mac address-table notification threshold show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定 を保存します。

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

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

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

show mac address-table notification threshold 特権 EXEC コマンドを入力すれば、設定を確認することができます。

スタティック アドレス エントリの追加および削除

スタティックアドレスには、次の特性があります。

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

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

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

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

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac address-table static mac-addr	MAC アドレス テーブルにスタティック アドレスを追加します。
	vlan vlan-id interface interface-id	 mac-addr には、アドレス テーブルに追加する宛先 MAC ユニ キャスト アドレスを指定します。この宛先アドレスを持つパ ケットが指定した VLAN に着信すると、指定したインターフェ イスに転送されます。
		 <i>vlan-id</i>には、指定した MAC アドレスを持つパケットを受信する VLAN を指定します。有効な VLAN ID は 1 ~ 4094 です。
		 interface-id には、受信したパケットの転送先インターフェイス を指定します。有効なインターフェイスには、物理ポートまたは ポートチャネルがあります。スタティック マルチキャスト アド レスの場合、複数のインターフェイス ID を入力できます。スタ ティック ユニキャスト アドレスの場合、インターフェイスは同 時に1つしか入力できません。ただし、同じ MAC アドレスおよ び VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table static	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

ユニキャスト MAC アドレス フィルタリングの設定

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

この機能を使用する場合は、次の注意事項に従ってください。

- マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、およびルータ MAC アドレス はサポートされていません。mac address-table static mac-addr vlan vlan-id drop グローバル コ ンフィギュレーション コマンドを入力するときに、これらのアドレスのいずれかを指定すると、 次のいずれかのメッセージが表示されます。
 - % Only unicast addresses can be configured to be dropped
 - $\ensuremath{\$}$ CPU destined address cannot be configured as drop address
- CPU に転送されるパケットもサポートされていません。
- ユニキャスト MAC アドレスをスタティック アドレスとして追加し、ユニキャスト MAC アドレス フィルタリングを設定すると、最後に入力したコマンドに応じて、スイッチは MAC アドレスをス タティック アドレスとして追加するか、MAC アドレスを持つパケットを廃棄します。2番めに入 力したコマンドは、1番めのコマンドより優先されます。

たとえば、mac address-table static *mac-addr* vlan *vlan-id* interface *interface-id* グローバル コン フィギュレーション コマンドに続けて、mac address-table static *mac-addr* vlan *vlan-id* drop コ マンドを入力すると、スイッチは、送信元または宛先として MAC アドレスを持つパケットを廃棄 します。

mac address-table static *mac-addr* **vlan** *vlan-id* **drop** グローバル コンフィギュレーション コマン ドに続けて、**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* コマンドを入 力すると、スイッチは、スタティック アドレスとして MAC アドレスを追加します。

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

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

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

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

次にユニキャスト MAC アドレス フィルタリングをイネーブルにし、送信元または宛先アドレスが c2f3.220a.12f4 であるパケットをスイッチが廃棄するように設定する例を示します。この MAC アドレ スを送信元または宛先アドレスとしたパケットを VLAN 4 で受信すると、パケットは廃棄されます。

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

VLAN の MAC アドレス学習のディセーブル化

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

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

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

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

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

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

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

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

show mac-address-table learning [vlan *vlan-id*] 特権 EXEC コマンドを入力すると、すべての VLAN、 または指定した VLAN の MAC アドレス学習のステータスを表示できます。

アドレス テーブル エントリの表示

表 6-4 に示す1つまたは複数の特権 EXEC コマンドを使用すると、MAC アドレス テーブルを表示できます。

表 6-4 MAC アドレス テーブル表示用のコマンド

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

ARP テーブルの管理

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

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

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



CLI の手順については、Cisco.com ホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline**)にある Cisco IOS Release 12.2 のマニュアルを参照してください。



CHAPTER

SDM テンプレートの設定

『Catalyst 2960 Switch Command Reference』には、コマンド構文および使用方法が記載されています。

- 「SDM テンプレートの概要」(P.7-1)
- 「スイッチ SDM テンプレートの設定」(P.7-2)
- 「SDM テンプレートの表示」(P.7-3)

SDM テンプレートの概要

ネットワークでのスイッチの使用状況に応じて、SDM テンプレートを使用して、特定の機能に対する サポートを最適化するようにスイッチのシステム リソースを設定できます。一部の機能にシステムを 最大限に利用させるようにテンプレートを選択したり、デフォルト テンプレートを使用してリソース を均衡化することができます。

Ternary CAM (TCAM) リソースをさまざまな用途に割り当てるために、スイッチ SDM テンプレートはシステム リソースにプライオリティを設定して、特定の機能のサポートを最適化します。SDM テンプレートを選択することにより、これらの機能を最適化できます。

- デフォルト:デフォルトテンプレートは、すべての機能に均等にリソースを割り当てます。
- デュアル:デュアル IPv4/IPv6 テンプレートを使用することにより、(IPv4 と IPv6 の両方をサポートする)デュアル スタック環境でスイッチを使用できるようになります。デュアル スタックテンプレートを使用すると、各リソースの TCAM の許容容量が少なくなります。IPv4 トラフィックだけを転送する場合は、デュアル スタックテンプレートを使用しないでください。
- QoS: QoS テンプレートは、QoS (Quality of Service) Access Control Entry (ACE; アクセス制御 エントリ)のためのシステム リソースを最大にします。

リソース	デフォルト	QoS	デュアル
ユニキャスト MAC アドレス	8 K	8 K	8 K
IPv4 IGMP グループ	256	256	256
IPv4 ユニキャスト ルート	0	0	0
IPv6 マルチキャスト グループ	0	0	0
直接接続された IPv6 アドレス	0	0	0
間接的な IPv6 ユニキャスト ルート	0	0	0
IPv4 ポリシーベース ルーティング ACE	0	0	0
IPv4 MAC QoS ACE	128	384	0

表 7-1 各テンプレートが許容する機能リソースの概数

表	7-1	各テンプレートが許容する機能リソースの概	ぬ (続き)

リソース	デフォルト	QoS	デュアル
IPv4 MAC セキュリティ ACE	384	128	256
IPv6 ポリシーベース ルーティング	0	0	0
IPv4 MAC QoS ACE	0	0	0
IPv4 MAC セキュリティ ACE	0	0	0

テーブル内の各行は、1 つのテンプレートを選択した場合の、ハードウェアの境界値セットの概数で す。ハードウェア リソースのある部分が一杯の場合は、処理のオーバーフローはすべて CPU に送ら れ、スイッチのパフォーマンスに重大な影響が出ます。

スイッチ SDM テンプレートの設定

ここでは、次の設定情報について説明します。

- 「デフォルトの SDM テンプレート」(P.7-2)
- 「SDM テンプレートの設定時の注意事項」(P.7-2)
- 「SDM テンプレートの設定」(P.7-3)

デフォルトの SDM テンプレート

デフォルトテンプレートがデフォルトです。

SDM テンプレートの設定時の注意事項

SDM テンプレートの選択と設定をおこなう場合は、次の注意事項に従ってください。

- SDM テンプレートの選択と設定を行う際、設定を有効にするため、スイッチをリロードする必要 があります。
- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 の機能を設定しようとすると、警告 メッセージが生成されます。
- デュアルスタックテンプレートを使用すると各リソースのTCAMの許容容量が少なくなるため、 IPv4トラフィックだけを転送する場合はデュアルスタックテンプレートを使用しないでください。

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	sdm prefer {default dual-ipv4-and-ipv6	スイッチで使用する SDM テンプレートを指定します。
	default qos}	キーワードの意味は次のとおりです。
		• default: すべての機能に均等にリソースを割り当てます。
		 dual-ipv4-and-ipv6 default:スイッチがデュアルスタック 環境で使用できます(IPv4 および IPv6 がサポートされま す)。
		• qos: QoS ACE 用のシステム リソースを最大にします。
		スイッチをデフォルト テンプレートに設定するには、no sdm prefer コマンドを使用します。デフォルト テンプレートは、シ ステム リソースを均等に割り当てます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	OS (オペレーティング システム) をリロードします。

システムの再起動後、show sdm prefer 特権 EXEC コマンドを使用して、新しいテンプレート設定を 確認できます。reload 特権 EXEC コマンドの前に show sdm prefer コマンドを入力すると、show sdm prefer コマンドによって、現在使用しているテンプレートと、再起動後にアクティブになるテンプ レートが表示されます。

SDM テンプレートの表示

アクティブ テンプレートを表示するには、パラメータを指定せずに show sdm prefer 特権 EXEC コマ ンドを使用します。

特定のテンプレートでサポートされるリソース数を表示するには、show sdm prefer [default | dual-ipv4-and-ipv6 default | qos] 特権 EXEC コマンドを使用します。

■ SDM テンプレートの表示



CHAPTER 8

スイッチ ベース認証の設定

この章では、Catalyst 2960 スイッチにスイッチベース認証を設定する方法について説明します。 この章で説明する内容は、次のとおりです。

- 「スイッチへの不正アクセスの防止」(P.8-1)
- 「特権 EXEC コマンドへのアクセスの保護」(P.8-2)
- 「TACACS+によるスイッチアクセスの制御」(P.8-11)
- 「RADIUS によるスイッチ アクセスの制御」(P.8-19)
- 「スイッチのローカル認証および許可の設定」(P.8-40)
- 「SSH のためのスイッチの設定」(P.8-42)
- 「SSL HTTP のためのスイッチの設定」(P.8-46)
- 「SCP のためのスイッチの設定」(P.8-54)

スイッチへの不正アクセスの防止

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

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

- 最低限のセキュリティとして、各スイッチ ポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。詳細については、「特権 EXEC コマンドへのアクセスの保護」(P.8-2)を参照してください。
- 追加のセキュリティレイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。詳細については、「ユーザ名とパスワードのペアの設定」(P.8-7)を参照してください。

ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティサーバ上のデータベースに保存できます。これにより、複数のネットワークデバイスが同じデータベースを使用してユーザ認証情報を(必要に応じて許可情報も)得ることができます。詳細については、「TACACS+によるスイッチアクセスの制御」(P.8-11)を参照してください。

特権 EXEC コマンドへのアクセスの保護

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



このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release* 12.2』を参照してください。これには、Cisco.com のホームページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からアクセス可能 です。

ここでは、次の設定情報について説明します。

- •「デフォルトのパスワードおよび権限レベル設定」(P.8-2)
- 「スタティック イネーブル パスワードの設定または変更」(P.8-3)
- 「暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護」(P.8-4)
- 「パスワード回復のディセーブル化」(P.8-5)
- 「端末回線に対する Telnet パスワードの設定」(P.8-6)
- 「ユーザ名とパスワードのペアの設定」(P.8-7)
- 「複数の権限レベルの設定」(P.8-8)

デフォルトのパスワードおよび権限レベル設定

表 8-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 8-1 デフォルトのパスワードおよび権限レベル設定

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブル パ スワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	enable password password	特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。
		デフォルトでは、パスワードは定義されません。
		<i>password</i> には、1~25文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符(?)は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。
		abc を入力します。
		Ctrl+v を入力します。
		?123 を入力します。
		システムからイネーブル パスワードを入力するように求められた場 合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロ ンプトにそのまま abc?123 と入力できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
		イネーブル パスワードは暗号化されず、スイッチのコンフィギュ レーション ファイル内では読み取ることができる状態です。

パスワードを削除するには、no enable password グローバル コンフィギュレーション コマンドを使用 します。

次に、イネーブル パスワードを*llu2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます(従来の特権 EXEC モード アクセス)。

Switch(config)# enable password l1u2c3k4y5

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

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

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

enable secret コマンドは **enable password** コマンドに優先します。2 つのコマンドが同時に有効にな ることはありません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで 次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
ステップ 2	enable password [level level] {password encryption-type encrypted-password}	特権 EXEC モードへのアクセス用に、新しいパスワード を定義するか、既存のパスワードを変更します。
	または	または
	enable secret [level level] {password encryption-type encrypted-password}	シークレット パスワードを定義し、非可逆暗号方式を使 用して保存します。
		 (任意) <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル1 が通常のユーザ EXEC モード権限です。デフォルトレベルは 15 です(特権 EXEC モード権限)。
		 passwordには、1~25文字の英数字のストリングを 指定します。ストリングを数字で始めることはでき ません。大文字と小文字を区別し、スペースを使用 できますが、先行スペースは無視されます。デフォ ルトでは、パスワードは定義されません。
		 (任意) encryption-type には、シスコ独自の暗号化ア ルゴリズムであるタイプ5しか使用できません。暗 号化タイプを指定する場合は、暗号化されたパス ワードを使用する必要があります。この暗号化パス ワードは、別のスイッチの設定からコピーします。
		(注) 暗号化タイプを指定してクリア テキスト パス ワードを入力した場合は、再び特権 EXEC モード を開始することはできません。暗号化されたパス ワードが失われた場合は、どのような方法でも回 復することはできません。
ステップ 3	service password-encryption	(任意)パスワードを定義するとき、または設定を保存す るときに、パスワードを暗号化します。
		暗号化によって、コンフィギュレーション ファイル内の パスワードが読み取り不能になります。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し
		ます。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネー ブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、level キーワードを使用します。レベルを指定して パスワードを設定したら、そのレベルでアクセスする必要のあるユーザだけにそのパスワードを渡して ください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、privilege level グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の権限レベルの設定」(P.8-8) を参照してください。

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

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

次に、権限レベル2に対して暗号化パスワード *\$1\$FaD0\$Xyti5Rkls3LoyxzS8*を設定する例を示します。

Switch(config) # enable secret level 2 5 \$1\$FaD0\$Xyti5Rkls3LoyxzS8

パスワード回復のディセーブル化

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

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



パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステム をデフォルトの状態に戻すような場合に備え、セキュアサーバにコンフィギュレーションファイルの バックアップコピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーションファイ ルのバックアップコピーを保存しないでください。VTP(VLANトランキングプロトコル)トランス ペアレントモードでスイッチが動作している場合は、VLANデータベースファイルのバックアップコ ピーも同様にセキュアサーバに保存してください。スイッチがシステムのデフォルト設定に戻ったと きに、XMODEMプロトコルを使用して、保存したファイルをスイッチにダウンロードできます。詳 細については、「パスワードを忘れた場合の回復」(P.37-4)を参照してください。 ■ 特権 EXEC コマンドへのアクセスの保護

パスワードの回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no service password-recovery	パスワードの回復をディセーブルにします。
		この設定は、フラッシュ メモリの中で、ブート ローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイル シ ステムには含まれません。また、ユーザがアクセスすることはできま せん。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show version	コマンド出力の最後の数行をチェックすることによって、設定を確認 します。

パスワードの回復を再びイネーブルにする場合は、service password-recovery グローバル コンフィ ギュレーション コマンドを使用します。

(注)

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

端末回線に対する Telnet パスワードの設定

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

スイッチを Telnet アクセス用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアを備えた PC またはワークステーショ ンとスイッチのコンソール ポートを接続します。
		コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 デー タ ビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトが表示されるまで、Return キーを何回か押す必要があり ます。
ステップ 2	enable password password	特権 EXEC モードを開始します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	line vty 0 15	Telnet セッション(回線)の数を設定し、ライン コンフィギュレー ション モードを開始します。
		コマンド対応スイッチでは、最大 16 のセッションが可能です。0 お よび 15 を指定すると、使用できる 16 の Telnet セッションすべてを 設定することになります。

	コマンド	目的
ステップ 5	password password	1 つまたは複数の回線に対応する Telnet パスワードを入力します。
		<i>password</i> には、1~25文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

パスワードを削除するには、no password グローバル コンフィギュレーション コマンドを使用します。

次に、Telnet パスワードを let45me67in89 に設定する例を示します。

Switch(config)# line vty 10
Switch(config-line)# password let45me67in89

ユーザ名とパスワードのペアの設定

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

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認 証システムでは、ログイン ユーザ名とパスワードが要求されます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	username name [privilege level] { password encryption-type password}	各ユーザのユーザ名、権限レベル、パスワードを入力します。
		 name には、ユーザ ID を 1 ワードで指定します。スペースおよび 引用符は使用できません。
		 (任意) level には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は0~15です。レベル15では特権 EXEC モードでのアクセスが可能です。レベル1では、ユーザ EXEC モードでのアクセスとなります。
		 <i>encryption-type</i>には、暗号化されていないパスワードが後ろに続く場合は0を、暗号化されたパスワードが後ろに続く場合は7を 指定します。
		 passwordには、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは1~25文字で、埋め込みスペースを使用でき、usernameコマンドの最後のオプションとして指定します。
ステップ 3	line console 0	ライン コンフィギュレーション モードを開始し、コンソール ポート
	または	(回線 0)または VTY 回線(回線 0 ~ 15)を設定します。
	line vty 0 15	

	コマンド	目的
ステップ 4	login local	ログイン時のローカル パスワード チェックをイネーブルにします。
		認証は、ステップ2で指定されたユーザ名に基づきます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、no username name グローバル コンフィギュ レーション コマンドを使用します。パスワード チェックをディセーブルにし、パスワードなしでの接 続を可能にするには、no login ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアはデフォルトで、2 種類のパスワード セキュリティ モードを使用します。ユー ザ EXEC および特権 EXEC です。モードごとに、コマンドの階層レベルを 16 まで設定できます。複 数のパスワードを設定することにより、さまざまなユーザ グループに対して特定のコマンドへのアク セスを許可できます。

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

ここでは、次の設定情報について説明します。

- 「コマンドの権限レベルの設定」(P.8-8)
- 「回線に対するデフォルトの権限レベルの変更」(P.8-10)
- 「権限レベルへのログインおよび終了」(P.8-10)

コマンドの権限レベルの設定

コマンドモードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	privilege mode level level command	コマンドの権限レベルを設定します。
		 mode には、グローバル コンフィギュレーション モードの場合は configure を、EXEC モードの場合は exec を、インターフェイ ス コンフィギュレーション モードの場合は interface を、ライン コンフィギュレーション モードの場合は line をそれぞれ入力し ます。
		 <i>level</i>に指定できる範囲は0~15です。レベル1が通常のユーザ EXEC モード権限です。レベル15は、enable パスワードによっ て許可されるアクセスレベルです。
		• command には、アクセスを制限したいコマンドを指定します。

	コマンド	目的
ステップ 3	enable password level level password	権限レベルに対応するイネーブル パスワードを指定します。
		 <i>level</i>に指定できる範囲は0~15です。レベル1が通常のユーザ EXECモード権限です。
		 passwordには、1~25文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
	または	show running-config コマンドはパスワードとアクセス レベルの設定
	show privilege	を表示します。show privilege コマンドは、権限レベルの設定を表示 します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして SecretPswd14 を定義する例を示します。

Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14

回線に対するデフォルトの権限レベルの変更

回線に対するデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	line vty line	アクセスを制限する仮想端末回線を選択します。
ステップ 3	privilege level level	回線のデフォルトの権限レベルを変更します。
		<i>level</i> に指定できる範囲は $0 \sim 15$ です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、enable パスワードによって許 可されるアクセス レベルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
	または show privilege	show running-config コマンドはパスワードとアクセス レベルの設定 を表示します。show privilege コマンドは、権限レベルの設定を表示 します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、特権 EXEC モードで 次の手順を実行します。

	コマンド	目的
ステップ 1	enable level	指定した権限レベルにログインします。
		<i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ 2	disablelevel	指定した権限レベルを終了します。
		<i>level</i> に指定できる範囲は 0 ~ 15 です。

TACACS+ によるスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus (TACACS+) をイネーブルにして 設定する方法について説明します。TACACS+ は、詳細なアカウンティング情報を収集し、認証およ び許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング)機能により拡張されており、TACACS+ をイ ネーブルにするには AAA コマンドを使用しなければなりません。

(注)

ここで使用するコマンドの構文および使用方法の詳細については、『Cisco IOS Security Command Reference, Release 12.2』を参照してください。

ここでは、次の設定情報について説明します。

- 「TACACS+の概要」(P.8-11)
- 「TACACS+の動作」(P.8-13)
- 「TACACS+の設定」(P.8-14)
- 「TACACS+ 設定の表示」(P.8-19)

TACACS+の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリ ケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼 動する TACACS+ デーモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するに は、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ は、個別のモジュール型認証、許可、およびアカウンティング機能を備えています。 TACACS+ では、単一のアクセス制御サーバ(TACACS+ デーモン)が各サービス(認証、許可、お よびアカウンティング)を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの 機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+の目的は、1つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式 を提供することです。スイッチは、他のシスコ製ルータやアクセス サーバとともにネットワーク アク セス サーバにできます。ネットワーク アクセス サーバは、個々のユーザ、ネットワークまたはサブ ネットワーク、および相互接続されたネットワークとの接続を実現します(図 8-1を参照)。



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

認証:ログインおよびパスワードダイアログ、チャレンジおよび応答、メッセージサポートによって認証の完全制御を行います。

認証機能は、ユーザとの対話を実行できます(たとえば、ユーザ名とパスワードが入力されたあ と、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすること によりユーザを試します)。TACACS+認証サービスは、ユーザ画面にメッセージを送信すること もできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があ ることをユーザに通知することもできます。

- 許可: autocommand、アクセス制御、セッション期間、プロトコル サポートの設定といった、 ユーザ セッション時のユーザ機能についてきめ細かく制御します。また、TACACS+許可機能に よって、ユーザが実行できるコマンドを制限することもできます。
- アカウンティング:課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモン に送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査の ためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカ ウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド(PPP な ど)、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼動するシステムが必要 です。
TACACS+ の動作

ユーザが、TACACS+を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要に なると、次のプロセスが発生します。

 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、 これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに 接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

- 2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
 - ACCEPT: ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが 設定されている場合は、この時点で許可処理が開始されます。
 - REJECT: ユーザは認証されません。TACACS+デーモンに応じて、ユーザはアクセスを拒否 されるか、ログイン シーケンスを再試行するように求められます。
 - ERROR: デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
 - CONTINUE: ユーザは、さらに認証情報の入力を求められます。

認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入りま す。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

- TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよ びそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛てのアトリ ビュートの形式でデータが含まれています。
 - Telnet、Secure Shell (SSH; セキュア シェル)、rlogin、または特権 EXEC サービス
 - 接続パラメータ(ホストまたはクライアントの IP アドレス、アクセスリスト、およびユーザ タイムアウトを含む)

TACACS+ の設定

ここでは、TACACS+をサポートするようにスイッチを設定する方法について説明します。最低限、 TACACS+デーモンを維持するホスト(1つまたは複数)を特定し、TACACS+認証の方式リストを定 義する必要があります。また、任意でTACACS+許可およびアカウンティングの方式リストを定義す ることもできます。方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と 方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを1つまたは複数指定 できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、 リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答 が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リス ト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

- 「TACACS+のデフォルト設定」(P.8-14)
- 「TACACS+ サーバ ホストの特定および認証鍵の設定」(P.8-14)
- 「TACACS+ ログイン認証の設定」(P.8-15)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」(P.8-17)
- 「TACACS+アカウンティングの起動」(P.8-18)

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されます。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設 定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセス するユーザを認証できます。

(注)

TACACS+の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定および認証鍵の設定

認証用に1つのサーバを使用することも、また、既存のサーバホストをグループ化するために AAA サーバグループを使用するように設定することもできます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバグループは、グ ローバル サーバホスト リストとともに使用され、選択されたサーバホストの IP アドレスのリストが 含まれています。 TACACS+ サーバを維持する IP ホストを特定し、任意で暗号鍵を設定するには、特権 EXEC モードで 次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	tacacs-server host hostname [port integer] [timeout integer] [key string]	TACACS+ サーバを維持する IP ホスト(1つまたは複数)を特定し ます。このコマンドを複数回入力して、優先ホストのリストを作成し ます。ソフトウェアは、指定された順序でホストを検索します。
		• hostname には、ホストの名前または IP アドレスを指定します。
		 (任意) port integer には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は1~65535 です。
		 (任意) timeout integer には、スイッチがデーモンからの応答を 待つ時間を秒数で指定します。これを過ぎるとスイッチはタイム アウトしてエラーを宣言します。デフォルトは5秒です。指定で きる範囲は1~1000秒です。
		 (任意) key string には、スイッチと TACACS+ デーモン間のすべてのトラフィックを暗号化および暗号解除するための暗号鍵を指定します。暗号化が成功するには、TACACS+ デーモンに同じ鍵を設定する必要があります。
ステップ 3	aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa group server tacacs+ group-name	(任意) グループ名で AAA サーバ グループを定義します。
		このコマンドによって、スイッチはサーバ グループ サブコンフィ ギュレーション モードになります。
ステップ 5	server ip-address	(任意)特定の TACACS+ サーバを定義済みサーバ グループに対応付 けます。AAA サーバ グループの各 TACACS+ サーバに対してこのス テップを繰り返します。
		グループの各サーバは、ステップ2で定義済みのものでなければなり ません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show tacacs	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、no tacacs-server host hostname グ ローバル コンフィギュレーション コマンドを使用します。設定リストからサーバ グループを削除する には、no aaa group server tacacs+ group-name グローバル コンフィギュレーション コマンドを使用 します。TACACS+ サーバの IP アドレスを削除するには、no server ip-address サーバ グループ サブ コンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適 用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポート に適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト (偶然に default と名前が付けられている)です。デフォルトの方式リストは、名前付き方式リストを明 示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方 式リストは、デフォルトの方式リストに優先します。 方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合の バックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを 認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択し ます。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終 わるまで繰り返されます。この処理のある時点で認証が失敗した場合(つまり、セキュリティサーバ またはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合)、認証プロセス は停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1 ステップ 2 ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
	aaa new-model	AAA をイネーブルにします。
	aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2</i>]	ログイン認証方式リストを作成します。
		 login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、 default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。
		 <i>list-name</i>には、作成するリストの名前として使用する文字列を 指定します。
		• <i>method1</i> には、認証アルゴリズムが試行する実際の方式を指定 します。追加の認証方式は、その前の方式でエラーが返された場 合に限り使用されます。前の方式が失敗した場合は使用されませ ん。
		次のいずれかの方式を選択します。
		 enable:イネーブルパスワードを認証に使用します。この認証 方式を使用するには、あらかじめ enable password グローバル コ ンフィギュレーション コマンドを使用してイネーブルパスワー ドを定義しておく必要があります。
		 group tacacs+: TACACS+認証を使用します。この認証方式を 使用するには、あらかじめ TACACS+ サーバを設定しておく必 要があります。詳細については、「TACACS+ サーバ ホストの特 定および認証鍵の設定」(P.8-14)を参照してください。
		 line:回線パスワードを認証に使用します。この認証方式を使用 するには、あらかじめ回線パスワードを定義しておく必要があり ます。password password ライン コンフィギュレーション コマ ンドを使用します。
		 local: ローカル ユーザ名データベースを認証に使用します。 データベースにユーザ名情報を入力しておく必要があります。 username password グローバル コンフィギュレーション コマン ドを使用します。
		 local-case:大文字と小文字が区別されるローカル ユーザ名デー タベースを認証に使用します。username name password グロー バル コンフィギュレーション コマンドを使用して、ユーザ名情 報をデータベースに入力する必要があります。
		• none : ログインに認証を使用しません。

	コマンド	目的
ステップ 4	line [console tty vty] line-number [ending-line-number]	ライン コンフィギュレーション モードを開始し、認証リストの適用 対象とする回線を設定します。
ステップ 5	login authentication {default	回線または回線セットに対して、認証リストを適用します。
	list-name}	 default を指定する場合は、aaa authentication login コマンドで 作成したデフォルトのリストを使用します。
		• <i>list-name</i> には、 aaa authentication login コマンドで作成したリ ストを指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、no aaa new-model グローバル コンフィギュレーション コマンドを 使用します。AAA 認証をディセーブルにするには、no aaa authentication login {default | *list-name*} *method1* [*method2*...] グローバル コンフィギュレーション コマンドを使用します。ログインの TACACS+ 認証をディセーブルにするかデフォルト値に戻す場合は、no login authentication {default | *list-name*} ライン コンフィギュレーション コマンドを使用します。

(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、ip http authentication aaa グローバル コンフィギュレーション コマンドでスイッチを設定する必要がありま す。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは 確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release* 12.2』を参照してください。これには、Cisco.com のホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**)からアクセス可能です。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルに設定され ていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、 ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定しま す。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアク セスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドに tacacs+ キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+を使用して認証を行った場合は、特権 EXEC アクセス許可に TACACS+を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



許可が設定されていても、CLIを使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization network tacacs+	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可を、スイッチに設定します。
ステップ 3	aaa authorization exec tacacs+	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ TACACS+ 許可をスイッチに設定します。
		exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、no aaa authorization {network | exec} *method1* グローバル コンフィ ギュレーション コマンドを使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量 をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況 をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティ ング レコードは、アカウンティングのアトリビュート値 (AV) ペアを含み、セキュリティ サーバに保 存されます。このデータを解析して、ネットワーク管理、クライアントへの課金、または監査に役立て ることができます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネー ブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa accounting network start-stop tacacs+	ネットワーク関連のすべてのサービス要求について、TACACS+ア カウンティングをイネーブルにします。
ステップ 3	aaa accounting exec start-stop tacacs+	TACACS+アカウンティングにより、特権 EXEC プロセスの最初に 記録開始アカウンティング通知、最後に記録停止通知を送信するよ うに設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、no aaa accounting {network | exec} {start-stop} *method1...* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、show tacacs 特権 EXEC コマンドを使用します。

RADIUS によるスイッチ アクセスの制御

ここでは、RADIUS をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカ ウンティング情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は、 AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。これには、Cisco.com のホームページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からアクセス可能 です。

ここでは、次の設定情報について説明します。

- 「RADIUS の概要」(P.8-19)
- 「RADIUS の動作」(P.8-21)
- **FRADIUS Change of Authorization** (P.8-21)
- 「RADIUS の設定」(P.8-27)
- 「RADIUS の設定の表示」(P.8-40)

RADIUS の概要

RADIUS は分散型クライアント/サーバ システムで、不正なアクセスからネットワークを保護します。 RADIUS クライアントは、サポート対象のシスコ製ルータおよびスイッチ上で稼動します。クライア ントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証 情報、ネットワーク サービス アクセス情報が登録されています。RADIUS ホストは、通常、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft、または他のソ フトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼動しているマルチユーザ システムです。 詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たと えば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データ ベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダ イヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セ キュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カードアクセス制御システムを使用するアクセス環境。あるケースでは、 RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リ ソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ製スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。図 8-2 (P.8-20)を参照してください。

- ユーザが1つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを1つのホスト、Telnet などの1つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第9章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソースアカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始お よび終了時点でデータを送信し、このセッション中に使用されるリソース(時間、パケット、バイ トなど)の量を表示できます。インターネットサービスプロバイダーは、RADIUS アクセス制御 およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリ ティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUSは、双方向認証を行いません。RADIUSは、他社製の デバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUSは、一般に1人のユーザを1つのサービスモデルにバインドします。



図 8-2 RADIUS サービスから TACACS+ サービスへの移行

RADIUS の動作

RADIUS サーバによってアクセス制御されるスイッチに、ユーザがログインおよび認証を試みると、 次のイベントが発生します。

- 1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
- 2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
- 3. ユーザは RADIUS サーバから、次のいずれかの応答を受信します。
 - a. ACCEPT: ユーザが認証されたことを表します。
 - **b.** REJECT: ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、また はアクセスが拒否されます。
 - **c.** CHALLENGE: ユーザに追加データを要求します。
 - d. CHALLENGE PASSWORD: ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります (イネーブルに設定されている場合)。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ(ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイ ムアウトを含む)

RADIUS Change of Authorization

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

ここでは、使用可能なプリミティブおよびそれらの Change of Authorization (CoA) での使用方法を 含む、RADIUS インターフェイスの概要について説明します。

- 「概要」(P.8-21)
- 「Change-of-Authorization 要求」(P.8-22)
- 「CoA 要求応答コード」(P.8-23)
- 「CoA 要求コマンド」(P.8-25)
- 「セッション再認証」(P.8-25)

概要

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、 クエリーが送信されたサーバが応答するプルモデルで使用されます。Catalyst スイッチは、通常プッ シュモデルで使用される RFC 5176 で定義された RADIUS Change of Authorization (CoA) 拡張機能 をサポートし、外部の認証、許可、およびアカウンティング (AAA) またはポリシーサーバからの セッションのダイナミック再設定ができるようにします。

Cisco IOS Release 12.2(52)SE 以降では、これらのセッションごとの CoA 要求がスイッチにサポート されています。

- セッション再認証
- セッション終了

- ポートシャットダウンでのセッション終了
- ポート バウンスでのセッション終了

Catalyst スイッチで、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、基本的なコンフィギュレーションの中には、次のアトリビュートが必要になるものもあります。

- セキュリティおよびパスワード:『Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE』の「Switch-Based Authentication」の章にある「Preventing Unauthorized Access to Your Switch」を参照してください。
- アカウンティング:『Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE』の 「Configuring Switch-Based Authentication」の章にある「Starting RADIUS Accounting」を参照 してください。

Change-of-Authorization 要求

Change of Authorization (CoA) 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用 することによって、セッション識別、ホスト再認証、およびセッション終了をおこなうことができま す。このモデルは、1 つの要求 (CoA-Request) と 2 つの可能な応答コードで構成されています。

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA non-acknowledgement (NAK) [CoA-NAK]

要求は CoA クライアント(通常は RADIUS またはポリシー サーバ)から発信されて、リスナーとして動作するスイッチに送信されます。

ここでは、次の内容について説明します。

- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect (POD) とも呼ばれますが、セッション終了に 対してスイッチでサポートされています。

表 8-2 に、この機能でサポートされている IETF アトリビュートを示します。

表 8-2 サポートされる IETF アトリビュート

アトリビュート番号	アトリビュート名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 8-3 に、Error-Cause アトリビュートの有効値を示します。

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット (無視)
401	サポートされていないアトリビュート
402	脱落しているアトリビュート
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効なアトリビュート値
501	管理上の禁止
502	ルート不可能な要求 (プロキシ)
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチ セッションの選択がサポートされてない

表 8-3 Error-Cause の値

前提条件

CoA インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。 CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定された セッションにだけ作用します。

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。サポートされているコマンドを表 8-4 (P.8-25) に示します。

セッションの識別

特定のセッションを対象とする接続解除要求および CoA 要求の場合は、次の1つ以上のアトリビュートに基づいて、スイッチはそのセッションを特定します。

- Calling-Station-Id (ホスト MAC アドレスを含んでいる IETF アトリビュート #31)
- Audit-Session-Id VSA (シスコの Vendor-Specific Attribute [VSA; ベンダー固有属性])
- Acct-Session-Id (IETF アトリビュート #44)

CoA メッセージに含まれているすべてのセッション識別アトリビュートがセッションと一致する場合 を除き、スイッチは、「無効なアトリビュート値」のエラー コード アトリビュートの設定で Disconnect-NAK または CoA-NAK を返します。

特定のセッションを対象とする接続解除要求または CoA 要求の場合は、次のいずれかのセッション識別子が使用されます。

- Calling-Station-ID (MAC アドレスを含んでいる必要がある IETF アトリビュート #31)
- Audit-Session-ID (シスコのベンダー固有属性)
- Accounting-Session-ID (IETF アトリビュート #44)

メッセージに複数のセッション識別アトリビュートが含まれている場合は、すべてのアトリビュートが セッションに一致する必要があります。そうでなければ、スイッチはエラー コード「無効なアトリ ビュート値」で接続解除: Negative Acknowledgement (NAK) または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケット フォーマットは、次のフィールドからなりま す。コード、識別子、オーセンティケータ、および Type Length Value (TLV; タイプ、長さ、値)のア トリビュート。

アトリビュート フィールドは、シスコの VSA を伝送するために使用されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定の確認応答(ACK)が送信されます。CoA ACK 内に返 されたアトリビュートは CoA 要求に基づいて異なり、各 CoA コマンドで確認されます。

CoA NAK 応答コード

否定の確認応答(NAK)は、許可ステートの変更に失敗したことを示し、その障害の理由を示すアト リビュートを含めることができます。CoA が成功したかを確認するには、show コマンドを使用しま す。

CoA 要求コマンド

ここでは、次の内容について説明します。

- セッション再認証
- セッション終了
- CoA 接続解除要求
- CoA 要求:ホストポートのディセーブル化
- CoA 要求:バウンスポート

Cisco IOS Release 12.2(52)SE 以降では、表 8-4に示されるコマンドがスイッチにサポートされています。

表 8-4 スイッチでサポートされている CoA コマンド

コマンド ¹	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があ ります。

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファ イル(たとえば、ゲスト VLAN)に関連付けられると、AAA サーバは通常、セッション再認証要求を 生成します。再認証要求は、認定証が不明である場合にホストが適切な認証グループに配置されること を許可します。

セッション認証を開始するために、AAA サーバは、次の型式のシスコのベンダー固有属性(VSA)および1つ以上のセッション ID アトリビュートを含んでいる標準 CoA-Request メッセージを送信します。*Cisco:Avpair="subscriber:command=reauthenticate"*

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、 IEEE 802.1x によって認証されている場合は、スイッチは、サーバに EAPoL¹-Requested メッセージ (下の脚注 1 を参照)を送信して応答します。

セッションが現在、MAC Authentication Bypass (MAB; MAC 認証バイパス) によって認証されてい る場合は、アクセス要求をサーバに送信し、最初の成功した認証で使用された同じ ID アトリビュート を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終 了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリ シーで認証されている場合は、再認証メッセージがアクセス制御方式を再開し、最初に試行されるよう に設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるま で維持されます。

1. Extensible Authentication Protocol over Lan

セッション終了

セッションを終了させる3種類の CoA 要求があります。CoA 接続解除要求は、ホスト ポートをディ セーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセン ティケータ ステート マシンが初期化されますが、そのホストのネットワークへのアクセスは制限され ません。

ホストのネットワークへのアクセスを制限するには、

Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコ マンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そ のホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネット ワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合(た とえば、VLAN 変更後)は、ポート バウンスでホスト ポート上のセッションを終了します(ポートを 一時的にディセーブルした後、再びイネーブルにする)。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。このコマンドはセッション指向であるため、「セッションの 識別」(P.8-23)に記載されている1つ以上のセッション ID アトリビュートを加える必要があります。 このセッションを検出できない場合は、スイッチは、「Session Context Not Found」エラー コードアト リビュートで接続解除 NAK メッセージを返します。セッションがある場合は、スイッチはセッション を終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合 は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰 り返されます。再送信の後にこのセッションがない場合は、「Session Context Not Found」エラー コー ド アトリビュートで接続 ACK が送信されます。

CoA 要求:ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッションの識別」(P.8-23) に記載されている1つ以上 のセッション ID アトリビュートを加える必要があります。このセッションを検出できない場合は、ス イッチは、「Session Context Not Found」エラー コード アトリビュートで CoA-NAK メッセージを返 します。このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。



再送信コマンドの後に接続解除要求が失敗すると、(接続解除 ACK が送信されてない場合に)チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがア クティブになるまでの間に発生した他の方法(たとえば、リンク障害)によりセッションが終了することがあります。

CoA 要求: バウンス ポート

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッションの識別」(P.8-23)に記載されている1つ以上 のセッション ID アトリビュートを加える必要があります。このセッションを検出できない場合は、ス イッチは、「Session Context Not Found」エラー コード アトリビュートで CoA-NAK メッセージを返 します。このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイ ネーブルにし (ポート バウンス)、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。

RADIUS の設定

ここでは、スイッチが RADIUS をサポートするように設定する方法について説明します。最低限、 RADIUS サーバ ソフトウェアが稼動するホスト(1つまたは複数)を特定し、RADIUS 認証の方式リ ストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを 定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。 方式リストを使用して、使用するセキュリティプロトコル (TACACS+、ローカル ユーザ名検索など) を1つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されま す。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行い ます。その方式で応答が得られなかった場合は、ソフトウェアはそのリストから次の方式を選択しま す。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わる まで続きます。

スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要 があります。

- 「RADIUS のデフォルト設定」(P.8-28)
- 「RADIUS サーバ ホストの識別」(P.8-28)(必須)
- 「RADIUS ログイン認証の設定」(P.8-30)(必須)
- 「AAA サーバ グループの定義」(P.8-32)(任意)
- 「ユーザイネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」 (P.8-34)(任意)
- 「RADIUS アカウンティングの起動」(P.8-35)(任意)
- 「すべての RADIUS サーバの設定」(P.8-36)(任意)
- 「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」(P.8-36)(任意)
- 「ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定」(P.8-38)(任意)
- 「スイッチ上での CoA の設定」(P.8-39)
- 「CoA 機能のモニタリングおよびトラブルシューティング」(P.8-40)
- 「RADIUS サーバ ロードバランシングの設定」(P.8-40)(任意)

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定 することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスす るユーザを認証できます。

RADIUS サーバ ホストの識別

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キーストリング
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、 または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組 み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして 個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ 上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス(たとえばアカウンティング) を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェール オーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、%RADIUS-4-RADIUS_DEAD メッセージが表示された後、スイッチは 同じデバイス上で2 番めに設定されたホスト エントリでアカウンティング サービスを試みます (RADIUS ホスト エントリは、設定した順序に従って試行されます)。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの 暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定 するには、RADIUS サーバ デーモンが稼動するホストと、そのホストがスイッチと共有するシーク レット テキスト (キー) ストリングを指定しなければなりません。

タイムアウト、再送信回数、および暗号鍵の値は、すべての RADIUS サーバに対してグローバルに設 定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単 位での設定を組み合わせることもできます。スイッチと通信するすべての RADIUS サーバに対して、 これらの設定をグローバルに適用するには、radius-server timeout、radius-server retransmit、およ び radius-server key の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。これ らの設定を特定の RADIUS サーバに適用するには、radius-server host グローバル コンフィギュレー ション コマンドを使用します。



スイッチ上にグローバルな機能とサーバ単位での機能(タイムアウト、再送信回数、およびキーコマン ド)を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、および鍵に関するコマンド は、グローバルに設定したタイムアウト、再送信回数、および鍵に関するコマンドを上書きします。す べての RADIUS サーバに対してこれらの値を設定する方法については、「すべての RADIUS サーバの 設定」(P.8-36)を参照してください。

既存のサーバホストを認証用にグループ化するため、AAA サーバグループを使用するようにスイッチを設定できます。詳細については、「AAA サーバグループの定義」(P.8-32)を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]	リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定 します。
		• (任意) auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。
	5	 (任意) acct-port port-number には、アカウンティング要求の UDP 宛先ポートを指定します。
		 (任意) timeout seconds には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。指定できる範囲は1~1000 です。この設定は、radius-server timeout グローバル コンフィギュレーション コマンドによる設定を上書きします。radius-server host コマンドでタイムアウトを設定しない場合は、radius-server timeout コマンドの設定が使用されます。
		 (任意) retransmit retries には、サーバが応答しない場合、また は応答が遅い場合に、RADIUS 要求をサーバに再送信する回数 を指定します。指定できる範囲は 1 ~ 1000 です。radius-server host コマンドで再送信回数を指定しない場合、radius-server retransmit グローバル コンフィギュレーション コマンドの設定 が使用されます。
		 (任意) key string には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定しま す。
		(注) 鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。鍵は常にradius-server host コマンドの最後のアイテムとして設定してください。先 行スペースは無視されますが、鍵の中間および末尾にあるス ペースは有効です。鍵にスペースを使用する場合は、引用符 が鍵の一部分である場合を除き、引用符で鍵を囲まないでく ださい。
		1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認 識するように設定するには、それぞれ異なる UDP ポート番号を使用 して、このコマンドを必要な回数だけ入力します。スイッチ ソフト ウェアは、指定された順序に従って、ホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号 鍵をそれぞれ設定してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、no radius-server host {*hostname* | *ip-address*} グローバル コ ンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう1 つの RADIUS サーバをアカウンティング用に設定す る例を示します。

Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1 Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2 次に、*hostl*を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトの ポートを使用するように設定する例を示します。

Switch(config) # radius-server host host1

(注)

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッ チの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細につい ては、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト(偶然に default と名前が付けられている)です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合の バックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを 認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択し ます。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終 わるまで繰り返されます。この処理のある時点で認証が失敗した場合(つまり、セキュリティサーバ またはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合)、認証プロセス は停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。

	 コマンド	目的
ステップ 3	aaa authentication login {default list-name} method1 [method2]	ログイン認証方式リストを作成します。
		 <i>login authentication</i> コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。
		• <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。
		• <i>method1</i> には、認証アルゴリズムが試行する実際の方式を指定しま す。追加の認証方式は、その前の方式でエラーが返された場合に限り 使用されます。前の方式が失敗した場合は使用されません。
		次のいずれかの方式を選択します。
		 enable:イネーブル パスワードを認証に使用します。この認証方 式を使用するには、あらかじめ enable password グローバル コン フィギュレーション コマンドを使用してイネーブル パスワードを 定義しておく必要があります。
		 group radius: RADIUS 認証を使用します。この認証方式を使用 するには、あらかじめ RADIUS サーバを設定しておく必要があり ます。詳細については、「RADIUS サーバ ホストの識別」 (P.8-28)を参照してください。
		 line:回線パスワードを認証に使用します。この認証方式を使用 するには、あらかじめ回線パスワードを定義しておく必要があり ます。password password ライン コンフィギュレーション コマ ンドを使用します。
		 local: ローカル ユーザ名データベースを認証に使用します。デー タベースにユーザ名情報を入力しておく必要があります。 username name password グローバル コンフィギュレーションコ マンドを使用します。
		 local-case:大文字と小文字が区別されるローカル ユーザ名デー タベースを認証に使用します。username password グローバル コ ンフィギュレーション コマンドを使用して、ユーザ名情報をデー タベースに入力する必要があります。
		- none:ログインに認証を使用しません。
ステップ 4	line [console tty vty] line-number [ending-line-number]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象 とする回線を設定します。
ステップ 5	login authentication {default	回線または回線セットに対して、認証リストを適用します。
	list-name}	• default を指定する場合は、aaa authentication login コマンドで作成 したデフォルトのリストを使用します。
		• <i>list-name</i> には、 aaa authentication login コマンドで作成したリスト を指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、no aaa new-model グローバル コンフィギュレーション コマンドを 使用します。AAA 認証をディセーブルにするには、no aaa authentication login {default | *list-name*} *method1* [*method2*...] グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、no login authentication {default | *list-name*} ライン コンフィギュレーション コマンドを使用します。

(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、ip http authentication aaa グローバル コンフィギュレーション コマンドでスイッチを設定する必要がありま す。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは 確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。これには、Cisco.com のホームページ(Documentation > Cisco IOS Software > 12.2 Mainline > Command References)からアクセス可能です。

AAA サーバ グループの定義

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチ を設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用し ます。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが 一意の ID (IP アドレスと UDP ポート番号の組み合わせ)を持っていることが条件です。この場合、 個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス(たとえばアカウンティング)を設 定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオー バー バックアップとして動作します。

定義したグループ サーバに特定のサーバを対応付けるには、server グループ サーバ コンフィギュレー ション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の auth-port および acct-port キーワードを使用して複数のホスト インスタンスまたはエントリを特定す ることもできます。 AAA サーバ グループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<pre>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</pre>	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。
		• (任意) auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを 指定します。
		 (任意) acct-port port-number には、アカウンティング要求の UDP 宛先ポートを指定します。
		 (任意) timeout seconds には、スイッチが RADIUS サーバの応答を 待機して再送信するまでの時間間隔を指定します。指定できる範囲 は1~1000です。この設定は、radius-server timeout グローバル コンフィギュレーション コマンドによる設定を上書きします。 radius-server host コマンドでタイムアウトを設定しない場合は、 radius-server timeout コマンドの設定が使用されます。
		 (任意) retransmit retries には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は1~1000です。radius-server host コマンドで再送信回数を指定しない場合、radius-server retransmit グローバル コンフィギュレーション コマンドの設定が使用されます。
		 (任意) key string には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
		(注) 鍵は、RADIUS サーバで使用する暗号鍵に一致するテキストストリングでなければなりません。鍵は常にradius-server host コマンドの最後のアイテムとして設定してください。先行スペースは無視されますが、鍵の中間および末尾にあるスペースは有効です。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
		1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識す るように設定するには、それぞれ異なる UDP ポート番号を使用して、 このコマンドを必要な回数だけ入力します。スイッチ ソフトウェアは、 指定された順序に従って、ホストを検索します。各 RADIUS ホストで使 用するタイムアウト、再送信回数、および暗号鍵をそれぞれ設定してく ださい。
ステップ 3	aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa group server radius	AAA サーバ グループを、特定のグループ名で定義します。
	group-name	このコマンドを使用すると、スイッチはサーバ グループ コンフィギュ レーション モードになります。
ステップ 5	server ip-address	特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。 AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返 します。
		クルーブの各サーバは、ステッブ2で定義済みのものでなければなりません。
ステップ 6	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」(P.8-30)を参照してください。

特定の RADIUS サーバを削除するには、no radius-server host {hostname | *ip-address*} グローバル コ ンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから 削除するには、no aaa group server radius group-name グローバル コンフィギュレーション コマンド を使用します。RADIUS サーバの IP アドレスを削除するには、no server *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ (group1 および group2) を認識するようにス イッチを設定しています。group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同 じサービス用に設定しています。2 番めのホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可をイネーブルにすると、 スイッチは(ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する) ユーザのプロ ファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロ ファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定するには、aaa authorization グローバル コンフィギュレーション コマンドとともに radius キーワードを使用します。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

(注)

許可が設定されていても、CLIを使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization network radius	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、スイッチに設定します。
ステップ 3	aaa authorization exec radius	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可を、スイッチに設定します。
		exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、no aaa authorization {network | exec} methodl グローバル コンフィ ギュレーション コマンドを使用します。

RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量 をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況 をアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティン グ レコードは、アカウンティングのアトリビュート値(AV)ペアを含み、セキュリティ サーバに保存 されます。このデータを解析して、ネットワーク管理、クライアントへの課金、または監査に役立てる ことができます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブ ルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa accounting network start-stop radius	ネットワーク関連のすべてのサービス要求について、RADIUS アカ ウンティングをイネーブルにします。
ステップ 3	aaa accounting exec start-stop radius	RADIUS アカウンティングにより、特権 EXEC プロセスの最初に 記録開始アカウンティング通知、最後に記録停止アカウンティング 通知を送信するように設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、no aaa accounting {network | exec} {start-stop} method1... グローバル コンフィギュレーション コマンドを使用します。

すべての RADIUS サーバの設定

スイッチとすべての RADIUS サーバ間でグローバルに通信を設定するには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server key string	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキ スト ストリングを指定します。
		(注) 鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。先行スペースは無視されま すが、鍵の中間および末尾にあるスペースは有効です。鍵にス ペースを使用する場合は、引用符が鍵の一部分である場合を除 き、引用符で鍵を囲まないでください。
ステップ 3	radius-server retransmit retries	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デ フォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 4	radius-server timeout seconds	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するま での時間(秒)を指定します。デフォルトは5秒です。指定できる範 囲は1~1000です。
ステップ 5	radius-server deadtime minutes	認証要求に応答しない RADIUS サーバをスキップする時間(分)を指定し、要求がタイムアウトするまで待機することなく、次に設定されているサーバを試行できるようにします。デフォルトは0です。指定できる範囲は0~1440分です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定値を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数、タイムアウト、および待機時間の設定をデフォルトに戻すには、これらのコマンドの no 形式を使用します。

ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定

Internet Engineering Task Force(IETF)ドラフト規格に、ベンダー固有のアトリビュート(アトリ ビュート 26)を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式 が定められています。各ベンダーは、Vendor-Specific Attribute(VSA)を使用することによって、一 般的な用途には適さない独自の拡張アトリビュートをサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを1つサポートして います。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダー タイプ1(名前は *cisco-avpair*)です。この値は、次のフォーマットのストリングです。

protocol : attribute sep value *

*protocol*は、特定の許可タイプに使用するシスコのプロトコルアトリビュートの値です。*attribute*および *value*は、シスコの TACACS+ 仕様で定義されている適切なアトリビュート値(AV)ペアです。 *sep*は、必須のアトリビュートの場合は=、任意指定のアトリビュートの場合は*です。TACACS+許可で使用できるすべての機能は、RADIUSでも使用できます。

たとえば、次の AV ペアを指定すると、IP 許可時 (PPP の IPCP アドレスの割り当て時) に、シスコの *複数の名前付き IP アドレス プール*機能が有効になります。

cisco-avpair= "ip:addr-pool=first"

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例 を示します。 cisco-avpair= "shell:priv-lvl=15" 次に、RADIUS サーバデータベース内の許可 VLAN を指定する例を示します。 cisco-avpair= "tunnel-type(#64)=VLAN(13)" cisco-avpair= "tunnel-medium-type(#65)=802 media(6)" cisco-avpair= "tunnel-private-group-ID(#81)=vlanid" 次に、この接続中に ASCII 形式の入力 ACL(アクセス コントロール リスト)をインターフェイスに 適用する例を示します。 cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0" cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any" cisco-avpair= "mac:inacl#3=deny any any decnet-iv" 次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。 cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any" 他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベン ダー ID および VSA の詳細については、RFC 2138 「Remote Authentication Dial-In User Service (RADIUS)」を参照してください。 スイッチが VSA を認識して使用するように設定するには、特権 EXEC モードで次の手順を実行しま

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server vsa send [accounting authentication]	スイッチが VSA(RADIUS IETF アトリビュート 26 で定義)を認識し て使用できるようにします。
		 (任意)認識されるベンダー固有属性の集合をアカウンティングアトリビュートだけに限定するには、accounting キーワードを使用します。
		 (任意)認識されるベンダー固有属性の集合を認証アトリビュート だけに限定するには、authentication キーワードを使用します。
		キーワードを指定せずにこのコマンドを入力すると、アカウンティン グおよび認証のベンダー固有属性の両方が使用されます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定値を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

<u>》</u> (注)

す。

RADIUS アトリビュートの全リストまたはベンダー固有属性 26 の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.2*』の付録「RADIUS Atributes」を参照してください。これ には、Cisco.com のホームページ (Documentation > Cisco IOS Software > 12.2 Mainline > Command References) からアクセス可能です。

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報 を通信する方式について定められていますが、RADIUS アトリビュート セットを独自に機能拡張して いるベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS アトリビュート のサブセットをサポートしています。

前述したように、RADIUS (ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問 わず)を設定するには、RADIUS サーバ デーモンが稼動しているホストと、そのホストがスイッチと 共有するシークレット テキスト ストリングを指定しなければなりません。RADIUS ホストおよびシー クレット テキスト ストリングを指定するには、radius-server グローバル コンフィギュレーション コ マンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト ストリングを 指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始 します。
ステップ 2	radius-server host {hostname ip-address} non-standard	リモート RADIUS サーバ ホストの IP アドレスま たはホスト名を指定し、そのホストが、ベンダー が独自に実装した RADIUS を使用していることを 指定します。
ステップ 3	radius-server key string	スイッチとベンダー独自仕様の RADIUS サーバと の間で共有されるシークレット テキスト ストリン グを指定します。スイッチおよび RADIUS サーバ は、このテキスト ストリングを使用して、パス ワードの暗号化および応答の交換を行います。
		(注) 鍵は、RADIUS サーバで使用する暗号鍵 に一致するテキスト ストリングでなけれ ばなりません。先行スペースは無視されま すが、鍵の中間および末尾にあるスペース は有効です。鍵にスペースを使用する場合 は、引用符が鍵の一部分である場合を除 き、引用符で鍵を囲まないでください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定値を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定 を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、no radius-server host {*hostname* | *ip-address*} non-standard グローバル コンフィギュレーション コマンド を使用します。鍵をディセーブルにする には、no radius-server key グローバル コンフィギュレーション コマンドを使用します。

次に、ベンダー独自仕様の RADIUS ホストを指定し、スイッチとサーバの間で rad124 という秘密鍵 を使用する例を示します。

Switch(config) # radius-server host 172.20.30.15 nonstandard Switch(config) # radius-server key rad124

スイッチ上での CoA の設定

スイッチ上で CoA を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。
ステップ 3	aaa server radius dynamic-author	スイッチを認証、許可、およびアカウンティング(AAA)サーバに 設定し、外部ポリシーサーバとの相互作用を実行します。
ステップ 4	client {ip-address name} [vrf vrfname] [server-key string]	ダイナミック認証ローカル サーバ コンフィギュレーション モードを 開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クラ イアントを指定します。
ステップ 5	server-key [0 7] string	RADIUS キーをデバイスと RADIUS クライアントとの間で共有され るように設定します。
ステップ 6	port port-number	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 7	auth-type {any all session-key}	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。
		クライアントは、認証用に設定されたすべてのアトリビュートと一致 する必要があります。
ステップ 8	ignore session-key	(任意) セッション キーを無視するようにスイッチを設定します。
		ignore コマンドの詳細については、Cisco.com 上の 『 <i>Cisco IOS</i> <i>Intelligent Services Gateway Command Reference</i> 』を参照してください。
ステップ 9	ignore server-key	(任意)サーバキーを無視するようにスイッチを設定します。
		ignore コマンドの詳細については、Cisco.com 上の 『 <i>Cisco IOS</i> <i>Intelligent Services Gateway Command Reference</i> 』を参照してください。
ステップ 10	authentication command bounce-port ignore	(任意) CoA 要求を無視して、セッションをホスティングするポート を一時的にディセーブルにするようにスイッチを設定します。ポート を一時的にディセーブルにする目的は、VLAN の変更が発生しても、 その変更を検出するサプリカントがエンドポイント上にない場合に、 ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 11	authentication command disable-port ignore	(任意) セッションをホスティングしているポートを管理上のシャッ トダウン状態にすることを要求する非標準コマンドを無視するように スイッチを設定します。ポートをシャットダウンすると、セッション が終了します。
		ポートを再びイネーブルにするには、標準の CLI または SNMP コマ ンドを使用します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show running-config	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、no aaa new-model グローバル コンフィギュレーション コマンドを 使用します。スイッチ上の AAA サーバ機能をディセーブルにするには、no aaa server radius dynamic authorization グローバル コンフィギュレーション コマンドを使用します。

CoA 機能のモニタリングおよびトラブルシューティング

次の Cisco IOS コマンドを使用すると、スイッチ上の CoA 機能モニタおよびトラブルシューティング をおこなうことができます。

- debug radius
- debug aaa coa
- debug aaa pod
- debug aaa subsys
- debug cmdhd [detail | error | events]
- show aaa attributes protocol radius

RADIUS サーバ ロードバランシングの設定

この機能を使用すると、アクセス要求および認証要求を、サーバ グループ内のすべての RADIUS サー バに対して均等に送信できます。詳細は、次の URL にアクセスして、『Cisco IOS Security Configuration Guide, Release 12.2』の「RADIUS Server Load Balancing」の章を参照してください。 http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

RADIUS の設定の表示

RADIUS の設定を表示するには、show running-config 特権 EXEC コマンドを使用します。

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウ ンティング機能は使用できません。

スイッチをローカル AAA 用に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。
ステップ 3	aaa authentication login default local	ローカルのユーザ名データベースを使用するようにログイン認証を設定 します。default キーワードにより、ローカル ユーザ データベース認証 がすべてのポートに適用されます。
ステップ 4	aaa authorization exec local	ユーザの AAA 許可を設定し、ローカル データベースを確認して、その ユーザに EXEC シェルの実行を許可します。
ステップ 5	aaa authorization network local	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 許可を 設定します。

	コマンド	目的
ステップ 6	username name [privilege level] { password encryption-type password}	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定 します。
		ユーザごとにコマンドを繰り返し入力します。
		 name には、ユーザ ID を 1 ワードで指定します。スペースおよび引用符は使用できません。
		 (任意) level には、アクセス権を得たユーザに設定する権限レベル を指定します。指定できる範囲は0~15です。レベル15では特権 EXECモードでのアクセスが可能です。レベル0では、ユーザ EXECモードでのアクセスとなります。
		 <i>encryption-type</i>には、暗号化されていないパスワードが後ろに続く 場合は0を、暗号化されたパスワードが後ろに続く場合は7を指定 します。
		 passwordには、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは1~25文字で、埋め込みスペースを使用でき、usernameコマンドの最後のオプションとして指定します。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show running-config	設定を確認します。
ステップ 9	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、no aaa new-model グローバル コンフィギュレーション コマンドを 使用します。許可をディセーブルにするには、no aaa authorization {network | exec} *method1* グロー バル コンフィギュレーション コマンドを使用します。

(注)

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、ip http authentication aaa グローバル コンフィギュレーション コマンドでスイッチを設定する必要がありま す。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは 確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release* 12.2』を参照してください。

SSH のためのスイッチの設定

ここでは、SSH 機能を設定する方法について説明します。この機能を使用するには、暗号(暗号化) ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必要があります。詳細について は、このリリースのリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「SSH の概要」(P.8-42)
- 「SSH の設定」(P.8-43)
- 「SSH の設定およびステータスの表示」(P.8-46)

SSH の設定例については、『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。URL は 次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfssh.html#wp1001292

(注)

ここで使用するコマンドの構文および使用方法の詳細については、次の URL にあるこのリリースに対応するコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a 0080087e33.html

SSH の概要

SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認 証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。 このソフトウェア リリースは、SSH バージョン 1 (SSHv1) および SSH バージョン 2 (SSHv2) をサ ポートしています。

ここでは、次の内容について説明します。

- 「SSH サーバ、統合クライアント、およびサポートされているバージョン」(P.8-42)
- 「制限事項」(P.8-43)

SSH サーバ、統合クライアント、およびサポートされているバージョン

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるア プリケーションです。SSH クライアントを使用すると、SSH サーバが稼動するスイッチに接続できま す。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH ク ライアントと使用します。また、SSH クライアントは、このリリースでサポートされている SSH サー バおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートしています。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、DES 暗号化アルゴリズム、Triple DES (3DES) 暗号化アルゴリズム、およびパスワード ベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+(詳細については、「TACACS+によるスイッチアクセスの制御」(P.8-11)を参照して ください)
- **RADIUS**(詳細については、「**RADIUS**によるスイッチアクセスの制御」(P.8-19)を参照してく ださい)
- ローカル認証および許可(詳細については、「スイッチのローカル認証および許可の設定」 (P.8-40)を参照)



このソフトウェア リリースは、IP Security (IPSec) をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman (RSA) 認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES (56 ビット) および 3DES (168 ビット) データ暗 号化ソフトウェアでのみサポートされます。
- スイッチは、Advanced Encryption Standard (AES) 対称暗号化アルゴリズムをサポートしません。

SSH の設定

内容は次のとおりです。

- 「設定時の注意事項」(P.8-43)
- 「スイッチで SSH を実行するためのセットアップ」(P.8-44)(必須)
- 「SSH サーバの設定」(P.8-45)(スイッチを SSH サーバとして設定する場合のみ必須)

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA 鍵のペアを使用できます(逆の場合も同様です)。
- crypto key generate rsa グローバル コンフィギュレーション コマンドを入力したあと、CLI エ ラーメッセージが表示される場合、RSA 鍵ペアは生成されていません。ホスト名およびドメイン を再設定してから、crypto key generate rsa コマンドを入力してください。詳細については、「ス イッチで SSH を実行するためのセットアップ」(P.8-44)を参照してください。
- RSA 鍵のペアを生成する場合に、メッセージNo host name specifiedが表示されることがあります。このメッセージが表示された場合は、hostname グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。

- RSA 鍵のペアを生成する場合に、メッセージNo domain specifiedが表示されることがあります。 このメッセージが表示された場合は、ip domain-name グローバル コンフィギュレーション コマ ンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされて いることを確認してください。

スイッチで SSH を実行するためのセットアップ

SSH を実行するようにスイッチをセットアップするには、次の手順を実行してください。

- **1.** 暗号化ソフトウェア イメージを Cisco.com からダウンロードします。この手順は必須です。詳細 については、このリリースのリリース ノートを参照してください。
- **2.** スイッチのホスト名および IP ドメイン名を設定します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
- **3.** スイッチが SSH を自動的にイネーブルにするための RSA 鍵のペアを生成します。この手順を実行 するのは、スイッチを SSH サーバとして設定する場合だけです。
- 4. ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。 詳細については、「スイッチのローカル認証および許可の設定」(P.8-40)を参照してください。

ホスト名と IP ドメイン名を設定し、RSA 鍵のペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	hostname hostname	スイッチのホスト名を設定します。
ステップ 3	ip domain-name domain_name	スイッチのホスト ドメインを設定します。
ステップ 4	crypto key generate rsa	スイッチ上でローカルおよびリモート認証用に SSH サーバをイネー ブルにし、RSA 鍵のペアを生成します。
		最小モジュラス サイズは、1024 ビットにすることを推奨します。
		RSA 鍵のペアを生成する場合に、モジュラスの長さの入力を求めら れます。モジュラスが長くなるほど安全ですが、生成と使用に時間が かかります。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
	または	
	show ssh	スイッチ上の SSH サーバのステータスを表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RSA 鍵のペアを削除するには、crypto key zeroize rsa グローバル コンフィギュレーション コマンド を使用します。RSA 鍵のペアを削除すると、SSH サーバは自動的にディセーブルになります。

| 第8章 スイッチベース認証の設定

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip ssh version [1 2]	(任意) SSHv1 または SSHv2 を実行するようにスイッチを設定します。
		• 1:SSHvl を実行するようにスイッチを設定します。
		• 2: SSHv2 を実行するようにスイッチを設定します。
		このコマンドを入力しない場合、またはキーワードを指定しない場 合、SSH サーバは、SSH クライアントでサポートされている最新 バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートしている場合、SSH サーバは SSHv2 を選択します。
ステップ 3	ip ssh {timeout seconds	SSH 制御パラメータを設定します。
	authentication-retries <i>number</i> }	 タイムアウト値は秒単位で指定します(デフォルト値は 120 秒)。 指定できる範囲は 0 ~ 120 秒です。このパラメータは、SSH ネ ゴシエーション フェーズに適用されます。接続が確立されると、 スイッチは CLI ベース セッションのデフォルトのタイムアウト 値を使用します。
		デフォルトでは、ネットワーク上の複数の CLI ベース セッショ ン(セッション 0 ~ 4)に対して、最大 5 つの暗号化同時 SSH 接 続を使用できます。実行シェルが起動すると、CLI ベース セッ ションのタイムアウト値はデフォルトの 10 分に戻ります。
		 クライアントをサーバへ再認証できる回数を指定します。デフォルトは3です。指定できる範囲は0~5です。
		両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 4	line vty line_number	(任意) 仮想端末回線設定を設定します。
	[ending_line_number] transport input ssh	 ライン コンフィギュレーション モードを開始して、仮想端末回 線設定を設定します。<i>line_number</i> および <i>ending_line_number</i> に対して、1 回線ペアを指定します。指定できる範囲は 0 ~ 15 です。
		 スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
	または	
	show ssh	スイッチ上の SSH サーバの接続ステータスを表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの SSH 制御パラメータに戻すには、no ip ssh {timeout | authentication-retries} グローバ ル コンフィギュレーション コマンドを使用します。

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

SSH の設定およびステータスの表示

SSH サーバの設定およびステータスを表示するには、表 8-5 の特権 EXEC コマンドを1 つまたは複数 使用します。

表 8-5 SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference, Cisco IOS Release 12.2*』の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfssh.html

SSL HTTP のためのスイッチの設定

ここでは、HTTP 1.1 のサーバおよびクライアントに対応した Secure Socket Layer (SSL) バージョン 3.0 を設定する方法について説明します。SSL は、セキュア HTTP 通信を実現するために、HTTP クラ イアント認証だけでなく、サーバ認証、暗号化、およびメッセージの完全性も提供します。SSL を使 用するには、暗号化ソフトウェア イメージがスイッチにインストールされている必要があります。こ の機能を使用し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードするには許可を得る必 要があります。暗号化イメージの詳細については、このリリースのリリース ノートを参照してくださ い。

ここでは、次の情報について説明します。

- 「セキュア HTTP サーバおよびクライアントの概要」(P.8-47)
- 「セキュア HTTP サーバおよびクライアントの設定」(P.8-49)
- 「セキュア HTTP サーバおよびクライアントのステータスの表示」(P.8-53)

ここで使用する設定例やコマンドの構文および使用方法の詳細については、次の URL にある Cisco IOS Release 12.2(15)T の「HTTPS - HTTP Server and Client with SSL 3.0」の機能説明を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftsslsht.html

セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信 されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュ アな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、ア プリケーション レイヤの暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と 省略されます(セキュアな接続の場合、URL が http://の代わりに https://で始まります)。

セキュア HTTP サーバ (スイッチ)の主な役割は、指定のポート (デフォルトの HTTPS ポートは 443)で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サー バはその要求を処理して、セキュア HTTP サーバへ応答 (呼び出す)します。セキュア HTTP サーバ は HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント(Web ブラウザ)の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を(そのアプリケーションに)返すことです。

CA の信頼点

Certificate Authority (CA; 認証局)は、要求を認可して参加するネットワークデバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集中的なセキュリティキーおよび証明書の管理を提供します。特定の CA サーバは*信頼点*と呼ばれます。

接続が実行されると、HTTPS サーバは、信頼点となる特定の CA から得た X.509v3 の証明書を発行す ることで、セキュアな接続をクライアントに提供します。クライアント(通常、Web ブラウザ)は、 その証明書の認証に必要な公開鍵を保有しています。

セキュア HTTP 接続には、CA の信頼点を設定することを強く推奨します。HTTPS サーバを実行して いるデバイスに CA の信頼点が設定されていないと、サーバは自身を認証して必要な RSA の鍵のペア を生成します。自身で認証した(自己署名)証明書は適切なセキュリティではないので、接続するクラ イアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択(確立または拒否)をさ せる必要があります。この選択肢は内部ネットワークトポロジ(テスト用など)に役立ちます。

CAの信頼点を設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ(またはクライアント)に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されてない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書 (一時的に)が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。

(注)

認証局および信頼点は、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、 それらはスイッチ上で無効になります。

自己署名証明書が生成された場合、その情報は show running-config 特権 EXEC コマンドで出力でき ます。自己署名証明書を表示するコマンドの出力(show running-config コマンド)を例として一部示 します。

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

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072

```
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3080755072
revocation-check none
rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
certificate self-signed 01
3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
59312F30 2D060355 04031326 494F532D 53656c66 2D536967 6E65642D 43657274
69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109

coutput truncated>
    自己署名証明書は、セキュア HTTP サーバを無効にして、no crypto pki trustpoint
TP-self-signed-30890755072 グローバル コンフィギュレーション コマンドを入力することで削除でき
```

ます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

```
<u>入</u>
(注)
```

TP self-signed の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド(**ip http secure-client-auth**)を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

認証局の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Configuring Authority Interoperability」の章を参照してください。これには、Cisco.com のホームページ (**Documentation > Cisco IOS Software > 12.2 Mainline > Command References**) からアクセス可能 です。

CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェスト アルゴリズムを指定して、SSL 接続に使用しま す。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリ ストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで 最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、 米国の セキュリティ(RSA 公開鍵暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC)をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアント ブラウザ(Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など)が必要です。 SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要にな ります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷(速さ)による CipherSuite のランク(速い順)を定義します。

- **1.** SSL_RSA_WITH_DES_CBC_SHA:メッセージの暗号化に DES-CBC、およびメッセージダイ ジェストに SHA を使用した RSA の鍵交換(RSA 公開鍵暗号化)
- SSL_RSA_WITH_RC4_128_MD5: RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA の鍵交換
- **3.** SSL_RSA_WITH_RC4_128_SHA: RC4 128 ビット暗号化、およびメッセージ ダイジェストに SHA を使用した RSA の鍵交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA:メッセージの暗号化に 3DES と DES-EDE3-CBC、 およびメッセージ ダイジェストに SHA を使用した RSA の鍵交換(RSA 公開鍵暗号化)

(暗号化およびダイジェスト アルゴリズムをそれぞれ指定して組み合わせた) RSA は、SSL 接続において鍵の生成および認証の両方に使用されます。これは、CA の信頼点が設定されているかどうかにかかわりません。

セキュア HTTP サーバおよびクライアントの設定

ここでは、次の設定情報について説明します。

- 「SSL のデフォルト設定」(P.8-49)
- 「SSL の設定時の注意事項」(P.8-49)
- 「CA の信頼点の設定」(P.8-50)
- 「セキュア HTTP サーバの設定」(P.8-51)
- 「セキュア HTTP クライアントの設定」(P.8-53)

SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA の信頼点は設定されていません。

自己署名証明書は生成されていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンダで終了します。クラスタ メンバーのスイッチは標準の HTTP で動作させる必要があります。

CA の信頼点を設定する前に、システム クロックが設定されていることを確認してください。クロック が設定されていないと、不正な日付により証明書が拒否されます。

CA の信頼点の設定

セキュア HTTP 接続には、CA の信頼点を正式に設定することを推奨します。CA の信頼点は、自己署 名証明書より高いセキュリティがあります。

CA の信頼点を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	hostname hostname	スイッチのホスト名を指定します(以前ホスト名を設定していない場合のみ必須)。ホスト名はセキュリティ鍵と証明書に必要です。
ステップ 3	ip domain-name domain-name	スイッチの IP ドメイン名を指定します(以前 IP ドメイン名を設定し ていない場合のみ必須)。IP ドメイン名はセキュリティ鍵と証明書に 必要です。
ステップ 4	crypto key generate rsa	(任意) RSA 鍵のペアを生成します。RSA 鍵のペアは、スイッチの 証明書を入手する前に必要です。RSA 鍵のペアは自動的に生成され ます。必要であれば、このコマンドを使用して鍵を再生成できます。
ステップ 5	crypto ca trustpoint name	CA の信頼点にローカルの設定名を指定して、CA 信頼点コンフィ ギュレーション モードを開始します。
ステップ 6	enrollment url <i>url</i>	証明書の要求の送信先スイッチの URL を指定します。
ステップ 7	enrollment http-proxy host-name port-number	(任意) HTTP プロキシ サーバを経由して CA から証明書を入手する ようにスイッチを設定します。
ステップ 8	crl query <i>url</i>	ピアの証明書が取り消されていないかを確認するために、Certificate Revocation List (CRL; 証明書失効リスト)を要求するようにスイッチを設定します。
ステップ 9	primary	(任意) 信頼点が CA 要求に対してプライマリ(デフォルト) 信頼点 として使用されるように指定します。
ステップ 10	exit	CA 信頼点コンフィギュレーション モードを終了し、グローバル コ ンフィギュレーション モードに戻ります。
ステップ 11	crypto ca authentication name	CA の公開鍵を取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	crypto ca enroll name	指定の CA の信頼点から証明書を取得します。このコマンドは、各 RSA 鍵のペアに対して1つの署名入りの証明書を要求します。
ステップ 13	end	特権 EXEC モードに戻ります。
ステップ 14	show crypto ca trustpoints	設定を確認します。
ステップ 15	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

no crypto ca trustpoint name グローバル コンフィギュレーション コマンドを使用して、CA に関連す るすべての ID 情報および証明書を削除できます。

セキュア HTTP サーバの設定

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA 信頼点を設定してから、 HTTP サーバを有効にする必要があります。CA の信頼点を設定していない場合、セキュア HTTP サー バを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定したあと、標準およびセ キュア HTTP サーバ両方に適用するオプション (パス、適用するアクセス リスト、最大接続数、また はタイムアウト ポリシー)を設定できます。

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的		
ステップ 1	show ip http server status	(任意) HTTP サーバのステータスを表示して、セキュア HTTP サーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。		
		HTTP secure server capability: Present or HTTP secure server capability: Not present		
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 3	ip http secure-server	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。		
ステップ 4	ip http secure-port port-number	(任意) HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ~ 65535 の範囲で指定できます。		
ステップ 5	ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴ リズム)を指定します。特定の CipherSuite を指定する理由がなけれ ば、サーバとクライアントが、両方がサポートする CipherSuite でネ ゴシエートするように設定します。これがデフォルトです。		
ステップ 6	ip http secure-client-auth	(任意) HTTP サーバを設定して、接続処理の間、認証のために、ク ライアントからの X.509v3 証明書を要求します。デフォルトでは、 クライアントがサーバからの証明書を要求する設定になっています が、サーバはクライアントを認証しないようになっています。		
ステップ 7	ip http secure-trustpoint name	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA の信頼点を指定します。		
		(注) このコマンドの使用は、前の手順に従って CA の信頼点をす でに設定しているという前提を踏まえて説明しています。		
ステップ 8	ip http path <i>path-name</i>	(任意) HTML ファイルのベースとなる HTTP パスを設定します。パ スは、ローカル システムにある HTTP サーバ ファイルの場所を指定 します (通常、システムのフラッシュ メモリを指定します)。		
ステップ 9	ip http access-class access-list-number	(任意) HTTP サーバへのアクセスの許可に使用するアクセス リスト を指定します。		
ステップ 10	ip http max-connections value	(任意) HTTP サーバへの同時最大接続数を指定します。指定できる 範囲は 1 ~ 16 です。デフォルトは 5 です。		

	コマンド	目的
ステップ 11	ip http timeout-policy idle seconds life seconds requests value	(任意) 指定の状況下における、HTTP サーバへの接続最大時間を指 定します。
		 idle: データの受信がないか、応答データが送信できない場合の 最大時間。指定できる範囲は1~600秒です。デフォルト値は 180秒です(3分)。
		• life:接続を確立している最大時間。指定できる範囲は1~ 86400秒です(24時間)。デフォルト値は180秒です。
		 requests: 永続的な接続で処理される要求の最大数。最大値は 86400です。デフォルトは1です。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show ip http server secure status	セキュア HTTP サーバのステータスを表示して、設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

標準の HTTP サーバをディセーブルにするには、no ip http server グローバル コンフィギュレーショ ン コマンドを使用します。セキュア HTTP サーバをディセーブルにするには、no ip http secure-server グローバル コンフィギュレーション コマンドを使用します。デフォルトの設定に戻すに は、no ip http secure-port および no ip http secure-ciphersuite グローバル コンフィギュレーション コマンドを使用します。クライアント認証の要件を削除するには、no ip http secure-client-auth グ ローバル コンフィギュレーション コマンドを使用します。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://URL を入力します(URL は IP アドレス、またはサーバ スイッチのホスト名)。デフォルト ポート以外のポートを設定している場合、 URL の後ろにポート番号も指定する必要があります。次に例を示します。

https://209.165.129:1026 または

https://host.domain.com:1026

セキュア HTTP クライアントの設定

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証 にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA の信頼点をス イッチに設定していることを前提にしています。CA の信頼点が設定されておらず、リモートの HTTPS サーバがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗し ます。

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	ip http client secure-trustpoint name	(任意) リモートの HTTP サーバがクライアント認証を要求した場合 に使用する、CA の信頼点を指定します。このコマンドの使用は、前 の手順を使用して CA の信頼点をすでに設定しているという前提を踏 まえて説明しています。クライアント認証が必要ない場合、またはプ ライマリの信頼点がすでに設定されている場合は、このコマンドは任 意です。		
ステップ 3	ip http client secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴ リズム)を指定します。特定の CipherSuite を指定する理由がなけれ ば、サーバとクライアントが、両方がサポートする CipherSuite でネ ゴシエートするように設定します。これがデフォルトです。		
ステップ 4	end	特権 EXEC モードに戻ります。		
ステップ 5	show ip http client secure status	セキュア HTTP サーバのステータスを表示して、設定を確認します。		
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。		

クライアントの信頼点の設定を削除するには、no ip http client secure-trustpoint name コマンドを使用します。クライアントにすでに設定されている CipherSuite 仕様を削除するには、no ip http client secure-ciphersuite コマンドを使用します。

セキュア HTTP サーバおよびクライアントのステータスの表示

SSL セキュア サーバおよびクライアントのステータスを表示するには、表 8-6 に記載された特権 EXEC コマンドを使用します。

表 8-6 SSL セキュア サーハおよひクライアントのステーダスを表示するコマン	£ 8-6	SSL セキュア サーバおよびクライアントのステータスを表示するコマ
---	-------	------------------------------------

コマンド	目的
show ip http client secure status	セキュア HTTP クライアントの設定を表示します。
show ip http server secure status	セキュア HTTP サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

SCP のためのスイッチの設定

Secure Copy Protocol (SCP) 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証 方式を提供します。SCP には、Berkeley r-tool に代わるセキュリティの高いアプリケーションおよび プロトコルであるセキュア シェル (SSH) が必要です。

SSH を動作させるには、スイッチに RSA の公開鍵と秘密鍵のペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらの鍵のペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に 設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA 鍵のペアが必要です。

(注)

SCP を使用する場合、コピー コマンドにパスワードを入力することはできません。プロンプトが表示 されたときに、入力する必要があります。

Secure Copy に関する情報

Secure Copy 機能を設定するには、次の概念を理解する必要があります。

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセ キュリティに対応している点を除けば、Remote Copy Protocol (RCP) と類似しています。また、SCP の設定には AAA の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する 必要があります。

適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System (IFS) のファイルをスイッチ に(またはスイッチから)自由にコピーできます。コピーには copy コマンドを使用します。また、許 可されている管理者もこの作業をワークステーションから実行できます。

SCP の設定および検証方法の詳細は、次の URL にアクセスして、Cisco IOS Release 12.2 の『Cisco IOS New Features』から「Secure Copy Protocol」の章を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18. html





IEEE 802.1x ポートベース認証の設定

IEEE 802.1x ポートベース認証は、不正なデバイス(クライアント)によるネットワーク アクセスを防止します。

Catalyst 2960 スイッチ コマンド リファレンスおよび『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」では、コマンドの構文および使用方法について説明していま す。

- 「IEEE 802.1x ポートベース認証の概要」(P.9-1)
- 「802.1x 認証の設定」(P.9-33)
- 「802.1x の統計情報およびステータスの表示」(P.9-68)

IEEE 802.1x ポートベース認証の概要

IEEE 802.1x 規格では、一般の人がアクセス可能なポートからクライアントが LAN に接続しないよう に規制する、クライアント/サーバベースのアクセス制御および認証プロトコルを定めています。認証 サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービス を利用できるようにします。

IEEE 802.1x アクセス制御では、クライアントを認証するまでの間、そのクライアントが接続している ポート経由では Extensible Authentication Protocol over LAN (EAPOL)、Cisco Discovery Protocol (CDP)、および Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) トラフィックしか許可 されません。認証後、通常のトラフィックをポート経由で送受信できます。

- •「デバイスの役割」(P.9-3)
- 「認証プロセス」(P.9-4)
- 「認証の開始およびメッセージ交換」(P.9-6)
- 「認証マネージャ」(P.9-8)
- 「許可ステートおよび無許可ステートのポート」(P.9-11)
- 「802.1x のホストモード」(P.9-12)
- 「マルチドメイン認証」(P.9-13)
- 「802.1x 複数認証モード」(P.9-14)
- 「MAC Move」 (P.9-15)
- 「802.1x アカウンティング」(P.9-15)
- 「802.1x アカウンティング アトリビュート値ペア」(P.9-15)
- 「802.1x 準備状態チェック」(P.9-17)

• 「VLAN 割り当てを使用した 802.1x 認証」(P.9-17)

• 「ユーザ単位 ACL を使用した 802.1x 認証の使用」(P.9-19)

	アクセス不能認証バイパスによる 802.1x 認証」(P.9-24)
	アクセス不能認証バイパスを使用した IEEE 802.1x 認証を使用するには、スイッチが L Base イメージを実行している必要があります。
Ę	音声 VLAN ポートを使用した 802.1x 認証」(P.9-25)
2	ポート セキュリティを使用した 802.1x 認証」(P.9-26)
V	Vake-on-LAN を使用した 802.1x 認証」 (P.9-27)
	Wake-on-LAN を使用した IEEE 802.1x 認証を使用するには、スイッチが LAN Base イ を実行している必要があります。
	AAC 認証バイパスによる 802.1x 認証」(P.9-28)
3	02.1x ユーザ ディストリビューション」 (P.9-29)
	Jetwork Admission Control レイヤ 2 802.1x 検証」 (P.9-29)
	Network Admission Control を使用するには、スイッチが LAN Base イメージを実行し 必要があります。
	柔軟な認証の順序設定」(P.9-30)
	Dpen1x 認証」(P.9-30)
Ĭ	- 音声認識 802.1x セキュリティの使用」(P.9-31)
	Network Edge Access Topology(NEAT)を使用した 802.1x サプリカントおよび認証者」 ?9-31)
	ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証」 (P.9-20)
	ACL および RADIUS Filter-Id アトリビュートを使用した IEEE 802.1x 認証の使用」(P.9

デバイスの役割



802.1x ポートベース認証におけるデバイスの役割

 クライアント: LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答 するデバイス(ワークステーション)。ワークステーションでは、Microsoft Windows XP OS(オ ペレーティング システム)に付属しているような 802.1x 準拠のクライアント ソフトウェアを実行 する必要があります(クライアントは、802.1x標準ではサプリカントといいます)。



Windows XP のネットワーク接続および 802.1x 認証については、次の URL にある「Microsoft Knowledge Base」を参照してください。 http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- 認証サーバ:クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントにLAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol (EAP) 拡張機能を備えた Remote Authentication Dial-In User Service (RADIUS) セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- スイッチ(エッジスイッチまたはワイヤレス アクセス ポイント): クライアントの認証ステータ スに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サー バとの仲介デバイス(プロキシ)として動作し、クライアントに識別情報を要求し、その情報を認 証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセ ル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれて います。(スイッチは、802.1x 標準ではオーセンティケータといいます)。

スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが 取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化 では EAP フレームの変更は行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サー バのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、ク ライアントに送信されます。 仲介デバイスとして動作できるものには、Catalyst 3750-E、Catalyst 3560-E、Catalyst3750、 Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、 Catalyst 2950、Catalyst 2940、またはワイヤレス アクセス ポイントがあります。これらのデバイ スでは、RADIUS クライアントおよび 802.1x 認証をサポートするソフトウェアが稼動している必 要があります。

認証プロセス

802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェ アをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアントMAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている 場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てること ができます。
- RADIUS 認証サーバが使用できず(ダウンしていて)アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

(注)

アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング)失敗ポリシーとも呼ばれます。

図 9-2 に、認証プロセスを示します。



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

• 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

RADIUS サーバを使用する 802.1x 認証を設定した後、スイッチは、Session-Timeout RADIUS ア トリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリ ビュート [29]) に基づいてタイマーを使用します。

Session-Timeout RADIUS アトリビュート (アトリビュート [27]) は、再認証が発生するまでの時間を指定します。

Termination-Action RADIUS アトリビュート (アトリビュート [29]) は、再認証中に行うアク ションを指定します。アクションは Initialize および ReAuthenticate に設定できます。Initialize ア クションが設定されていると (アトリビュートの値は DEFAULT)、802.1x セッションが終了し、 再認証中に接続が切断されます。ReAuthenticate アクションが設定されていると (アトリビュート の値は RADIUS-Request)、再認証中にセッションは影響を受けません。

 クライアントを手動で再認証するには、dot1x re-authenticate interface interface-id 特権 EXEC コマンドを入力します。

Multidomain Authentication (MDA; マルチドメイン認証)がポートでイネーブルにされている場合、 このフローが使用されます。ただし、音声許可の場合はいくつかの例外があります。MDA の詳細につ いては、「マルチドメイン認証」(P.9-13)を参照してください。

認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。authentication port-control auto または dot1x port-control auto インターフェイス コンフィギュレーション コマンドを使用して ポート上で認証をイネーブルにした場合、スイッチはポートのリンク ステートがダウンからアップに 変更した時点で、またはポートが認証されてないままアップの状態であるかぎり定期的に認証を開始し ます。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。ク ライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチ に対し、クライアントの識別情報を要求するように指示します。



ネットワーク アクセス デバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされ ていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証 の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポート が許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、 クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無 許可ステートのポート」(P.9-11)を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が 成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成 功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、 ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが 許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポー ト」(P.9-11)を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 9-3 に、クライアントが RADIUS サーバとの間で OTP (ワンタイム パスワード) 認証方式を使用する際に行われるメッセージ交換を示します。

図 9-3

メッセージ交換



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの 場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証でき ます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS アクセス/要求フレームにこの情報を保存します。サーバがスイッチに RADIUS アクセス/承 認フレームを送信(認証が成功)すると、ポートが許可されます。認証に失敗してゲスト VLAN が指 定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネットパケットの待機 中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、 802.1x 認証を停止します。

図 9-4 に、MAC 認証バイパス中のメッセージ交換を示します。



図 9-4 MAC 認証バイパス中のメッセージ交換

認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、スイッチ上および Catalyst 6000 などの他のネットワーク デ バイス上で、CLI コマンドおよびメッセージなど、同じ認証方法を使用することができず、異なる認証 設定を使用しなければなりませんでした。Cisco IOS Release 12.2(50)SE 以降では、ネットワークのす べての Catalyst スイッチで同じ認証方法を使用できます。

- 「Port-Based 認証方法」(P.9-8)
- 「ユーザ単位 ACL および Filter-Id」(P.9-9)
- 「認証マネージャ CLI コマンド」(P.9-10)

Port-Based 認証方法

表 9-1 に、これらのホスト モードでサポートされている認証方法を示します。

- シングル ホスト:ポートで認証できるデータまたは音声ホスト (クライアント) は1 つだけです。
- マルチホスト:同じポートで複数のデータホストを認証できます(ポートがマルチホストモードで無許可になると、スイッチは接続しているクライアントのネットワークアクセスをすべて禁止します)。
- マルチドメイン認証(MDA):同じスイッチ ポートでデータ デバイスと音声デバイスの両方を認 証できます。ポートはデータ ドメインと音声ドメインに分割されます。
- 複数認証:複数のホストがデータ VLAN で認証できます。このモードでは、音声 VLAN が設定されている場合、VLAN で1 クライアントだけ使用できます。

表 9-1 802.1xの機能

	モード				
認証方法	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²	
802.1x	VLAN 割り当て	VLAN 割り当て	VLAN 割り当て	ユーザ単位 ACL ³	
	ユーザ単位 ACL	ユーザ単位 ACL	ユーザ単位 ACL ³	Filter-Id アトリビュート ³	
	Filter-ID アトリビュート	Filter-ID アトリビュート	Filter-Id アトリビュート ³	ダウンロード可能 ACL ³	
	ダウンロード可能 ACL ³	ダウンロード可能 ACL ⁴	ダウンロード可能 ACL ³	リダイレクト URL ³	
	リダイレクト URL ³	リダイレクト URL ³	リダイレクト URL ³		
MAC 認証	VLAN 割り当て	VLAN 割り当て	VLAN 割り当て	ユーザ単位 ACL ³	
バイパス	ユーザ単位 ACL	ユーザ単位 ACL	ユーザ単位 ACL ³	Filter-Id アトリビュート ³	
	Filter-ID アトリビュート	Filter-ID アトリビュート	Filter-Id アトリビュート ³	ダウンロード可能 ACL ³	
	ダウンロード可能 ACL ³	ダウンロード可能 ACL ³	ダウンロード可能 ACL ³	リダイレクト URL ³	
	リダイレクト URL ³	リダイレクト URL ³	リダイレクト URL ³		
スタンドアロン	Proxy ACL、Filter-Id アト	、リビュート、ダウンロート	「可能 ACL ²		
Web 認証 ⁴	Web 認証 ⁴				

表 9-1 802.1x の機能 (続き)

	モード				
認証方法	シングル ホスト	マルチ ホスト	MDA ¹	複数認証 ²	
NAC レイヤ 2	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	
IP 検証	ダウンロード可能 ACL	ダウンロード可能 ACL	ダウンロード可能 ACL	ダウンロード可能 ACL ³	
	リダイレクト URL	リダイレクト URL	リダイレクト URL	リダイレクト URL ³	
フォールバック	Proxy ACL	Proxy ACL	Proxy ACL	Proxy ACL ³	
メソッドとして の Web 認証 ⁵	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	Filter-Id アトリビュート ³	
	ダウンロード可能 ACL ³	ダウンロード可能 ACL ³	ダウンロード可能 ACL ³	ダウンロード可能 ACL ³	

1. MDA = マルチドメイン認証

2. *multiauth* とも呼ばれます。

3. Cisco IOS Release 12.2(50)SE 以降でサポートされています。

4. Cisco IOS Release 12.2(50)SE 以降でサポートされています。

5. 802.1x 認証をサポートしていないクライアントの場合

ユーザ単位 ACL および Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL および Filter-Id がサポート されているのは、シングル ホスト モードだけでした。Cisco IOS Release 12.2(50) では、MDA および 複数認証(multiauth)をイネーブルにしたポートのサポートが追加されました。12.2(52)SE 以降では、 マルチホスト モードのポートのサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、 Catalyst 6000 スイッチなど、Cisco IOS ソフトウェアを実行する別のデバイスで設定された ACL と互 換性がありませんでした。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行 する他のデバイスで設定された ACL と互換性があります。



any は、ACL の発信元としてだけ設定できます。

(注)

マルチ ホスト モードで設定された ACL では、ステートメントの発信元部分は *any* でなければなりま せん (たとえば、**permit icmp** *any* **host 10.10.1.1**)。

定義された ACL の発信元ポートには any を指定する必要があります。指定しない場合、ACL は適用できず、認証は失敗します。シングル ホストは唯一例外的に後方互換性をサポートします。

複数のホストを MDA がイネーブルにされたポートおよび複数認証ポートで認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。

マルチ ホスト ポートで認証されるホストが1つだけで、他のホストが認証なしでネットワーク アクセ スを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接 続ホストに適用できます。

認証マネージャ CLI コマンド

認証マネージャインターフェイス コンフィギュレーションコマンドは、802.1x、MAC 認証バイパス および Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適 用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能 を制御します。一般的な認証コマンドには、authentication host-mode、authentication violation お よび authentication timer インターフェイス コンフィギュレーション コマンドがあります。

802.1x 固有コマンドは dot1x キーワードで始まります。たとえば、authentication port-control auto インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにし ます。ただし、dot1x system-authentication control グローバル コンフィギュレーション コマンドは 常にグローバルに 802.1x 認証をイネーブルまたはディセーブルにします。

(注)

802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは、以前の 802.1x コマンドと同じ機能を提供します。

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
authentication control-direction {both in}	dot1x control-direction {both in}	Wake-on-LAN(WoL)機能を使用した認証をイ ネーブルにし、ポート制御を単一方向または双方 向に設定します。
authentication event	dot1x auth-fail vlan dot1x critical (interface	ポート上で制限付き VLAN をイネーブルにしま す。
	configuration)	アクセス不能認証バイパス機能をイネーブルにし ます。
		アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback fallback-profile	dot1x fallback fallback-profile	認証をサポートしないクライアント用のフォール バック方法として Web 認証を使用するようポー トを設定します。
authentication host-mode [multi-auth multi-domain multi-host single-host]	dot1x host-mode {single-host multi-host multi-domain}	認可ポートでシングル ホスト(クライアント)ま たはマルチ ホストを許可します。
authentication order	dot1x mac-auth-bypass	使用される認証方法の順序を柔軟に定義できるよ うにします。
authentication periodic	dot1x reauthentication	クライアントの定期的再認証をイネーブルにしま す。
authentication port-control {auto force-authorized force-un authorized}	dot1x port-control {auto force-authorized force-unauthorized}	ポートの許可ステートの手動制御をイネーブルに します。

表 9-2 認証マネージャ コマンドおよび以前の 802.1x コマンド

表 9-2 認証マネージャ コマンドおよび以前の 802.1x コマンド (続き)

Cisco IOS Release 12.2(50)SE	Cisco IOS Release 12.2(46)SE	
以降での認証マネージャ コマンド	以前での同等の 802.1x コマンド	説明
authentication timer	dot1x timeout	タイマーを設定します。
authentication violation {protect	dot1x violation-mode {shutdown	新しいデバイスがポートに接続された場合、また
restrict shutdown}	restrict protect}	は最大数のデバイスがポートに接続された後に新
		しいデバイスがそのポートに接続された場合に発
		生する違反モードを設定します。

詳細については、このリリースのコマンドリファレンスを参照してください。

許可ステートおよび無許可ステートのポート

802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアントア クセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN(仮想 LAN)ポートとして設定されていないポートは 802.1x 認証、CDP、および STPパケットを除くすべ ての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ス テートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLANポートとして設定されている場合、VoIPトラフィックおよび 802.1x プロトコルパケットが許 可されたあとクライアントが正常に認証されます。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼動していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。また、応答がない場合は、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control または dot1x port-control インターフェイス コンフィギュレーション コ マンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- force-authorized: 802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- force-unauthorized: クライアントからの認証の試みをすべて無視し、ポートを無許可ステートの ままにします。スイッチは、ポートを介してクライアントに認証サービスを提供できません。
- auto: 802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC (メディア アクセス制御) アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると(認証サーバから Accept フレームを受信すると)、ポートが許可ス テートに変わり、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可され ます。認証に失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。 認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバか ら応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンクステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信 した場合に、ポートは無許可ステートに戻ります。

802.1x のホスト モード

802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホス トモード(図 9-1 (P.9-3)を参照)では、802.1x 対応のスイッチ ポートに接続できるのはクライアン ト1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレーム を送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライア ントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ス テートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。図 9-5 (P.9-12) に、ワイヤレス LAN における 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると(再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合)、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチ ホスト モードがイネーブルの場合、802.1x 認証を使用してポートおよびポート セキュリティを 認証し、クライアントを含むすべての MAC アドレスのネットワーク アクセスを管理できます。



スイッチはマルチドメイン認証 (MDA)をサポートしています。これにより、データ装置と IP Phone などの音声装置(シスコ製品またはシスコ以外の製品)の両方を同じスイッチ ポートに接続できます。 詳細については、「マルチドメイン認証」(P.9-13)を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証 (MDA)をサポートしています。これにより、データ装置と IP Phone などの音声装置(シスコ製品またはシスコ以外の製品)の両方を同じスイッチ ポート上で認証できます。ポートはデータ ドメインと音声ドメインに分割されます。



MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応の ポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定するには、「ホスト モードの設定」(P.9-44)を参照してください。
- ホストモードがマルチドメインに設定されている場合、IP Phoneの音声 VLAN を設定する必要が あります。詳細は、第13章「VLAN の設定」を参照してください。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。

(注) ダイナミック VLAN を使用して Cisco IOS Release 12.2(37)SE を実行するスイッチの MDA 対応のスイッチ ポートで音声 VLAN を割り当てると、音声デバイス許可が失敗します。

- 音声デバイスを許可するには、値 device-traffic-class=voice の Cisco Attribute-Value (AV; ア トリビュート値)ペア アトリビュートを送信するように AAA サーバを設定する必要があります。 この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータドメインの許可を行おうとすると、errordisableになります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone また は音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバ イスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。 音声デバイスが 音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされま す。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC ア ドレス制限にカウントされません。
- MDA は、フォールバック方法として MAC 認証バイパスを使用して、IEEE 802.1x 認証をサポートしていないデバイスにスイッチポートを接続できます。詳細については、「MAC 認証バイパス」 (P.9-37)を参照してください。
- データまたは 音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが5分間ブロックされたままになります。
- ポートが未認証中に6つ以上のデバイスがデータVLANで検出された場合や、複数の音声デバイスが音声VLANで検出された場合、ポートは errdisable になります。
- ポートのホストモードがシングルホストまたはマルチホストからマルチドメインモードに変更される場合、許可済みのデータデバイスはポートで許可済みのままになります。ただし、ポート音声 VLANの Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。

- ポートがシングルまたはマルチ ホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック方法は設定されたままになります。
- マルチドメインモードからシングルホストまたはマルチホストモードにポートを切り替えると、 ポートからすべての認証済デバイスが削除されます。
- データドメインがまず許可されてゲスト VLAN に配置された場合、IEEE 802.1x 非対応音声デバイスは認証をトリガするために音声 VLAN 上のパケットにタグを付ける必要があります。電話機はタグ付きトラフィックを送信する必要はありません(802.1x 対応電話の場合も同様です)。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーがある許可済 みデバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性が あります。使用する場合、ポート上の1デバイスだけでユーザ単位 ACL が実行されます。

詳細については、「ホストモードの設定」(P.9-44)を参照してください。

802.1x 複数認証モード

複数認証(multiauth)モードでは、データ VLAN で複数のクライアントを認証できます。各ホストは 個別に認証されます。音声 VLAN が設定されている場合、このモードでは、VLAN で1クライアント だけ認証できます(ポートが他の音声クライアントを検出すると、これらはポートから廃棄されます が、違反エラーは発生しません)。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライア ントを認証する必要があります。

802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メ ソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

複数認証ポートで認証できるデータホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは1台だけです。ホスト制限がないため、定義された違反はトリガされません。たとえば、2台目の音声デバイスが検出された場合、これは通知なしで廃棄され、違反はトリガされません。

音声 VLAN の MDA 機能の場合、複数認証モードでは、認証サーバから受け取った VSA に応じて、認 証されたデバイスがデータまたは音声のいずれかの VLAN に割り当てられます。



ポートが複数認証モードの場合、RADIUS サーバにより提供される VLAN 割り当て、ゲスト VLAN、 および認証失敗 VLAN 機能はアクティブになりません。

クリティカル認証モードおよびクリティカル VLAN の詳細については、「アクセス不能認証バイパスに よる 802.1x 認証」(P.9-24)を参照してください。

ポートでの multiauth モードの設定の詳細については、「ホスト モードの設定」(P.9-44) を参照してく ださい。

MAC Move

MAC アドレスがスイッチ ポートで認証されると、そのアドレスは、スイッチの別の 802.1x ポートで は許可されません。スイッチが同じ MAC アドレスを別の 802.1x ポートで検出すると、そのアドレス は許可されなくなります。

場合によっては、MAC アドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、 認証ホストとスイッチ ポート間に別のデバイス(ハブまたは IP Phone など)がある場合、ホストをデ バイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC Move をグローバルにイネーブルにできます。 ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再 認証されます。

MAC Move はすべてのホスト モードでサポートされます (認証ホストは、ポートでイネーブルにされ ているホスト モードに関係なく、スイッチの任意のポートに移動できます)。

(注)

MAC Move はポート セキュリティ対応 802.1x ポートではサポートされません。MAC Move がスイッ チでグローバルに設定されていて、ポート セキュリティ対応ホストが 802.1x 対応のポートに移動され ると、違反エラーが発生します。

詳細については、「MAC Move のイネーブル化」(P.9-51)を参照してください。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次のアクティビティを 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログオフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1x アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設 定する必要があります。

802.1x アカウンティング アトリビュート値ペア

RADIUS サーバに送信された情報は、アトリビュート値(AV)ペアの形式で表示されます。これらの AVペアのデータは、各種アプリケーションによって使用されます(たとえば課金アプリケーションの 場合、RADIUSパケットの Acct-Input-Octets または Acct-Output-Octets アトリビュートの情報が必要 です)。 AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の 種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START:新規ユーザ セッションが始まると送信されます。
- INTERIM:既存のセッションが更新されると送信されます。
- STOP:セッションが終了すると送信されます。

次の表 9-3 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 9-3 アカウンティング AV ペア

アトリビュート番号	AV ペア名	START	INTERIM	STOP
アトリビュート [1]	User-Name	常時送信	常時送信	常時送信
アトリビュート [4]	NAS-IP-Address	常時送信	常時送信	常時送信
アトリビュート [5]	NAS-Port	常時送信	常時送信	常時送信
アトリビュート [8]	Framed-IP-Address	非送信	条件に応じ て送信 ¹	条件に応じ て送信 ¹
アトリビュート[25]	Class	常時送信	常時送信	常時送信
アトリビュート[30]	Called-Station-ID	常時送信	常時送信	常時送信
アトリビュート[31]	Calling-Station-ID	常時送信	常時送信	常時送信
アトリビュート[40]	Acct-Status-Type	常時送信	常時送信	常時送信
アトリビュート[41]	Acct-Delay-Time	常時送信	常時送信	常時送信
アトリビュート[42]	Acct-Input-Octets	非送信	常時送信	常時送信
アトリビュート[43]	Acct-Output-Octets	非送信	常時送信	常時送信
アトリビュート[44]	Acct-Session-ID	常時送信	常時送信	常時送信
アトリビュート[45]	Acct-Authentic	常時送信	常時送信	常時送信
アトリビュート [46]	Acct-Session-Time	非送信	常時送信	常時送信
アトリビュート[49]	Acct-Terminate-Cause	非送信	非送信	常時送信
アトリビュート[61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol (DHCP) バインディングが DHCP ス ヌーピング バインディング テーブルに存在している場合にのみ、Framed-IP-Address の AV ペ アは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力するこ とで表示できます。このコマンドの詳細については、次の URL で『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/122debug.html

AV ペアの詳細については、RFC 3580 『802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

802.1x 準備状態チェック

(注)

802.1x 準備状態チェックを使用するには、スイッチが LAN Base イメージを実行している必要があります。

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティを監視し、802.1x を サポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサ ポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサプリカントで NOTIFY EAP 通知パケットでのクエリーがサ ポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりま せん。

802.1x 準備状態チェックのスイッチの設定については、「802.1x 準備状態チェックの設定」(P.9-38) を参照してください。

VLAN 割り当てを使用した 802.1x 認証

RADIUS サーバは、VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ デー タベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントの ユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アク セスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされ ます。Cisco IOS Release 12.2(40)SE 以降では、音声デバイスが許可され、RADIUS サーバが許可済み VLAN を返すと、ポートの音声 VLAN が、割り当てられた音声 VLAN のパケットを送受信するよう に設定されます。音声 VLAN 割り当ては、マルチドメイン認証(MDA)対応のポートでのデータ VLAN 割り当てと同じように機能します。詳細については、「マルチドメイン認証」(P.9-13)を参照 してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認 証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポー トに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に 所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済の VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、間違った VLAN ID、存在しない VLAN ID、RSPAN VLAN、シャットダウンし ている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホ スト ポートの場合、設定エラーには、設定済または割り当て済 VLAN ID と一致するデータ VLAN の割り当て試行(またはその逆)のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホ ストと同じ VLAN (RADIUS サーバにより指定) に配置されます。

- ポートセキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には 影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済の音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、その ポートのアクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポー トが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
 - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済または割り当て済の VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済の VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメインホストモードがディセーブルになります。
 - ・ 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声
 VLAN 設定を削除したり設定値を dot1p または untagged に修正したりすると、音声デバイス
 が未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可(force-authorized)ステート、強制無許可(force-unauthorized)ステート、無許 可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセス VLAN に配置され ます。

トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server (VMPS; VLAN メ ンバシップ ポリシー サーバ) によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て 機能を使用した 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- network キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインター フェイス設定を可能にします。
- 802.1x 認証をイネーブルにします (アクセス ポートで 802.1x 認証を設定すると、VLAN 割り当 て機能は自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネルアトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに返す必要があります。
 - [64] Tunnel-Type = VLAN
 - [65] Tunnel-Medium-Type = 802
 - [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID または VLAN-Group
 - [83] Tunnel-Preference

アトリビュート [64] は、値 VLAN (タイプ 13) でなければなりません。アトリビュート [65] は、 値 802 (タイプ 6) でなければなりません。アトリビュート [81] は、802.1x 認証ユーザに割り当て られた VLAN 名または VLAN ID を指定します。

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するス イッチ設定」(P.8-36)を参照してください。

ユーザ単位 ACL を使用した 802.1x 認証の使用

ユーザ単位アクセス コントロール リスト (ACL) をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザに提供できます。RADIUS サーバは、802.1x ポートに接 続されるユーザを認証する場合、ユーザ ID に基づいて ACL アトリビュートを受け取り、これらをス イッチに送信します。送信されたアトリビュートは、ユーザ セッション期間中、802.1x ポートに適用 されます。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユー ザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーション には保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する 場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。 他のポートで受信した着信のルーティング パケットには、ルータ ACL のフィルタが適用されます。発信 するルーティング パケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛 盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、Vendor-Specific Attribute (VSA; ベンダー固有属性) などのユーザ単位アトリビュート をサポートします。ベンダー固有属性 (VSA) は、オクテット ストリング形式で、認証プロセス中に スイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<n>で、出力方 向では outacl#<n>です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限り サポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細は、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザ単位コンフィギュレーションを 定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただ し、Filter-Id アトリビュートを使用する場合、標準 ACL を示すことができます。

Filter-Id アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定で きます。アトリビュートには、ACL 番号と、その後に入力フィルタリングか出力フィルタリングを示 す.*in* または.*out* が含まれています。RADIUS サーバが.*in* または.*out* 構文を許可しない場合、アクセ スリストはデフォルトで発信 ACL に適用されます。スイッチ上では Cisco IOS アクセス リストのサ ポートは限定されているため、Filter-Id アトリビュートは番号が 1 ~ 199 および 1300 ~ 2699 までの IP ACL (IP 標準 ACL と IP 拡張 ACL) でだけサポートされています。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大 サイズにより制限されます。

ベンダー固有属性の例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」(P.8-36)を参照してください。ACL の設定の詳細については、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。



ユーザ単位 ACL がサポートされるのはシングル ホスト モードだけです。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- network キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインター フェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。

設定の詳細については、「認証マネージャ」(P.9-8)を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもで きます。



ダウンロード可能な ACL は dACL とも呼ばれます。

ホストモードがシングルホスト、MDA、または複数認証モードの場合、スイッチは、ACLの送信元 アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。音声 VLAN ポートでは、スイッチは、ACL を電話機だけに適用します。



ダウンロード可能な ACL またはリダイレクト URL が認証サーバのクライアントに設定される場合、 接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

リダイレクト URL の Cisco Secure ACS およびアトリビュート値ペア

スイッチはこれらの cisco-av-pair VSA を使用します。

- url-redirect は HTTP to HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL AV ペアを使用して、エンドポイント デバイスからの HTTP または HTTPS リクエストを代行受信します。スイッチは、クライアント Web ブラウザを指定された リダイレクト アドレスに転送します。Cisco Secure ACS の url-redirect AV ペアには、Web ブラウザが リダイレクトされる URL が含まれます。url-redirect-acl AV ペアには、リダイレクトする HTTP また は HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL の permit ACE と一致 するトラフィックがリダイレクトされます。



スイッチの URL リダイレクト ACL およびデフォルト ポート ACL を定義します。

リダイレクト URL が認証サーバのクライアントに設定される場合、接続されるクライアント スイッチ ポートのデフォルト ポート ACL も設定する必要があります。

ダウンロード可能な ACL の Cisco Secure ACS およびアトリビュート値ペア

RADIUS の cisco-av-pair ベンダー固有属性(VSA)を使用すると、Cisco Secure ACS で CiscoSecure-Defined-ACL アトリビュート値(AV)ペアを設定できます。このペアは、 #ACL#-IP-name-number アトリビュートで Cisco Secure ACS のダウンロード可能な ACL の名前を指 定します。

- *name* は ACL の名前です。
- number はバージョン番号(たとえば 3f783768)です。

ダウンロード可能な ACL が認証サーバのクライアントに設定される場合、接続されるクライアント ス イッチ ポートのデフォルト ポート ACL も設定する必要があります。

デフォルト ACL がスイッチで設定されている場合、Cisco Secure ACS がホスト アクセス ポリシーを スイッチに送信すると、スイッチは、スイッチ ポートに接続されるホストからのトラフィックにこの ポリシーを適用します。ポリシーが適用されない場合、デフォルト ACL が適用されます。Cisco Secure ACS がダウンロード可能な ACL をスイッチに送信する場合、この ACL は、スイッチ ポートに 設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホス ト アクセス ポリシーを受信し、デフォルト ACL が設定されていない場合、許可失敗が宣言されます。

設定の詳細については、「認証マネージャ」(P.9-8) および「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定」(P.9-63) を参照してください。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、 VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されてい る場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS (Microsoft) RADIUS サー バに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバで使用することで、ネットワークで一定数の VLAN を使用できます。

この機能を使用すると、STP により監視および処理される VLAN の数も制限されます。ネットワークは、固定 VLAN として管理できます。



この機能は Cisco ACS Server ではサポートされていません (ACS サーバは、新しいホストに送信される VLAN-ID を無視して、MAC アドレスに基づいた認証だけを行います)。

設定情報については、「VLAN ID ベース MAC 認証の設定」(P.9-65)を参照してください。追加設定 は、同様の MAC 認証バイパスです(「MAC 認証バイパスの設定」(P.9-58)を参照してください)。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます (802.1x クライアントのダウンロードなど)。これらのクライアントは 802.1x 認証用にシ ステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは、EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインター フェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1x 対 応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インター フェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットが インターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認 証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンド シーケンスを使用します。

- dot1x guest-vlan supplicant グローバル コンフィギュレーション コマンドを入力して、ゲスト VLAN へのアクセスを許可します。
- shutdown インターフェイス コンフィギュレーション コマンドを入力し、さらに no shutdown イ ンターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。



インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可され ます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、 ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、シングル ホスト モードおよびマルチ ホスト モードの 802.1x ポート上でサポートさ れます。

RSPAN VLAN または音声 VLAN を除くあらゆるアクティブ VLAN を、802.1x ゲスト VLAN として 設定できます。ゲスト VLAN 機能は、トランク ポートではサポートされていません。アクセス ポート 上でのみサポートされます。

スイッチは *MAC 認証バイパス*をサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの 場合、スイッチは、802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クラ イアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のク ライアントを検出した後で、クライアントからのイーサネット パケットを待機します。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス/要求フレームを認証 サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可 します。認証に失敗した場合、ゲスト VLAN が指定されていれば、スイッチはポートをゲスト VLAN に割り当てます。詳細については、「MAC 認証バイパスによる 802.1x 認証」(P.9-28) を参照してくだ さい。

詳細については、「ゲスト VLAN の設定」(P.9-52)を参照してください。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、ス イッチの各 802.1x ポートに対して制限付き VLAN (認証失敗 VLAN と呼ばれることもあります)を設 定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効な証明書を持ってい ないユーザ(通常、企業にアクセスするユーザ)に、サービスを制限したアクセスを提供できます。管 理者は制限付き VLAN のサービスを制御できます。

(注)

両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じ に設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがス パニング ツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能 を使用することで、クライアントの認証試行回数を指定し(デフォルト値は3回)、一定回数後にス イッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を 超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。 ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます(デフォルトは 60 秒)。再認証に失敗している 間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルに することもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しないか ぎり、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再 認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の擬似メッセージがクライアントに送信されます。 このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントに よっては(Windows XP が稼動しているデバイスなど)、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1x ポート上でシングル ホスト モードの場合だけサ ポートされます。

RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定でき ます。制限付き VLAN 機能は、トランク ポートではサポートされていません。アクセス ポート上での みサポートされます。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポー ト セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、また はセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、errordisable ステー トに移行します。

ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査、DHCP スヌーピン グ、および IP 送信元ガードのような他のポート セキュリティ機能は、制限付き VLAN に対して個別 に設定できます。

詳細については、「制限付き VLAN の設定」(P.9-53)を参照してください。

アクセス不能認証バイパスによる 802.1x 認証

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または AAA 失敗ポリシーとも呼ばれます。これらのホストをクリティカル ポートに接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートに接続しようとすると、そのホストはユーザ指定のアクセス VLAN、クリティカル VLAN に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカル ポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバのステータスをチェックします。利用可能なサーバが1つあれば、スイッチはホスト を認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへの ネットワーク アクセスを許可して、ポートを認証ステートの特別なケースである*クリティカル認証*ス テートにします。

複数認証ポートのサポート

複数認証(multiauth) ポートでのアクセス不能バイパスをサポートするには、authentication event server dead action reinitialize vlan *vlan-id* を使用できます。新しいホストがクリティカル ポートに接続しようとすると、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

authentication event server dead action reinitialize vlan *vlan-id* インターフェイス コンフィギュレー ション コマンドは、すべてのホスト モードでサポートされています。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべての サーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在のVLAN(事前に RADIUS サーバ により割り当てられた)でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、ス イッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動す るように、クリティカル ポートを設定できます。このように設定した場合、クリティカル認証ステー トのすべてのクリティカル ポートは自動的に再認証されます。詳細については、このリリースのコマ ンドリファレンスおよび「アクセス不能認証バイパス機能の設定」(P.-55)を参照してください。

機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN: アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
 - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも1つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
 - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN: ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1x アカウンティング: RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN: プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN: アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer (RSPAN): アクセス不能認証バイパスの RADIUS 設定または ユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを 伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートに関わらず、IP Phone は音声トラフィックに対して VVID を使用します。これ により、IP Phone は 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。 マルチ ホスト モードでは、 サプリカントが PVID で認証されたあと、追加のクライアントがトラフィックを音声 VLAN 上で送信 できます。 マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影 響します。 リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージ を受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け 取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、 スイッチは直接接続されている1台の IP Phone のみを認識します。音声 VLAN ポートで 802.1x 認証 がイネーブルの場合、スイッチは2ホップ以上離れた認識されない IP Phone からのパケットを廃棄し ます。

802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。

(注)

音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで 802.1x 認証をイネーブ ルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、第15章「音声 VLAN の設定」を参照してください。

ポート セキュリティを使用した 802.1x 認証

シングル ホスト モードまたはマルチ ホスト モードのどちらでもポート セキュリティを備えた 802.1x ポートを設定できます (switchport port-security インターフェイス コンフィギュレーション コマン ドを使用してポートにポート セキュリティを設定する必要があります)。ポートでポート セキュリティ および 802.1x 認証をイネーブルに設定すると、802.1x 認証はそのポートを認証し、ポート セキュリ ティはそのクライアントを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。 この場合、802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限 できます。

次に、スイッチ上での802.1x認証とポートセキュリティ間における相互関係の例を示します。

クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

クライアントが認証されて、ポート セキュリティが手動で設定された場合、セキュア ホスト テー ブル内のエントリは保証されます (ポート セキュリティのスタティック エージングがイネーブル になっていない場合)。

クライアントが認証されてもポート セキュリティ テーブルがいっぱいの場合、セキュリティ違反 が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセ キュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントの アドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内でのエントリ は他のホストに取って代わられます。

最初に認証されたホストが原因でセキュリティ違反が発生すると、ポートは errdisable ステートに なり、ただちにシャットダウンします。

セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細に ついては、「セキュリティ違反」(P.23-11)を参照してください。

- no switchport port-security mac-address mac-address インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから 802.1x クライアント アドレスを手動で削除する場合、dot1x re-authenticate interface interface-id 特権 EXEC コマンドを使用して、802.1x クライアントを再認証する必要があります。
- 802.1x クライアントがログオフすると、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュアホストテーブル内のダイナミックエントリがすべてクリアされます。ここで通常の認証が実行されます。

- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュアホストテーブルから削除されます。
- シングルホストモードまたはマルチホストモードのいずれの場合でも、802.1x ポート上でポート セキュリティと音声 VLAN を同時に設定できます。ポートセキュリティは、Voice VLAN Identifier (VVID)および Port VLAN Identifier (PVID)の両方に適用されます。
- ポートが 802.1x 対応のポートに接続したとき、または認証されるデバイス数が最大数に達したときにポートがシャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットの廃棄するように、authentication violation または dot1x violation-mode インターフェイス コンフィギュレーション コマンドを設定できます。詳細については、「ポートあたりのデバイスの最大数」(P.9-37) およびこのリリースのコマンド リファレンスを参照してください。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」 (P.23-9)を参照してください。

Wake-on-LAN を使用した 802.1x 認証

(注)

Wake-on-LAN を使用した IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

802.1x 認証の Wake-on-LAN (WoL)機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1x ポートを通じて接続され、ホストの電源がオフになると、802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、 WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくな るため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1x 認証を使用している場合、スイッチはマジック パケットを 含むトラフィックを無許可の 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケッ トをネットワーク内にある他のデバイスに送信できません。

(注)

PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in または dot1x control-direction in インターフェイス コンフィギュ レーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニング ツリー フォ ワーディング ステートに変わります。ポートはパケットをホストに送信できますが、ホストからパ ケットを受信できません。

authentication control-direction both または **dot1x control-direction both** インターフェイス コン フィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方 向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスによる 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレス(図 9-2 (P.9-5) を参照) に基づいて クライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続さ れた 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、802.1x ポート上のクライアントを検出した後 で、クライアントからのイーサネット パケットを待機します。スイッチは MAC アドレスに基づいて、 ユーザ名とパスワードとともに RADIUS アクセス/要求フレームを認証サーバに送信します。認証に 成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場 合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そ のインターフェイスに接続されているデバイスが 802.1x 対応サプリカントであることを確認し、 (MAC 認証バイパス機能ではなく) 802.1x 認証を使用してインターフェイスを認証します。インター フェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1x サプリカントを検出してい る場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、 Termination-Action RADIUS アトリビュート値が DEFAULT であるために前のセッションが終了した 場合、スイッチは優先再認証プロセスとして 802.1x 認証を使用します。

MAC 認証バイパスを使用して許可されたクライアントを再認証できます。再認証プロセスは、802.1x を 使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てら れた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に 失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS アトリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリビュート [29]) に基づいており、Termination-Action RADIUS アト リビュート (アトリビュート [29]) のアクションが *Initialize (初期化)* される場合 (アトリビュート 値が *DEFALUT*)、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC 認証バイパス機能が 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用 して再認証を開始します。AV ペアの詳細については、RFC 3580 『802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- 802.1x 認証: 802.1x 認証がポートでイネーブルの場合にだけ MAC 認証バイパスをイネーブルに できます。
- ゲスト VLAN: クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されてい れば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN: 802.lx ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポートセキュリティ:「ポートセキュリティを使用した 802.1x 認証」(P.9-26)を参照してください。
- 音声 VLAN : 「音声 VLAN ポートを使用した 802.1x 認証」(P.9-25) を参照してください。
- VLAN メンバシップ ポリシー サーバ (VMPS): 802.1x および VMPS は相互に排他的です。
- プライベート VLAN: クライアントをプライベート VLAN に割り当てられます。

設定の詳細については、「認証マネージャ」(P.9-8)を参照してください。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザ のロードバランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定され ます。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユー ザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することで ロードバランシング行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユー ザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、 選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

(注) RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合せて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも1つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされ ませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザ はクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

詳細については、「802.1x ユーザディストリビューションの設定」(P.9-59)を参照してください。

Network Admission Control レイヤ 2 802.1x 検証

(注)

Network Admission Control を使用するには、スイッチが LAN Base イメージを実行している必要があります。

スイッチは、デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライア ントのウィルス対策の状態または*ポスチャ*をチェックする Network Admission Control (NAC) レイヤ 2 802.1x 検証をサポートしています。NAC レイヤ 2 802.1x 検証を使用すると、次の作業を実行できま す。

 Session-Timeout RADIUS アトリビュート (アトリビュート [27]) と Termination-Action RADIUS アトリビュート (アトリビュート [29]) を認証サーバからダウンロードします。

- Session-Timeout RADIUS アトリビュート (アトリビュート [27])の値として再認証試行間の秒数 を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS アトリビュート (アトリビュート [29])を使用してクラ イアントを再認証する際のアクションを設定します。値が DEFAULT であるか、値が設定されてい ない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID (アトリビュート [81])の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference (アトリビュート [83])の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID (アトリビュート [81])アトリビュートがリストから選択されます。
- show authentication または show dot1x 特権 EXEC コマンドを使用して、クライアントのポス チャを表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があること を除いて、802.1x ポートベース認証と似ています。NAC レイヤ 2 802.1x 検証の設定に関する詳細につ いては、「NAC レイヤ 2 802.1x 検証の設定」(P.9-60)および「定期的な再認証の設定」(P.9-45)を参 照してください。

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

設定の詳細については、「認証マネージャ」(P.9-8)を参照してください。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときに使用する方法の順序を設定 できます。MAC認証バイパスおよび802.1xは、プライマリまたはセカンダリ認証方法として使用し、 Web認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用 できます。詳細については、「柔軟な認証の順序設定」(P.9-66)を参照してください。

Open1x 認証

Open1x 認証を使用すると、デバイスは認証前にポートにアクセスできます。オープン認証が設定されている場合、ポートの新しいホストは、トラフィックにスイッチを送信することだけが許可されます。 ホストが認証されると、RADIUSサーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングルホストモードでのオープン認証:1人のユーザだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証:音声ドメインの1人のユーザだけ、およびデータドメインの1人のユーザだけが許可されます。
- マルチホストモードでのオープン認証:任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証: MDA の場合と似ていますが、複数のホストを認証できます。

詳細については、「ホスト モードの設定」(P.9-44)を参照してください。
音声認識 802.1x セキュリティの使用

(注)

音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースで は、データ クライアントを認証しようとしてセキュリティ違反が発生すると、ポート全体がシャット ダウンされ、接続が完全に切断されていました。

この機能は、PC が IP Phone に接続されている場合に使用できます。この機能を使用した場合、データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされ、音声 VLAN のトラフィックは中断することなく処理を続行できます。

音声認識 802.1x セキュリティの設定については、「音声認識 802.1x セキュリティの設定」(P.9-39)を 参照してください。

Network Edge Access Topology (NEAT) を使用した 802.1x サプリカ ントおよび認証者

Network Edge Access Topology (NEAT)機能は、ワイヤリング クローゼット (会議室など)外の領 域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

802.1x スイッチ サプリカント: 802.1x サプリカント機能を使用することで、別のスイッチのサプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリングクローゼット外にあり、トランクポートを介してアップストリームスイッチに接続される場合に役に立ちます。802.1x スイッチサプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリームスイッチで認証します。

サプリカント スイッチが認証に成功すると、ポート モードがアクセスからトランクに変更されま す。

アクセス VLAN は、認証者スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

1 つ以上のサプリカント スイッチに接続する認証者スイッチ インターフェイスで MDA または multiauth モードをイネーブルにできます。マルチホスト モードは認証者スイッチ インターフェイスで はサポートされていません。

すべてのホスト モードで機能するように dot1x supplicant force-multicast グローバル コンフィギュ レーション コマンドを Network Edge Access Topology (NEAT) のサプリカント スイッチで使用しま す。

- ホスト許可:許可済み(サプリカントでスイッチに接続する)ホストからのトラフィックだけが ネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol (CISP)を使用して、サプリカントスイッチに接続する MAC アドレスを認証者スイッチに送信し ます(図 9-6 を参照してください)。
- 自動イネーブル化:認証者スイッチでのトランク コンフィギュレーションを自動的にイネーブル 化します。これにより、サプリカント スイッチから着信する複数の VLAN のユーザ トラフィック が許可されます。ACS で cisco-av-pair を device-traffic-class=switch として設定します (この設 定は group または user 設定で行うことができます)。



注意事項

- NEAT ポートは、他の認証ポートと同じコンフィギュレーションで設定できます。サプリカント スイッチが認証すると、ポートモードはベンダー固有属性(VSA)に基づいてアクセスからトラ ンクに変更されます(device-traffic-class=switch)。
- VSA は認証者スイッチ ポート モードをアクセスからトランクに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします(任意の VLAN がネイティブトランク VLAN に変換される場合)。VSA はサプリカントのポート コンフィギュレーションは変更しません。
- ホストモードを変更して、認証者スイッチポートの標準ポートコンフィギュレーションを適用するには、スイッチ VSA ではなく、AutoSmart ポートユーザ定義マクロを使用することもできます。これにより、認証者スイッチポートでサポートされていないコンフィギュレーションを削除して、ポートモードをアクセスからトランクに変更できます。詳細については、第12章「AutoSmartPortマクロの設定」を参照してください。

詳細については、「NEAT での認証者およびサプリカント スイッチの設定」(P.9-61)を参照してください。

ACL および RADIUS Filter-ld アトリビュートを使用した IEEE 802.1x 認 証の使用

<u>》</u> (注)

ACL および *Filter-Id* アトリビュートを使用した IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

スイッチは、入力ポートの IP 標準および IP 拡張ポートのアクセス コントロール リスト (ACL) の両 方をサポートします。

- 設定する ACL
- Access Control Server (ACS) からの ACL

シングル ホスト モードでの IEEE 802.1x ポートは、ACS からの ACL を使用して、異なるレベルの サービスを IEEE 802.1x 認証ユーザに提供します。RADIUS サーバは、このタイプのユーザおよび ポートを認証する場合、ユーザ ID に基づいた ACL アトリビュートをスイッチに送信します。送信さ れたアトリビュートは、ユーザ セッション期間中、ポートに適用されます。セッションが終了、認証 が失敗、またはリンクで故障が発生した場合、ポートは無許可になり、スイッチは ACL をポートから 削除します。

ACS からの IP 標準および IP 拡張ポート ACL だけが Filter-Id アトリビュートをサポートします。これは ACL の名前または番号を指定します。Filter-id アトリビュートは、方向(インバウンドまたはアウトバウンド)、およびユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id アトリビュートは、グループの Filter-Id アトリビュートよりも優先されます。
- ACS からの Filter-Id アトリビュートが、すでに設定されている ACL を指定する場合、これは、 ユーザ設定 ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id アトリビュートを送信する場合、最後のアトリビュートだけが 適用されます。

Filter-Id アトリビュートがスイッチで定義されていない場合、認証が失敗し、ポートが無許可ステート に戻ります。

802.1x 認証の設定

ここでは、次の設定情報について説明します。

- 「802.1x 認証のデフォルト設定」(P.9-34)
- 「802.1x 認証設定時の注意事項」(P.9-35)
- 「802.1x 準備状態チェックの設定」(P.9-38)(任意)
- 「音声認識 802.1x セキュリティの設定」(P.9-39)(任意)
- 「802.1x 違反モードの設定」(P.9-40)(任意)
- 「スイッチおよび RADIUS サーバ間の通信の設定」(P.9-43)(必須)
- 「ホストモードの設定」(P.9-44)(任意)
- 「定期的な再認証の設定」(P.9-45)(任意)
- 「ポートに接続するクライアントの手動での再認証」(P.9-46)(任意)
- 「待機時間の変更」(P.9-47)(任意)
- •「スイッチからクライアントへの再送信時間の変更」(P.9-48)(任意)

- •「スイッチからクライアントへのフレーム再送信回数の設定」(P.9-49)(任意)
- 「再認証回数の設定」(P.9-50)(任意)
- 「802.1x アカウンティングの設定」(P.9-51)(任意)
- 「MAC Move のイネーブル化」(P.9-51)(任意)
- 「ゲスト VLAN の設定」(P.9-52)(任意)
- 「制限付き VLAN の設定」(P.9-53)(任意)
- 「アクセス不能認証バイパス機能の設定」(P.9-55)(任意)
- 「WoL を使用した 802.1x 認証の設定」(P.9-57)(任意)
- 「MAC 認証バイパスの設定」(P.9-58)(任意)
- 「NAC レイヤ 2 802.1x 検証の設定」(P.9-60)(任意)
- 「NEAT での認証者およびサプリカント スイッチの設定」(P.9-61)
- 「ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定」(P.9-63)
- 「柔軟な認証の順序設定」(P.9-66)
- 「ポート上での 802.1x 認証のディセーブル化」(P.9-67)(任意)
- 「802.1x 認証設定のデフォルト値へのリセット」(P.9-68)(任意)

802.1x 認証のデフォルト設定

表 9-4 に、802.1x 認証のデフォルト設定を示します。

表 9-4 802.1x 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル (force-authorized)
	ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィッ クを送受信します。
Authentication, Authorization, Accounting	ディセーブル
(AAA; 認証、許可、アカウンティング)	
RADIUS サーバ	
・ IP アドレス	 指定なし
 UDP 認証ポート 	• 1812
• 鍵	 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔(秒)	3600 秒
再認証回数	2回(ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開 する回数)
待機時間	60 秒(スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数)

表 9-4 802.1x 認証のデフォルト設定 (続き)

機能	デフォルト設定
再送信時間	30 秒 (スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数)
最大再送信回数	2回(スイッチが認証プロセスを再開する前に、EAP-Request/Identityフレームを送信する回数)
クライアント タイムアウト時間	30 秒(認証サーバからの要求をクライアントにリレーするとき、スイッチが 返答を待ち、クライアントに要求を再送信するまでの時間)
認証サーバ タイムアウト時間	30 秒(クライアントからの応答を認証サーバにリレーするとき、スイッチが 応答を待ち、応答をサーバに再送信するまでの時間)
	このタイムアウト時間は、authentication timer server または dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用し て変更できます。
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
認証者(スイッチ)モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

802.1x 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1x 認証」(P.9-35)
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」(P.9-36)
- 「MAC 認証バイパス」(P.9-37)
- 「ポートあたりのデバイスの最大数」(P.9-37)

802.1x 認証

- IEEE 802.1x 認証をイネーブルにすると、他のレイヤ2機能がイネーブルになる前に、ポートが認 証されます。
- 802.1x 対応ポートのモードを(たとえばアクセスからトランクに)変更しようとしても、エラー メッセージが表示され、ポートモードは変更されません。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチ には影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てら れ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される 場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャッ トダウンまたは削除されたあと、ポートは無許可になります。

- IEEE 802.1x プロトコルは、レイヤ2のスタティックアクセス ポートおよび音声 VLAN ポート上 ではサポートされますが、次のポート タイプではサポートされません。
 - トランクポート:トランクポート上で802.1x認証をイネーブルにしようとすると、エラーメッセージが表示され、802.1x認証はイネーブルになりません。802.1x対応ポートのモードをトランクに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
 - ダイナミックポート:ダイナミックモードのポートは、ネイバとトランクポートへの変更を ネゴシエートする場合があります。ダイナミックポートで802.1x認証をイネーブルにしよう とすると、エラーメッセージが表示され、802.1x認証はイネーブルになりません。802.1x対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、 ポートモードは変更されません。
 - ダイナミック アクセス ポート:ダイナミック アクセス (VLAN Query Protocol [VQP]) ポートで 802.1x 認証をイネーブルにしようとすると、エラーメッセージが表示され、802.1x 認証 はイネーブルになりません。802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。
 - EtherChannel ポート:アクティブまたはアクティブでない EtherChannel メンバーを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしよ うとすると、エラー メッセージが表示され、802.1x 認証はイネーブルになりません。
 - Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN; リモート SPAN) 宛先ポート: SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛 先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、dot1x system-auth-control グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されて いるインターフェイスから、EtherChannel の設定を削除してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り 当ての場合、VLAN 割り当て機能を使用した 802.1x 認証はサポートされません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定で きます。ゲスト VLAN 機能は、トランク ポートではサポートされていません。アクセス ポート上 でのみサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時 間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を減らしてください (authentication timer inactivity または dot1x timeout quiet-period および authentication timer reauthentication または dot1x timeout tx-period インターフェイス コンフィギュレーション コマ ンド)。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。

- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
 - この機能はシングルホストモードおよびマルチホストモードの802.1x ポートでサポートされます。
 - Windows XP を稼動しているクライアントに接続されたポートがクリティカル認証ステートの 場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
 - Windows XP クライアントに DHCP が設定されていて、DHCP サーバからの IP アドレスを持 つ場合、クリティカル ポート上で EAP 成功メッセージを受信すると、DHCP 設定プロセスが 再始動しない場合があります。
 - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッ チが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバ が利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制 限付き VLAN に残ります。
 - 同じスイッチポート上にアクセス不能バイパス機能とポートセキュリティを設定できます。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定 できます。制限付き VLAN 機能は、トランク ポートではサポートされていません。アクセス ポー ト上でのみサポートされます。

MAC 認証バイパス

- 特に明記していない限り、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。詳細 については、「802.1x 認証」(P.9-35)を参照してください。
- ポートが MAC アドレスで許可されたあとに、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが無許可ステートでクライアント MAC アドレスが認証サーバ データベースにない場合、 ポートは無許可ステートのままになります。ただし、クライアント MAC アドレスがデータベース に追加された場合、スイッチは MAC 認証バイパスを使用してポートを再認証できます。
- ポートが許可ステートである場合、再認証が発生するまでポートのステートは変わりません。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は1~65535秒です。タイムアウト値を設定する前にポートセキュリティをイネーブルにする必要があります。詳細については、「ポートセキュリティの設定」(P.23-9)を参照してください。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングルホストモードの場合、アクセス VLAN で接続できるデバイスは1台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限 はありません。
- マルチドメイン認証(MDA)モードの場合、アクセス VLAN で1台のデバイス、音声 VLAN で1台の IP Phone が許可されます。
- マルチホストモードの場合、1台の802.1xサプリカントだけがポートで許可されます。ただし、 アクセス VLAN で許可される802.1x 非対応ホストの数には制限はありません。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティを監視し、802.1x を サポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、dot1x force-unauthorized として設定されるポートでは使用できません。

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに dot1x test eapol-capable 特権 EXEC コマンドを使用すると、ス イッチ スタックのすべてのポートがテストされます。
- dot1x test eapol-capable コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、 ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答す ると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x に対応していません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト(たとえば、IP Phone に接続される PC)を扱うポートに送信 できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアント に生成されます。

スイッチ上で 802.1x 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行 します。

	コマンド	目的	
ステップ 1	dot1x test eapol-capable [interface	スイッ	チ上で 802.1x 準備状態チェックをイネーブルにします。
	interface-id]	(任意) トを指;	<i>interface-id</i> には、802.1x 準備状態チェックを実行するポー 定します。
		(注)	オプションの interface キーワードを省略した場合、スイッチ のすべてのインターフェイスがテストされます。
ステップ 1	configure terminal	(任意)	グローバル コンフィギュレーション モードを開始します。
ステップ 2	dot1x test timeout timeout	(任意) 指定で:	EAPOL 応答の待機に使用するタイムアウトを設定します。 きる範囲は 1 ~ 65535 秒です。デフォルト値は 10 秒です。
ステップ 3	end	(任意)	特権 EXEC モードに戻ります。
ステップ 4	show running-config	(任意)	変更したタイムアウト値を確認します。

次の例では、スイッチ上の準備状態チェックをイネーブルにして、ポートを照会する方法を示します。 また、照会済みポートから受信した応答も示し、接続しているデバイスが 802.1x 対応であることを確 認します。

switch# dot1x test eapol-capable interface gigabitethernet0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is EAPOL capable

音声認識 802.1x セキュリティの設定

(注)

音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータ または音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接 続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、デー タ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで 送受信されます。

スイッチで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

 errdisable detect cause security-violation shutdown vlan グローバル コンフィギュレーションコ マンドを入力して、音声認識 802.1x セキュリティをイネーブルにします。音声認識 802.1x セキュ リティをディセーブルにするには、このコマンドの no バージョンを入力します。このコマンドは、 スイッチの 802.1x 設定ポートのすべてに適用されます。



shutdown vlan キーワードを含めない場合、errordisable ステートになったときにポート全体がシャットダウンされます。

- errdisable recovery cause security-violation グローバル コンフィギュレーション コマンドを使用 して、errordisable リカバリを設定すると、ポートは自動的に再びイネーブルにされます。
 errordisable リカバリがポートで設定されていない場合、shutdown および no-shutdown インター フェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、clear errdisable interface interface-id vlan [vlan-list] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause security-violation shutdown vlan	セキュリティ違反エラーが発生したすべての VLAN をシャットダウ ンします。
		(注) shutdown vlan キーワードは含めない場合、すべてのポート が errordisable ステートになり、シャットダウンされます。
ステップ 3	errdisable recovery cause security-violation	(任意)自動 VLAN 単位エラー リカバリをイネーブルにします。
ステップ 4	clear errdisable interface interface-id vlan [vlan-list]	(任意) errordisable になっている個々の VLAN を再びイネーブルに します。
		 <i>interface-id</i>の場合、個々のVLANを再びイネーブルにするポートを指定します。
		 (任意) vlan-list の場合、再びイネーブルにする VLAN のリスト を指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。

		_ ··
	コマンド	目的
ステップ 5	shutdown	(任意) errordisable の VLAN を再びイネーブルにして、すべての
	no-shutdown	errordisable 指示をクリアします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show errdisable detect	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定 する例を示します。

Switch(config) # errdisable detect cause security-violation shutdown vlan

次の例では、errdisable ステートになっているポート ギガビット イーサネット 0/2 上のすべての VLAN を再度イネーブルにする方法を示します。

Switch# clear errdisable interface gigabitethernet0/2 vlan

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

802.1x 違反モードの設定

(注)

違反モードを使用するには、スイッチが LAN Base イメージを実行している必要があります。

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃 棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。
ステップ 3	aaa authentication dot1x {default} method1	802.1x 認証方式リストを作成します。
		authentication コマンドに名前付きリストが <i>指定されていない</i> 場合に 使用するデフォルトのリストを作成するには、デフォルト状況で使用 することになっている方法に続いて default キーワードを使用しま す。デフォルトの方式リストは、自動的にすべてのポートに適用され ます。
		<i>method1</i> には、 group radius キーワードを入力して、認証用のすべ ての RADIUS サーバ リストを使用できるようにします。
		(注) group radius キーワード以外にもコマンドラインのヘルプストリングに表示されますが、サポートされていません。

	コマンド	目的
ステップ 4	interface interface-id	802.1x 認証をイネーブルにするクライアントに接続しているポート を指定し、インターフェイス コンフィギュレーション モードを開始 します。
ステップ 5	switchport mode access	ポートをアクセス モードにします。
ステップ 6	authentication violation shutdown	違反モードを設定します。キーワードの意味は次のとおりです。
	restrict protect}	• shutdown : ポートを errordisable にします。
	または	• restrict : Syslog エラーを生成します。
	dot1x violation-mode {shutdown restrict protect}	 protect:トラフィックをポートに送信するすべての新しいデバイスからパケットを廃棄します。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show authentication	設定を確認します。
	または	
	show dot1x	
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の設定

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング(AAA)をイネーブルにし て認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う 手順と認証方式を記述したものです。

VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1xのAAA プロセスを示します。

- ステップ1 ユーザがスイッチのポートに接続します。
- **ステップ 2** 認証が実行されます。
- **ステップ 3** RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
- **ステップ4** スイッチが開始メッセージをアカウンティングサーバに送信します。
- ステップ 5 必要に応じて、再認証が実行されます。
- **ステップ6** スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに 送信します。
- ステップ7 ユーザがポートから切断します。
- **ステップ8** スイッチが停止メッセージをアカウンティング サーバに送信します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa new-model	AAA をイネーブルにします。
ステップ 3	aaa authentication dot1x {default}	802.1x 認証方式リストを作成します。
	methou 1	authentication コマンドに名前付きリストが <i>指定されていない</i> 場合に 使用するデフォルトのリストを作成するには、デフォルト状況で使用 することになっている方法に続いて default キーワードを使用しま す。デフォルトの方式リストは、自動的にすべてのポートに適用され ます。
		<i>method1</i> には、 group radius キーワードを入力して、認証用のすべ ての RADIUS サーバ リストを使用できるようにします。
		(注) group radius キーワード以外にもコマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 4	dot1x system-auth-control	スイッチで 802.1x 認証をグローバルにイネーブルにします。
ステップ 5	aaa authorization network {default} group radius	(任意) VLAN 割り当てなど、ネットワーク関連のすべてのサービス 要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 6	radius-server host ip-address	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7	radius-server key string	(任意) RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
ステップ 8	interface interface-id	802.1x 認証をイネーブルにするクライアントに接続しているポート を指定し、インターフェイス コンフィギュレーション モードを開始 します。
ステップ 9	switchport mode access	(任意) ステップ6および7で RADIUS サーバを設定した場合のみ、 ポートをアクセス モードに設定します。
ステップ 10	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
	または	機能の相互作用については、「802.1x 認証設定時の注意事項」
	dot1x port-control auto	(P.9-35)を参照してください。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show authentication	設定を確認します。
	または	
	show dot1x	
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、 または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組 み合せによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに 同じサービス (たとえば認証)を設定した場合、2 番めに設定されたホスト エントリは、最初に設定さ れたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリ は、設定した順序に従って試行されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server host {hostname ip-address} auth-port port-number key string	RADIUS サーバ パラメータを設定します。
		<i>hostname</i> <i>ip-address</i> には、リモート RADIUS サーバのホスト名ま たは IP アドレスを指定します。
		auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定し ます。デフォルトは 1812 です。指定できる範囲は 0 ~ 65536 です。
		key string には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵は、 RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングで なければなりません。
		(注) 鍵の先行スペースは無視されますが、途中および末尾のス ペースは有効なので、鍵は必ず radius-server host コマンド 構文の最後の項目として設定してください。鍵にスペースを 使用する場合は、引用符が鍵の一部分である場合を除き、引 用符で鍵を囲まないでください。鍵は RADIUS デーモンで使 用する暗号鍵に一致している必要があります。
		複数の RADIUS サーバを使用する場合には、このコマンドを繰り返 し入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバをクリアするには、no radius-server host {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポー トとして使用し、暗号鍵を RADIUS サーバ上の鍵と同じ *rad123* に設定する例を示します。

Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定 するには、radius-server host グローバル コンフィギュレーション コマンドを使用します。これらの オプションをサーバ単位で設定するには、radius-server timeout、radius-server retransmit、および radius-server key グローバル コンフィギュレーション コマンドを使用します。詳細については、「す べての RADIUS サーバの設定」(P.8-36) を参照してください。 RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されている 802.1x 許可ポート上で、シングル ホスト (クライアント) または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。multi-domain キーワードを使用して、マルチドメイン認証 (MDA)を設定し、同じスイッチ ポート上の IP Phone (シスコ製品または他社製品) など、ホストと 音声デバイスの両方の認証をイネーブルにします。

この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server vsa send authentication	VSA(Vendor-Specific Attribute; ベンダー固有属性)を認識し使用 するために、ネットワーク アクセス サーバを設定します。
ステップ 3	interface interface-id	複数ホストが間接的に接続されているポートを指定し、インターフェ イス コンフィギュレーション モードを開始します。
ステップ 4	authentication host-mode [multi-auth multi-domain multi-host single-host] # 7- 17	 キーワードの意味は次のとおりです。 multi-auth:音声 VLAN で1 クライアント、データ VLAN で複数の認証クライアントを許可します。各ホストは個別に認証されます。
	dot1x host-mode {single-host multi-host multi-domain}	(注) multi-auth キーワードを使用できるのは、authentication host-mode コマンドだけです。
		 multi-host:シングルホストの認証後に802.1x許可ポートで複数のホスト(クライアント)の接続を許可します。
		• multi-domain : IP Phone(シスコ製または他社製)など、ホス トおよび音声の両方のデバイスを 802.1x 許可ポートで認証でき るようにします。
		 (注) ホスト モードが multi-domain に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。詳細は、第 15 章「音声 VLAN の設定」を参照してください。
		 single-host: 802.1x 許可ポートでシングル ホスト (クライアント)の接続を許可します。
		指定するインターフェイスで、authentication port-control または dot1x port-control インターフェイス コンフィギュレーション コマ ンドが auto に設定されていることを確認してください。
ステップ 5	switchport voice vlan vlan-id	(任意) 音声 VLAN を設定します。
ステップ 6	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	show authentication interface <i>interface-id</i>	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上で複数のホストをディセーブルにするには、no authentication host-mode または no dot1x host-mode multi-host インターフェイス コンフィギュレーション コマンドを使用します。

次に、802.1x 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにして、ポートでホストおよび音声デバイスの両方を許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔(秒)を設定するには、特権 EXECモードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	authentication periodic	クライアントの定期的な再認証(デフォルトではディセーブル)をイ
	または	ネーブルにします。
	dot1x reauthentication	

	コマンド	目的
ステップ 4	authentication timer {{[inactivity reauthenticate] [server <i>am</i>]} {restart <i>value</i> }}	再認証の間隔(秒)を指定します。
		authentication timer キーワードの意味は次のとおりです。
	または	 inactivity: クライアントからのアクティビティがなくなり無許可になるまでの間隔(秒単位)。
	dot1x timeout reauth-period {seconds server}	 reauthenticate:自動再認証が開始するまでの時間(秒単位)。
		 server <i>am</i>:無許可ポートの認証を試行するまでの間隔(秒単位)。
		 restart value: 無許可ポートの認証を試行するまでの間隔(秒単位)。
		dot1x timeout reauth-period キーワードの意味は次のとおりです。
		 seconds: 秒数を1~65535の範囲で設定します。デフォルトは 3600秒です。
		 server : Session-Timeout RADIUS アトリビュート (アトリ ビュート [27]) および Terminate-Action RADIUS アトリビュー ト (アトリビュート [29]) の値に基づいて秒数を指定します。
		このコマンドがスイッチの動作に影響するのは、定期的な再認証をイ ネーブルに設定した場合だけです。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

定期的な再認証をディセーブルにするには、no authentication periodic または no dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用します。再認証の間隔を デフォルトの秒数に戻すには、no authentication timer または no dot1x timeout reauth-period イン ターフェイス コンフィギュレーション コマンドを使用します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する例を示します。

Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface *interface-id 特*権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「定期的な再認証の設定」(P.9-45)を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

Switch # dot1x re-authenticate interface gigabitethernet0/1

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、そのあと再 び認証を試みます。dot1x timeout quiet-period インターフェイス コンフィギュレーション コマンド がその待ち時間を制御します。クライアント認証が失敗する理由としては、クライアントが無効なパス ワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユー ザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	dot1x timeout quiet-period seconds	スイッチがクライアントとの認証情報の交換に失敗した後、待機状態 を続ける秒数を設定します。
		指定できる範囲は1~65535秒です。デフォルトは60秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

待機時間をデフォルトに戻すには、no dot1x timeout quiet-period インターフェイス コンフィギュ レーション コマンドを使用します。

次に、スイッチの待機時間を30秒に設定する例を示します。

Switch(config-if) # dot1x timeout quiet-period 30

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレー ムで応答します。スイッチがこの応答を受信できなかった場合、所定の時間(再送信時間)だけ待機 し、そのあとフレームを再送信します。

(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバ の動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してくださ い。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を 実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	dot1x timeout tx-period seconds	スイッチが EAP-Request/Identity フレームに対するクライアントか らの応答を待ち、要求を再送信するまでの秒数を設定します。
		指定できる範囲は1~65535秒です。デフォルトは5秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信時間をデフォルトに戻すには、no dot1x timeout tx-period インターフェイス コンフィギュレー ション コマンドを使用します。

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

Switch(config-if) # dot1x timeout tx-period 60

スイッチからクライアントへのフレーム再送信回数の設定

(クライアントから応答が得られなかった場合に)スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバ の動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してくださ い。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を 実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	dot1x max-reauth-req count	スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は $1 \sim 10$ です。デフォルトは 2 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信回数をデフォルトに戻すには、no dot1x max-req インターフェイス コンフィギュレーション コ マンドを使用します。

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を5に設定する例を示します。

Switch(config-if) # dot1x max-req 5

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

(注)

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバ の動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してくださ い。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	dot1x max-reauth-req count	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再 開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォル トは 2 です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface <i>interface-id</i>	設定を確認します。
	または	
	show dot1x interface interface-id	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

再認証回数をデフォルトに戻すには、no dot1x max-reauth-req インターフェイス コンフィギュレー ション コマンドを使用します。

次に、ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数として4を設定 する例を示します。

Switch(config-if) # dot1x max-reauth-req 4

MAC Move のイネーブル化

MAC Move を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC Move をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始し
	ます。
authentication mac-move permit	イネーブル
end	特権 EXEC モードに戻ります。
show run	設定を確認します。
copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保
	存します。

次の例では、スイッチで MAC Move をグローバルにイネーブルにする方法を示します。

Switch(config)# authentication mac-move permit

802.1x アカウンティングの設定

802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギ ングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバ は、アクティブな 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好 でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティン グ要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場 合、次のメッセージが表示されます。

Accounting message %s for session %s failed to receive Accounting Response.

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.



ロギングの開始、停止、仮のアップデートメッセージ、タイム スタンプなどのアカウンティング タス クを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、 RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] の ロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。 AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	aaa accounting dot1x default start-stop group radius	すべての RADIUS サーバのリストを使用して、802.1x アカウンティ ングをイネーブルにします。
ステップ 4	aaa accounting system default start-stop group radius	(任意)システムアカウンティングをイネーブルにし(すべての RADIUSサーバのリストを使用)、スイッチがリロードするときにシ ステムアカウンティングリロードイベントメッセージを生成します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、show radius statistics 特権 EXEC コマンドを使用します。

次に、802.1x アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

Switch (config) # radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123 Switch (config) # aaa accounting dot1x default start-stop group radius Switch (config) # aaa accounting system default start-stop group radius

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、 802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗 したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.9-35)を参照してください。
ステップ 3	switchport mode access	ポートをアクセス モードにします。
ステップ 4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
	または	
	dot1x port-control auto	

	コマンド	目的
ステップ 5	dot1x guest-vlan vlan-id	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定 できる範囲は 1 ~ 4094 です。
		RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ゲスト VLAN をディセーブルにして削除するには、no dot1x guest-vlan インターフェイス コンフィ ギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を 802.1x ゲスト VLAN としてイネーブルにする例を示します。

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x guest-vlan 2

次に、スイッチの待機時間として3を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間(秒)を15に設定し、802.1x ポートの DHCP クライアント接続時に、 VLAN 2を 802.1x ゲスト VLAN としてイネーブルにする例を示します。

Switch(config-if)# dotlx timeout quiet-period 3
Switch(config-if)# dotlx timeout tx-period 15
Switch(config-if)# dotlx guest-vlan 2

制限付き VLAN の設定

スイッチ上に、制限付き VLAN を設定していて、認証サーバが有効なユーザ名またはパスワードを受信できない場合は、802.1x に準拠したクライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	 目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.9-35)を参照してください。
ステップ 3	switchport mode access	ポートをアクセス モードにします。
ステップ 4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
	または	
	dot1x port-control auto	
ステップ 5	authentication event fail action authorize <i>vlan-id</i>	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指 定できる範囲は 1 ~ 4094 です。
		RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。

	コマンド	目的
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface-id	(任意)設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

制限付き VLAN をディセーブルにして削除するには、no dot1x auth-fail vlan インターフェイス コン フィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を IEEE 802.1x 制限付き VLAN としてイネーブルにする例を示します。

-if)# dot1x auth-fail vlan 2

ユーザに制限付き VLAN を割り当てる前に、dot1x auth-fail max-attempts インターフェイス コン フィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数 は1~3 です。デフォルトは3回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.9-35)を参照してください。
ステップ 3	switchport mode access	ポートをアクセス モードにします。
ステップ 4	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
	または	
	dot1x port-control auto	
ステップ 5	dot1x auth-fail vlan vlan-id	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指 定できる範囲は 1 ~ 4094 です。
		RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。
ステップ 6	dot1x auth-fail max-attempts max attempts	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は1~3秒です。デフォルトは3です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show authentication interface-id	(任意)設定を確認します。
	または	
	show dot1x interface interface-id	
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定数をデフォルトに戻すには、no dot1x auth-fail max-attempts インターフェイス コンフィギュ レーション コマンドを使用します。

次に、ポートを制限付き VLAN にするために、認証試行回数を2に設定する方法を示します。

Switch(config-if)# dot1x auth-fail max-attempts 2

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能(クリティカル認証または AAA 失敗ポリシーとも呼ばれます)を設定できます。

ポートをクリティカル ポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、 特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	radius-server dead-criteria time time tries tries	(任意) RADIUS サーバが使用できない、または dead と見なされるときを判別するのに使われる条件を設定します。
		指定できる time の範囲は $1 \sim 120$ 秒です。 スイッチは、 デフォルトの seconds 値を $10 \sim 60$ 秒の間で動的に決定します。
		指定できる tries の範囲は $1 \sim 100$ です。スイッチは、デフォルトの tries パラ メータを $10 \sim 100$ の間で動的に決定します。
ステップ 3	radius-server deadtime minutes	(任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる 範囲は 0 ~ 1440 分です(24 時間)。デフォルト値は 0 分です。
ステップ 4	radius-server host	(任意) 次のキーワードを使用して RADIUS サーバ パラメータを設定します。
	<i>ip-address</i> [acct-port <i>udp-port</i>] [auth-port <i>udp-port</i>] [test username <i>name</i> [idle-time time] [ignore-acct-port] [ignore-auth-port]] [key <i>string</i>]	 acct-port udp-port : RADIUS アカウンティング サーバの UDP ポートを 指定します。UDP ポート番号の範囲は 0 ~ 65536 です。デフォルトは 1646 です。
		 auth-port <i>udp-port</i>: RADIUS 認証サーバの UDP ポートを指定します。 UDP ポート番号の範囲は 0 ~ 65536 です。デフォルトは 1645 です。
		(注) RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サー バの UDP ポートを非デフォルト値に設定します。
		• test username name : RADIUS サーバ ステータスの自動テストをイネー ブルにして、使用するユーザ名を指定します。
		 idle-time time : スイッチがテスト パケットをサーバに送信したあとの間 隔を分数で設定します。指定できる範囲は1~35791分です。デフォルト は 60 分(1 時間)です。
		 ignore-acct-port : RADIUS サーバ アカウンティング ポートのテストを ディセーブルにします。
		• ignore-auth-port : RADIUS サーバ認証ポートのテストをディセーブルに します。
		 key string: スイッチと RADIUS デーモンとの間のすべての RADIUS 通 信で使用する認証および暗号鍵を指定します。
		(注) 鍵の先行スペースは無視されますが、途中および末尾のスペースは有 効なので、鍵は必ず radius-server host コマンド構文の最後の項目と して設定してください。鍵にスペースを使用する場合は、引用符が鍵 の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵に一致している必要があります。
		radius-server key {0 string 7 string string} グローバル コンフィギュ レーション コマンドを使用しても認証および暗号鍵を設定できます。

	コマンド	目的
ステップ 5	dot1x critical {eapol	(任意)アクセス不能認証バイパスのパラメータを設定します。
	recovery delay milliseconds}	eapol:スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。
		recovery delay milliseconds:使用できない RADIUS サーバが使用できるよう になったときに、スイッチがクリティカル ポートを再初期化するために待機す る回復遅延期間を設定します。指定できる範囲は1~10000 ミリ秒です。デ フォルトは1000 ミリ秒です(ポートは毎秒再初期化できます)。
ステップ 6	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モード を開始します。サポートされるポートのタイプについては、「802.1x 認証設定 時の注意事項」(P.9-35)を参照してください。
ステップ 7	authentication event server dead action [authorize	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートで ホストを移動します。
	reinitialize] vlan vlan-id	 authorize:認証しようとする新しいホストをユーザ指定のクリティカル VLANに移動します。
		 reinitialize: ポートのすべての許可済みホストをユーザ指定のクリティカル VLAN に移動します。
ステップ 8	dot1x critical [recovery action reinitialize vlan	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用し て機能を設定します。
	vlan-id]	 recovery action reinitialize:回復機能をイネーブルにして、認証サーバが使用可能なとき、回復動作中にポートを認証するように指定します。
		 vlan vlan-id:スイッチがクリティカル ポートに割り当てるアクセス VLAN を指定します。指定できる範囲は1~4094です。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show authentication interface interface-id	(任意)設定を確認します。
	または	
	show dot1x interface interface-id	
ステップ 11	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

RADIUS サーバのデフォルト設定に戻すには、no radius-server dead-criteria、no radius-server deadtime、および no radius-server host グローバル コンフィギュレーション コマンドを使用します。 アクセス不能認証バイパスのデフォルト設定に戻すには、no dot1x critical {eapol | recovery delay} グローバル コンフィギュレーション コマンド を使用します。アクセス不能認証バイパスをディセーブ ルにするには、no dot1x critical インターフェイス コンフィギュレーション コマンドを使用します。

```
次に、アクセス不能認証バイパス機能を設定する例を示します。
```

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abcl234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet0/2
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.9-35)を参照してください。
ステップ 3	authentication control-direction {both in}	ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキー ワードを使用してポートを双方向または単方向に設定します。
	または dot1x control-direction {both in}	 both:ポートを双方向に設定します。ポートは、ホストとの間で パケットを送受信できません。デフォルトでは、ポートは双方向 です。
		 in:ポートを単方向に設定します。ポートはパケットをホストに 送信できますが、ホストからパケットを受信できません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface <i>interface-id</i>	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチで WoL を使用した 802.1x 認証をディセーブルにするには、no authentication control-direction または no dot1x control-direction インターフェイス コンフィギュレーション コマ ンドを使用します。

次に、WoL を使用した 802.1x 認証をイネーブルにして、ポートを双方向に設定する例を示します。 Switch(config-if)# authentication control-direction both

または

Switch(config-if) # dot1x control-direction both

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。サポートされるポートのタイプについては、 「802.1x 認証設定時の注意事項」(P.9-35)を参照してください。
ステップ 3	authentication port-control auto	ポート上で 802.1x 認証をイネーブルにします。
	または	
	dot1x port-control auto	
ステップ 4	dot1x mac-auth-bypass [eap timeout activity {value}]	MAC 認証バイパスをイネーブルにします。
		(任意) eap キーワードを使用して認証用の EAP を使用するようにス イッチを設定します。
		(任意) timeout activity キーワードを使用して、接続されたホストが 無許可ステートになる前に非アクティブである秒数を設定します。指 定できる範囲は $1 \sim 65535$ です。
		タイムアウト値を設定する前にポート セキュリティをイネーブルに する必要があります。詳細については、「ポート セキュリティの設 定」(P.23-9)を参照してください。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MAC 認証バイパスをディセーブルにするには、no dot1x mac-auth-bypass インターフェイス コン フィギュレーション コマンドを使用します。

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

Switch(config-if) # dot1x mac-auth-bypass

802.1x ユーザ ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、グローバル コンフィギュ レーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	vlan group vlan-group-name vlan-list vlan-list	VLAN グループを設定し、単一の VLAN または VLAN の範
		囲をそのグループにマッピングします。
ステップ 2	show vlan group all vlan-group-name	設定を確認します。
ステップ 3	no vlan group <i>vlan-group-name</i> vlan-list	VLAN グループ コンフィギュレーションまたは VLAN グ
	viun-iisi	ルーノ コンノイヤュレーションの安素をクリノ します。

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィ ギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

switch(config) # vlan group eng-dept vlan-list 10

<pre>switch(config)# show vlan group </pre>	group-name eng-dept
Group Name	Vlans Mapped
eng-dept	10
switch# show dot1x vlan-group a	11
Group Name	Vlans Mapped
eng-dept	10
hr-dept	20

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name Vlans Mapped
-----eng-dept 10,30

次に、VLAN を VLAN グループから削除する例を示します。

switch# no vlan group eng-dept vlan-list 10

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアさ れる例を示します。

switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config) # show vlan group group-name eng-dept

次の例では、すべての VLAN グループをクリアする方法を示します。

switch(config)# no vlan group end-dept vlan-list all switch(config)# show vlan-group all

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバを使用した 802.1x 認証とも呼ば れます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	dot1x guest-vlan vlan-id	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定 できる範囲は 1 ~ 4094 です。
		RSPAN VLAN または音声 VLAN を除くあらゆるアクティブ VLAN を、802.1x ゲスト VLAN として設定できます。
ステップ 4	authentication periodic	クライアントの定期的な再認証(デフォルトではディセーブル)をイ
	または	ネーブルにします。
	dot1x reauthentication	
ステップ 5	dot1x timeout reauth-period { <i>seconds</i> server }	再認証の間隔(秒)を指定します。
		キーワードの意味は次のとおりです。
		 seconds: 秒数を1~65535の範囲で設定します。デフォルトは 3600秒です。
		 server: Session-Timeout RADIUS アトリビュート (アトリ ビュート [27]) および Terminate-Action RADIUS アトリビュー ト (アトリビュート [29])の値に基づいて秒数を指定します。
		このコマンドがスイッチの動作に影響するのは、定期的な再認証をイ ネーブルに設定した場合だけです。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show authentication interface <i>interface-id</i>	802.1x 認証の設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、NAC レイヤ 2 IEEE 802.1x 検証を設定する例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# dot1x reauthentication Switch(config-if)# dot1x timeout reauth-period server

NEAT での認証者およびサプリカント スイッチの設定

この機能を設定するには、ワイヤリングクローゼット外の1つのスイッチがサプリカントとして設定 され、認証者スイッチに接続されている必要があります。

概要については、「Network Edge Access Topology (NEAT)を使用した 802.1x サプリカントおよび認 証者」(P.9-31)を参照してください。

(注)

cisco-av-pairs は、ACS で *device-traffic-class=switch* として設定されている必要があります。これは、 サプリカントが正常に認証された後でトランクとしてインターフェイスを設定します。

スイッチを認証者に設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cisp enable	CISP をイネーブルにします。
ステップ 3	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 4	switchport mode access	ポート モードを access に設定します。
ステップ 5	authentication port-control auto	ポート認証モードを auto に設定します。
ステップ 6	dot1x pae authenticator	インターフェイスを Port Access Entity(PAE; ポート アクセス エン ティティ)を認証者として設定します。
ステップ 7	spanning-tree portfast	単一ワークステーションまたはサーバに接続されたアクセス ポート 上で PortFast をイネーブルにします。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show running-config interface <i>interface-id</i>	設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、スイッチを802.1x認証者として設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサプリカントに設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cisp enable	CISP をイネーブルにします。
ステップ 3	dot1x credentials profile	802.1x 証明書プロファイルを作成します。これは、サプリカントとして設定されるポートに接続されなければなりません。
ステップ 4	username suppswitch	ユーザ名を作成します。
ステップ 5	password password	新しいユーザ名のパスワードを作成します。

	コマンド	目的
ステップ 6	dot1x supplicant force-multicast	ユニキャストまたはマルチキャスト パケットのいずれかを受信した 場合にスイッチに強制的にマルチキャスト EAPOL <i>だけ</i> を送信させま す。
		これにより、NEAT がすべてのホスト モードでのサプリカント ス イッチで機能できるようにもなります。
ステップ 7	interface <i>interface-id</i>	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 8	switchport trunk encapsulation dot1q	ポートをトランク モードにします。
ステップ 9	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	dot1x pae supplicant	インターフェイスをポート アクセス エンティティ(PAE)をサプリ カントとして設定します。
ステップ 11	dot1x credentials profile-name	802.1x 証明書プロファイルをインターフェイスに接続します。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	show running-config interface <i>interface-id</i>	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

ASP での NEAT の設定

スイッチ VSA ではなく AutoSmart Ports ユーザ定義マクロを使用して、認証者スイッチを設定することもできます。詳細については、第12章「Auto SmartPort マクロの設定」を参照してください。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証 の設定

スイッチで 802.1x 認証を設定するほか、ACS を設定する必要があります。詳細については、『Cisco Secure ACS configuration guides』を参照してください。



スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、show ip access-list 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示します。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイス トラッキン グ テーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに 適用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip device tracking	IP デバイス トラッキング テーブルを設定します。
ステップ 3	aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa authorization network default group radius	許可の方法をローカルに設定します。許可の方法を削除する には、 no aaa authorization network default group radius コ マンドを使用します。
ステップ 5	radius-server vsa send authentication	radius vsa send authentication を設定します。
ステップ 6	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ステップ 7	ip access-group acl-id in	ポートの入力方向のデフォルト ACL を設定します。
		(注) acl-id はアクセス リストの名前または番号です。
ステップ 8	show running-config interface interface-id	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

ダウンロード ポリシーの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number deny source source-wildcard log	送信元アドレスおよびワイルドカードを使用してデフォルト ポート ACL を定義します。
		access-list-number には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。
		条件が一致した場合にアクセスを拒否する場合は deny、許可する場合は permit を指定します。
		<i>source</i> は、次のようなパケットを送信するネットワークまたはホスト の送信元アドレスです。
		 ドット付き 10 進表記による 32 ビット長の値。
		 source および source-wildcard の値 0.0.0.0 255.255.255.255 の省 略形を意味するキーワード any。source-wildcard 値を入力する必 要はありません。
		 source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。
		(任意)source-wildcard ビットを送信元アドレスに適用します。
		(任意) ログを入力して、エントリと一致するパケットに関する情報 ロギング メッセージをコンソールに送信します。
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip access-group acl-id in	ポートの入力方向のデフォルト ACL を設定します。
		(注) acl-id はアクセス リストの名前または番号です。
ステップ 5	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	aaa new-model	AAA をイネーブルにします。
ステップ 7	aaa authorization network default group radius	許可の方法をローカルに設定します。許可の方法を削除するには、 no aaa authorization network default group radius コマンドを使用 します。
ステップ 8	ip device tracking	IP デバイス トラッキング テーブルをイネーブルにします。
		IP デバイス トラッキング テーブルをディセーブルにするには、no ip device tracking グローバル コンフィギュレーション コマンドを使用 します。
ステップ 9	ip device tracking probe count count	(任意) IP デバイス トラッキング テーブルを設定します。
		 count count: スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は1~5です。デフォルト値は3です。
		 interval interval: スイッチが ARP プローブを再送信するまでに 応答を待機する時間(秒単位)を設定します。指定できる範囲は 30~300秒です。デフォルト値は 30秒です。
ステップ 10	radius-server vsa send authentication	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。
		(注) ダウンロード可能な ACL が機能する必要があります。
ステップ 11	end	 特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	show ip device tracking all	IP デバイス トラッキング テーブルに関するエントリの情報を表示し
ステップ 13	copy running-config startup-config	ょ 9 。 (任意) コンフィギュレーション ファイルに設定を保存します。

次に、ダウンロードポリシーのスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開
		始します。
ステップ 2	mab request format attribute 32 vlan access-vlan	VLAN ID ベース MAC 認証をイネーブルにしま
		す。
ステップ 3	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定
		を保存します。

VLAN ID ベース MAC 認証のステータスを確認する show コマンドはありません。debug radius accounting 特権 EXEC コマンドを使用して RADIUS アトリビュート 32 を確認できます。このコマンドの詳細については、次の URL で『*Cisco IOS Debug Command Reference, Release 12.2*』を参照して ください。

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db q1.html#wp1123741

次の例では、スイッチで VLAN ID ベース MAC 認証をグローバルにイネーブルにする方法を示します。

Switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# mab request format attribute 32 vlan access-vlan Switch(config-if)# exit

柔軟な認証の順序設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ップ 3	authentication order [dot1x mab] {webauth}	(任意) ポート上で使用される認証方式の順序を設定します。
ップ 4	authentication priority [dot1x mab] {webauth}	(任意)認証方式をポート プライオリティ リストに追加しま す。
ップ 5	show authentication	(任意)設定を確認します。
ップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

次に、ポートが最初に 802.1x 認証を試行してから Web 認証をフォールバック方法として設定する例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config)# authentication order dot1x webauth

Open1x の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ステップ 3	authentication control-direction {both in}	(任意) ポート制御を単一方向モードまたは双方向モードに設 定します。
ステップ 4	authentication fallback <i>name</i>	(任意) 802.1x 認証をサポートしないクライアント用のフォー ルバック方法として Web 認証を使用するようポートを設定し ます。
ステップ 5	authentication host-mode [multi-auth multi-domain multi-host single-host]	(任意) ポート上で認証マネージャ モードを設定します。
ステップ 6	authentication open	(任意) ポート上でオープン アクセスをイネーブルまたはディ セーブルにします。
ステップ 7	authentication order [dot1x mab] {webauth}	(任意) ポート上で使用される認証方式の順序を設定します。
ステップ 8	authentication periodic	(任意) ポート上で再認証をイネーブルまたはディセーブルに します。
ステップ 9	authentication port-control {auto force-authorized force-un authorized}	(任意) ポートの許可ステートの手動制御をイネーブルにしま す。
	コマンド	目的
---------	------------------------------------	------------------------------
ステップ 10	show authentication	(任意) 設定を確認します。
ステップ 11	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま
		す

次の例では、ポートのオープン 1x を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、no dot1x pae インターフェイス コンフィギュレー ション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	no dot1x pae	ポート上で 802.1x 認証をディセーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface-id	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x ポート アクセス エンティティ (PAE) 認証者としてポートを設定するには、dot1x pae authenticator インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで 802.1x がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次の例では、ポートの 802.1x 認証をディセーブルにする方法を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no dot1x pae authenticator

802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、設定す るポートを指定します。
ステップ 3	dot1x default	802.1x パラメータをデフォルト値に戻します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show authentication interface <i>interface-id</i>	設定を確認します。
	または	
	<pre>show dot1x interface interface-id</pre>	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

802.1x の統計情報およびステータスの表示

すべてのポートに関する 802.1x 統計情報を表示するには、show dot1x all statistics 特権 EXEC コマン ドを使用します。特定のポートに関する 802.1x 統計情報を表示するには、show dot1x statistics interface *interface-id* 特権 EXEC コマンドを使用します。

スイッチに関する 802.1x 管理および動作ステータスを表示するには、show dot1x all [details | statistics | summary] 特権 EXEC コマンドを使用します。特定のポートに関する 802.1x 管理および動作ステータスを表示するには、show dot1x interface *interface-id* 特権 EXEC コマンドを使用します。 出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。



CHAPTER **10**

Web ベース認証の設定

この章では、Web ベース認証を設定する方法について説明します。内容は次のとおりです。

- 「Web ベース認証の概要」(P.10-1)
- 「Web ベース認証の設定」(P.10-9)
- 「Web ベース認証ステータスの表示」(P.10-18)

(注)

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

Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホスト システムのエンド ユーザを認証するには、*Web* 認証プロキシと呼ばれる Web ベース認証機能を使用します。

(注)

Web ベース認証は、レイヤ2およびレイヤ3インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの入力 HTTP パケットを代行受信し、 ユーザに HTML ログイン ページを送信します。ユーザは証明書を入力します。この証明書は、Web ベース認証機能により、認証のために Authentication, Authorization, Accounting (AAA; 認証、許可、 アカウンティング)サーバに送信されます。

認証に成功した場合、Web ベース認証は、ログインの成功を示す HTML ページをホストに送信し、 AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザに転送し、ロ グインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは待機期間中、 ウォッチ リストに載せられます。

ここでは、AAAの一部としてのWebベース認証の役割について説明します。

- •「デバイスの役割」(P.10-2)
- 「ホストの検出」(P.10-2)
- 「セッションの作成」(P.10-3)
- 「認証プロセス」(P.10-3)

- 「Web 認証カスタマイズ可能な Web ページ」(P.10-6)
- 「その他の機能と Web ベース認証の相互作用」(P.10-7)

デバイスの役割

Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント: LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答 するデバイス (ワークステーション)。このワークステーションでは、Java Script がイネーブルに 設定された HTML ブラウザが実行されている必要があります。
- *認証サーバ*: クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのク ライアントに LAN およびスイッチ サービスへのアクセスを許可するか、拒否するかをスイッチに 通知します。
- スイッチ:クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス(プロキシ)として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。
- 図 10-1 は、ネットワークでのこれらのデバイスの役割を示しています。



ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス トラッキング テーブルを 維持します。

(注)

デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ2インターフェイスでは、Webベース認証は、これらのメカニズムを使用して、IPホストを検 出します。

- ARP ベースのトリガ: ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング:スイッチにより、このホストに対する DHCP バインディング エントリが作成されると、Web ベース認証に通知が送られます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。
 ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、
 セッションが確立されます。
- 認証バイパスをレビューします。

ホスト IP が例外リストに含まれていない場合、Web ベース認証は NonResponsive-Host (NRH; 応 答しないホスト)要求をサーバに送信します。

サーバの応答が access accepted であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

• HTTP インターセプト ACL を設定します。

NRH 要求に対するサーバの応答が access rejected であった場合、HTTP インターセプト ACL が アクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証をイネーブルにすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTPトラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログインページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは、認証サーバからこのユーザのアクセス ポリシーをダウンロー ドし、アクティブ化します。ログインの成功ページがユーザに送信されます。
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチは、ログイン期限切れページを送信します。このホストはウォッチリストに入れられます。ウォッチリストのタイムアウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答しない場合、AAA 失敗ポリシーが設定されていれば、スイッチは失敗アクセスポリシーにホストを適用します。ログインの成功ページがユーザに送信されます (「ローカル Web 認証バナー」(P.10-4)を参照)。
- ホストがレイヤ2インターフェイス上のARPプローブに応答しなかった場合、またはホストがレイヤ3インターフェイスでアイドルタイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッションタイム アウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。 Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除 されます。

ローカル Web 認証バナー

Web 認証を使用してスイッチにログインしたときに表示されるバナーを作成できます。 このバナーは、ログイン ページと認証結果ポップアップ ページの両方に表示されます。

- 認証成功
- 認証失敗
- 認証期限切れ

バナーを作成するには、ip admission auth-proxy-banner http グローバル コンフィギュレーション コ マンドを使用します。ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は、図 10-2 に示すように、認証結果のポッ プアップ ページに表示されます。

図 10-2 認証成功パナー



また、図 10-3 に示すように、バナーをカスタマイズすることもできます。

- バナーにスイッチ、ルータ、または会社名を追加するには、ip admission auth-proxy-banner http banner-text グローバル コンフィギュレーション コマンドを使用します。
- バナーにロゴ、またはテキスト ファイルを追加するには、ip admission auth-proxy-banner http *file-path* グローバル コンフィギュレーション コマンドを使用します。



バナーがイネーブルにされていない場合、図 10-4 に示すように、Web 認証ログイン画面にはユーザ名 とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示さ れません。

Authentication Proxy Login Page - Microsoft Internet Explorer	
🕝 Back - 🕥 - 💌 😰 🏠 🔎 Search 👷 Favorites 🍕	0 @· 🎍 🖃 🖏
iddress 1 http://10.100.100.150/	💌 🛃 Go Linis '
Usemane: Guest	🖹 http://10.100.100.150 - Succe 💽 🗖 🔀
Password:	Authentication Successful !
Done	

図 10-4 パナーが表示されていないログイン画面

詳細については、『Cisco IOS Security Command Reference 』および「Web 認証ローカル バナーの設 定」(P.10-17)を参照してください。

Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の 認証プロセス ステートを通知します。

- ログイン:証明書が要求されています。
- 成功:ログインに成功しました。
- 失敗:ログインに失敗しました。
- 期限切れ:ログインの失敗回数が多すぎて、ログイン セッションが期限切れになります。

注意事項

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナーページで、ログインページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL(例: http://www.cisco.com)でなければなりません。不完全な URLは、Webブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる 可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド (例:ページのタイム アウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信され ていないことの確認など)を記入する必要があります。
- 設定されたログインフォームがイネーブルにされている場合、特定のURLにユーザをリダイレクトするCLIコマンドは使用できません。管理者は、Webページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を 持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- 設定されたページには、スタックマスターまたはメンバー上のフラッシュからアクセスできます。
- ログインページを1つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ(たとえば、 スタックマスター、またはメンバーのフラッシュ)にすることができます。
- 4ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システムディレクトリ(たとえば、flash、disk0、disk)に保存されていて、ログインページに表示する必要のあるロゴファイル(イメージ、フラッシュ、オーディオ、ビデオなど)すべてには、 必ず、web auth <filename>の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

図 10-5 (P.10-7) に示すとおり、デフォルトの内部 HTML ページの代わりに、独自の HTML ページを 使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。



詳細については、「認証プロキシ Web ページのカスタマイズ」(P.10-14)を参照してください。

その他の機能と Web ベース認証の相互作用

- 「ポート セキュリティ」 (P.10-7)
- 「LAN ポート IP」 (P.10-8)
- 「ゲートウェイ IP」 (P.10-8)
- 「ACL」 (P.10-8)
- 「コンテキストベース アクセス コントロール」(P.10-8)
- 「802.1x 認証」(P.10-8)
- [EtherChannel] (P.10-8)

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。Web ベース認証はポートを認 証し、ポート セキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対する ネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできる クライアントの数とグループを制限できます。

ポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」(P.23-9)を 参照してください。

LAN ポート IP

LAN Port IP (LPIP; LAN ポート IP) とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホ ストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホスト ポリ シーは、Web ベース認証のホスト ポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポ スチャが再度検証されます。

ゲートウェイ IP

VLAN のいずれかのスイッチ ポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN イン ターフェイス上に Gateway IP (GWIP; ゲートウェイ IP) を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェア で、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホス ト ポリシーに優先されます。

ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証 のホスト ポリシーが適用された後だけ、ホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、Port ACL (PACL; ポート ACL) をデフォルトのアクセス ポリシーとして設定する必要があります。認証 後、Web ベース認証のホスト ポリシーは、PACL に優先されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

コンテキストベース アクセス コントロール

Context-Based Access Control (CBAC; コンテキストベース アクセス コントロール) が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証 は設定できません。

802.1x 認証

フォールバック認証メソッドとして設定する場合を除き、Web ベース認証は 802.1x 認証と同じポート 上には設定できません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス.上に設定できます。Web ベース認証設 定は、すべてのメンバー チャネルに適用されます。

Web ベース認証の設定

- 「デフォルトの Web ベース認証の設定」(P.10-9)
- 「Web ベース認証の設定に関する注意事項と制約事項」(P.10-9)
- 「Web ベース認証の設定タスク リスト」(P.10-10)
- 「認証ルールとインターフェイスの設定」(P.10-10)
- 「AAA 認証の設定」(P.10-11)
- 「スイッチから RADIUS サーバへの通信のコンフィギュレーション」(P.10-12)
- 「HTTP サーバの設定」(P.10-13)
- 「Web ベース認証パラメータの設定」(P.10-16)
- 「Web ベース認証キャッシュ エントリの削除」(P.10-17)

デフォルトの Web ベース認証の設定

表 10-1 は、デフォルトの Web ベース認証の設定を示しています。

表 10-1 デフォルトの Web ベース認証の設定

機能	デフォルト設定
Authentication, Authorization, Accounting	ディセーブル
(AAA; 認証、許可、アカウンティング)	
RADIUS サーバ	
・ IP アドレス	 指定なし
• UDP 認証ポート	• 1812
• 鍵	 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、 EtherChannel メンバー ポート、またはダイナミック トランク ポートではサポートされていません。
- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ2インターフェイスに対してポート ACL を設定するか、またはレイヤ3インターフェイスに対して Cisco IOS ACL を設定します。
- スタティックな ARP キャッシュが割り当てられているレイヤ2インターフェイス上のホストは認 証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検 出されません。
- デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルに設定されています。
 Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

- スイッチ HTTP サーバを実行するには、IP アドレスを少なくとも1つ設定する必要があります。 また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、 ホストに HTTP ログインページを送信します。
- 2ホップ以上離れたところにあるホストでは、STPトポロジの変更により、ホストトラフィックの 到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レ イヤ2(STP)トポロジの変更後に、ARPおよびDHCPの更新が送信されていない場合に発生し ます。
- Web ベース認証は、ダウンロード可能なホスト ポリシーとして、VLAN 割り当てをサポートして いません。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。

Web ベース認証の設定タスク リスト

- 「認証ルールとインターフェイスの設定」(P.10-10)
- 「AAA 認証の設定」(P.10-11)
- 「スイッチから RADIUS サーバへの通信のコンフィギュレーション」(P.10-12)
- 「HTTP サーバの設定」(P.10-13)
- 「AAA 失敗ポリシーの設定」(P.10-16)
- 「Web ベース認証パラメータの設定」(P.10-16)
- 「Web ベース認証キャッシュ エントリの削除」(P.10-17)

認証ルールとインターフェイスの設定

	コマンド	目的
ステップ 1	ip admission name name proxy http	Web ベース認証で使用される認証ルールを設定します。
ステップ 2	interface <i>type slot/port</i>	インターフェイス コンフィギュレーション モードを開始し、Web ベースの認証のためにイネーブルにされる入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。
		<i>type</i> には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 3	ip access-group name	デフォルト ACL を適用します。
ステップ 4	ip admission name	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 5	exit	コンフィギュレーション モードに戻ります。
ステップ 6	ip device tracking	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show ip admission configuration	コンフィギュレーションを表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、Fast Ethernet ポート 5/1 で Web ベース認証をイネーブルにする例を示します。

Switch(config)# ip admission name webauth1 proxy http Switch(config)# interface fastethernet 5/1 Switch(config-if)# ip admission webauth1 Switch(config-if)# exit Switch(config)# ip device tracking 次に、設定を確認する例を示します。 Switch# show ip admission configuration Authentication Proxy Banner not configured Authentication global cache time is 60 minutes Authentication global absolute time is 0 minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list is disabled Authentication Proxy Rule Configuration Auth-proxy name webauth1 http list not specified inactivity-time 60 minutes Authentication Proxy Auditing is disabled Max Login attempts per user is 5

AAA 認証の設定

	コマンド	目的
ステップ 1	aaa new-model	AAA 機能をイネーブルにします。
ステップ 2	aaa authentication login default group { <i>tacacs</i> + <i>radius</i> }	ログイン時の認証方法のリストを定義します。
ステップ 3	aaa authorization auth-proxy default group { <i>tacacs+</i> <i>radius</i> }	Web ベースの認証で使用される認証方法のリストを 作成します。
ステップ 4	tacacs-server host { <i>hostname</i> <i>ip_address</i> }	AAA サーバを指定します。RADIUS サーバについて は、「スイッチから RADIUS サーバへの通信のコン フィギュレーション」(P.10-12)を参照してくださ い)。
ステップ 5	tacacs-server key {key-data}	スイッチと TACACS サーバの間で使用される認証お よび暗号鍵を設定します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保 存します。

次の例では、AAA をイネーブルにする方法を示します。

Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group tacacs+
Switch(config)# aaa authorization auth-proxy default group tacacs+

スイッチから RADIUS サーバへの通信のコンフィギュレーション

RADIUS セキュリティ サーバの識別情報は次のとおりです。

- ホスト名
- ホスト IP アドレス
- ホスト名および特定の UDP ポート番号
- IP アドレスおよび特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレ ス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上 の異なる 2 つのホスト エントリに同じサービス(たとえば認証)を設定した場合、2 番めに設定された ホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作し ます。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	ip radius source-interface interface_name	RADIUS パケットが、指示されたインターフェイスの IP アドレスを持つことを指定します。
ステップ 2	radius-server host { <i>hostname</i> <i>ip-address</i> } test username <i>username</i>	リモート RADIUS サーバ ホストのホスト名または IP アドレスを指定します。
		test username <i>username</i> は、RADIUS サーバ接続の 自動テストをイネーブルにするオプションです。指定 された <i>username</i> は有効なユーザ名である必要はあり ません。
		key オプションは、スイッチと RADIUS サーバの間 で使用される認証と暗号鍵を指定します。
		複数の RADIUS サーバを使用するには、それぞれの サーバでこのコマンドを入力してください。
ステップ 3	radius-server key string	RADIUS サーバ上で動作するスイッチと RADIUS デーモンの間で使用される認証および暗号鍵を設定し ます。
ステップ 4	radius-server vsa send authentication	RADIUS サーバからの ACL のダウンロードをイネー ブルにします。この機能は、 Cisco IOS Release 12.2(50)SG でサポートされていま す。
ステップ 5	radius-server dead-criteria tries num-tries	RADIUS サーバに送信されたメッセージへの応答が ない場合に、このサーバが非アクティブであると見な すまでの送信回数を指定します。指定できる num-tries の範囲は1~100です。

RADIUS サーバ パラメータを設定する場合は、次の点に注意してください。

- key string は独立したコマンドラインに指定します。
- key string には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認 証および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト スト リングでなければなりません。

- key string を指定する場合、鍵の中間、および末尾にスペースを使用します。鍵にスペースを使用 する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵に一致している必要があります。
- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに 設定するには、radius-server host グローバル コンフィギュレーション コマンドを使用します。 これらのオプションをサーバ単位で設定するには、radius-server timeout、radius-server retransmit、および radius-server key グローバル コンフィギュレーション コマンドを使用しま す。詳細については、次の URL にある 『Cisco IOS Security Configuration Guide, Release 12.2』、および 『Cisco IOS Security Command Reference, Release 12.2』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

(注)

RADIUS サーバでは、スイッチ IP アドレス、サーバとスイッチで共有される key string、および Downloadable ACL (DACL; ダウンロード可能な ACL) などの設定を行う必要があります。詳細につ いては、RADIUS サーバのマニュアルを参照してください。

次の例では、スイッチで RADIUS サーバ パラメータを設定する方法を示します。

Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。この サーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

	コマンド	目的
ステップ 1	ip http server	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用
		してホストと通信し、ユーザ認証を行います。
ステップ 2	ip http secure-server	HTTPS をイネーブルにします。

カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。

(注)

ip http secure-secure コマンドを入力したときに、セキュア認証が確実に行われるようにするには、 ユーザが HTTP 要求を送信した場合でも、ログイン ページは必ず HTTPS (セキュア HTTP) 形式にな るようにします。

- 認証プロキシ Web ページのカスタマイズ
- 成功ログインに対するリダイレクション URL の指定

認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、スイッチのデフォルト HTML ページではなく、代わりの HTML ページがユー ザに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、まず、カスタム HTML ファイルをスイッチ のフラッシュ メモリに保存し、次にグローバル コンフィギュレーション モードでこのタスクを実行し ます。

	コマンド	目的
ステップ 1	ip admission proxy http login page file <i>device:login-filename</i>	スイッチのメモリ ファイル システムで、デフォルト のログイン ページの代わりに使用されるカスタム HTML ファイルの所在地を指定します。 <i>device</i> : はフ ラッシュ メモリです。
ステップ 2	ip admission proxy http success page file <i>device:success-filename</i>	デフォルトのログイン成功ページの代わりに使用され るカスタムの HTML ファイルの所在地を指定します。
ステップ 3	ip admission proxy http failure page file <i>device:fail-filename</i>	デフォルトのログイン失敗ページの代わりに使用され るカスタムの HTML ファイルの所在地を指定します。
ステップ 4	ip admission proxy http login expired page file <i>device:expired-filename</i>	デフォルトのログイン期限切れページの代わりに使用 されるカスタムの HTML ファイルの所在地を指定し ます。

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら4個の HTML ファイルは、スイッチのフラッシュメモリ内に存在しなければなりません。 各 HTML ファイルの最大サイズは8KB です。
- カスタムページ上のイメージはすべて、アクセス可能は HTTP サーバ上に存在しなければなりま せん。インターセプト ACL は、管理ルール内で設定します。
- カスタムページからの外部リンクはすべて、管理ルール内でのインターセプトACLの設定を必要 とします。
- 有効な DNS サーバにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理 ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルに設定されている場合、ログインの成功に対するリダイレ クション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの no 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事 項に従ってください。

- ログインフォームは、ユーザによるユーザ名とパスワードの入力を受け付け、これらを uname および pwd として示す必要があります。
- カスタム ログインページは、ページタイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベストプラクティスに従う必要があります。

次の例では、カスタム認証プロキシ Web ページを設定する方法を示します。

Switch(config) # ip admission proxy http login page file flash:login.htm

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
次の例では、カスタム認証プロキシ Web ページの設定を確認する方法を示します。
Switch# show ip admission configuration
Authentication proxy webpage
Login page
                    : flash:login.htm
 Success page
                     : flash:success.htm
Fail Page
                    : flash:fail.htm
Login expired Page
                   : flash:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Switch(config)# ip admission proxy http success page file flash:success.htm

成功ログインに対するリダイレクション URL の指定

認証後に、内部*成功*HTMLページを効果的に置き換え、ユーザのリダイレクト先となる URL を指定 することができます。

コマンド	目的
ip admission proxy http success redirect url-string	デフォルトのログイン成功ページの代わりに、ユーザの
	リダイレクト先となる URL を指定します。

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログ イン成功ページで実行できます。
- リダイレクション URL 機能がイネーブルに設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの no 形式を使用します。

次の例では、成功したログインに対するリダイレクション URL を設定する方法を示します。

Switch(config) # ip admission proxy http success redirect www.cisco.com

次の例では、成功したログインに対するリダイレクション URL を確認する方法を示します。

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

	コマンド	目的
ステップ 1	ip admission name <i>rule-name</i> proxy http event timeout aaa policy	AAA サーバに到達できない場合、AAA 失敗ルールを作成し、セッ ションに適用される ID ポリシーを関連付けます。
	identity identity_policy_name	(注) ルールを削除するには、no ip admission name rule-name proxy http event timeout aaa policy identity グローバル コ ンフィギュレーション コマンドを使用します。
ステップ 2	ip admission ratelimit aaa-down number_of_sessions	(任意) AAA ダウン ステートで、ホストからの認証の試行をレート 制限し、サービスに戻ってきたときの AAA サーバ フラッディングを 回避します

次に、AAA 失敗ポリシーを適用する例を示します。

Switch(config) # ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy identity GLOBAL_POLICY1

次に、接続されているホストが AAA ダウン ステートであるかどうかを判断する例を示します。

```
Switch# show ip admission cache
Authentication Proxy Cache
Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて、特定のセッションに関する詳細情報を表示する例を示します。

Switch# show ip admission cache 209.165.201.11 Address : 209.165.201.11 MAC Address : 0000.0000.0000 : Vlan333 Interface Port : 3999 Timeout : 60 Age : 1 : AAA Down State AAA Down policy : AAA FAIL POLICY

Web ベース認証パラメータの設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライア ントは待機期間中、ウォッチリストに載せられます。

	コマンド	目的
ステップ 1	ip admission max-login-attempts number	失敗できるログイン試行の最高回数を設定します。指 定できる範囲は1~2147483647回です。デフォルト 値は5です。
ステップ 2	end	特権 EXEC モードに戻ります。
ステップ 3	show ip admission configuration	認証プロシキ設定を表示します。
ステップ 4	show ip admission cache	認証エントリのリストを表示します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保 存します。

次の例では、失敗ログイン試行の最大回数を10に設定する方法を示します。

Switch(config) # ip admission max-login-attempts 10

Web 認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、特権 EXEC モードで次の手順 を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip admission auth-proxy-banner http	ローカル バナーをイネーブルにします。
	[banner-text file-path]	(任意) <i>C banner-text C</i> と入力して、カスタム バナーを作成します。 ここで、 <i>C</i> は区切り文字、またはバナーに表示されるファイル(例: ロゴ、またはテキスト ファイル)を示すファイルパスです。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、「*My Switch*」というカスタム メッセージが表示されているローカル バナーを設定する方 法を示します。

Switch(config) configure terminal Switch(config)# aaa new-model Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C Switch(config) end

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com の『*Cisco IOS Security Command Reference*』にある「Authentication Proxy Commands」セクションを参照してください。

Web ベース認証キャッシュ エントリの削除

コマンド	目的
<pre>clear ip auth-proxy cache {* host ip address}</pre>	Delete 認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用し ます。シングル ホストのエントリを削除するには、具体 的な IP アドレスを入力します。
clear ip admission cache {* <i>host ip address</i> }	Delete 認証プロキシエントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用し ます。シングルホストのエントリを削除するには、具体 的な IP アドレスを入力します。

次に、IP アドレス 209.165.201.1 のクライアントに対する Web ベース認証セッションを削除する例を 示します。

Switch# clear ip auth-proxy cache 209.165.201.1

Web ベース認証ステータスの表示

すべてのインターフェイス、または特定のポートに対する Web ベースの認証設定を表示する手順は、 次のとおりです。

	コマンド	目的
ステップ 1	show authentication sessions	Web ベース認証設定を表示します。
	[interface type slot/port]	type には、fastethernet、gigabitethernet、または tengigabitethernet を指定できます。
		(任意) 特定のインターフェイスに対する Web ベース 認証設定を表示するには、キーワード interface を使 用します。

次に、グローバルな Web ベース認証のステータスだけを表示する例を示します。

Switch# show authentication sessions

次に、ギガビット インターフェイス 3/27 に対する Web ベースの認証設定を表示する例を示します。 Switch# show authentication sessions interface gigabitethernet 3/27



CHAPTER

インターフェイス特性の設定

この章では、Catalyst 2960 スイッチ上の各種インターフェイスのタイプ、およびその設定方法について説明します。

この章で説明する内容は、次のとおりです。

- 「インターフェイス タイプの概要」(P.11-1)
- 「インターフェイス コンフィギュレーション モードの使用方法」(P.11-11)
- 「イーサネットインターフェイスの設定」(P.11-16)
- 「システム MTU の設定」(P.11-30)
- 「インターフェイスのモニタおよびメンテナンス」(P.11-31)

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Interface Command Reference, Release 12.2*』を参照してく ださい。これには、Cisco.com のホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**)からアクセス可能です。

インターフェイス タイプの概要

ここでは、スイッチによってサポートされる各種インターフェイス タイプについて説明するとともに、 これらのインターフェイス タイプの設定に関する詳細情報が記載された章についても言及します。

- 「ポートベースの VLAN」 (P.11-2)
- 「スイッチ ポート」 (P.11-2)
- 「EtherChannel ポート グループ」 (P.11-4)
- 「デュアルパーパス アップリンク ポート」(P.11-4)
- [Power over Ethernet (PoE) #- h (P.11-5)
- 「インターフェイスの接続」(P.11-10)

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的 に分割されたスイッチによるネットワークです。VLAN の詳細については、第13章「VLAN の設定」 を参照してください。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に 属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックを ルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。 また、各 VLAN には固有の MAC (メディア アクセス制御) アドレス テーブルがあります。VLAN が 認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) トランク上のネイバからその存在を学習したとき、 またはユーザが VLAN を作成したときです。

VLAN を設定するには、vlan vlan-id グローバル コンフィギュレーション コマンドを使用して、 VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の VLAN 設定は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 の場合に拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を設定するには、最初に VTP モードをトランスペアレントに設定す る必要があります。トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベース には追加されず、スイッチの実行コンフィギュレーションに格納されます。VTP バージョン 3 では、 クライアントまたはサーバ モードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN デー タベースに格納されます。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加 されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて所属できる VLAN を定義します。
- アクセスポートには、所属する VLAN を設定して定義します。

スイッチ ポート

スイッチ ポートは、物理ポートに対応付けられたレイヤ2専用インターフェイスです。スイッチ ポートは1つまたは複数の VLAN に所属します。スイッチ ポートは、物理インターフェイスおよび対応するレイヤ2プロトコルの管理に使用されます。

スイッチ ポートは、アクセス ポートまたはトランク ポートにも使用できます。ポートは、アクセス ポートまたはトランク ポートに設定できます。また、ポート単位で Dynamic Trunking Protocol (DTP) を稼動させ、リンクのもう一端のポートとネゴシエートすることで、スイッチ ポート モードも 設定できます。

スイッチ ポートの設定には、switchport インターフェイス コンフィギュレーション コマンドを使用します。

アクセス ポート特性およびトランク ポート特性の設定についての詳細については、第13章「VLAN の設定」を参照してください。

アクセス ポート

アクセス ポートは(音声 VLAN ポートとして設定されている場合を除き)1つの VLAN だけに所属 し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タギングなしのネイティ ブフォーマットで送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てら れている VLAN に所属すると見なされます。

アクセス ポートが 802.1Q タグ付きパケットを受信した場合、そのパケットは廃棄され、送信元アドレスは学習されません。

2 種類のアクセス ポートがサポートされています。

- スタティック アクセス ポート。このポートは、手動で VLAN に割り当てます(IEEE 802.1x で使用する場合は RADIUS サーバを使用します。詳細については、「VLAN 割り当てを使用した802.1x 認証」(P.9-17)を参照してください。
- ダイナミック アクセス ポートの VLAN メンバシップは、着信パケットを通じて学習されます。デフォルトでは、ダイナミック アクセス ポートはどの VLAN のメンバーでもなく、ポートとの伝送はポートの VLAN メンバシップが検出されたときにだけイネーブルになります。スイッチ上のダイナミック アクセス ポートは、VLAN Membership Policy Server (VMPS; VLAN メンバシップポリシー サーバ)によって VLAN に割り当てられます。VMPS として動作できるのは、Catalyst 6500 シリーズ スイッチです。Catalyst 2960 スイッチを VMPS サーバにすることはできません。

また、Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように 設定できます。音声 VLAN ポートの詳細については、第15章「音声 VLAN の設定」を参照してくだ さい。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のす べての VLAN のメンバーとなります。

スイッチは、IEEE 802.1Q トランク ポートだけをサポートします。IEEE 802.1Q トランク ポートは、 タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートは、 デフォルトの Port VLAN ID (PVID; ポート VLAN ID) に割り当てられ、すべてのタグなしトラ フィックはポートのデフォルト PVID 上を流れます。NULL VLAN ID を備えたすべてのタグなしおよ びタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートの デフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。残りのトラフィッ クはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは、VTP に認識されているすべての VLAN のメンバーですが、トラ ンク ポートごとに VLAN の許可リストを設定して、VLAN メンバシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えま す。デフォルトでは、使用可能なすべての VLAN (VLAN ID 1 ~ 4094) が許可リストに含まれます。 トランク ポートは、VTP が VLAN を認識し、VLAN がイネーブル状態にある場合に限り、VLAN の メンバーになることができます。VTP が新しいイネーブル VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバーにな り、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランク ポートの許可リストに登録されていない、新しいイネーブル VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トランクポートの詳細については、第13章「VLANの設定」を参照してください。

EtherChannel ポート グループ

EtherChannel ポート グループは、複数のスイッチ ポートを 1 つのスイッチ ポートとして扱います。こ のようなポート グループは、スイッチ間、またはスイッチおよびサーバ間で広帯域接続を行う単一論 理ポートとして動作します。EtherChannel は、チャネルのリンク全体でトラフィックの負荷を分散さ せます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたト ラフィックが EtherChannel 内の残りのリンクに切り替えられます。複数のトランク ポートを 1 つの論 理トランク ポートに、または複数のアクセス ポートを 1 つの論理アクセス ポートにグループ化できま す。ほとんどのプロトコルは単一のまたは集約スイッチ ポートで動作し、ポート グループ内の物理 ポートを認識しません。例外は、DTP、Cisco Discovery Protocol (CDP)、および Port Aggregation Protocol (PAgP) で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャネル論理インターフェイスを作成し、EtherChannel にイン ターフェイスを割り当てます。channel-group インターフェイス コンフィギュレーション コマンドを使 用して、ダイナミックにポート チャネル論理インターフェイスを作成します。このコマンドは物理お よび論理ポートをバインドします。

詳細は、第36章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

デュアルパーパス アップリンク ポート

一部の 2960 スイッチでは、デュアルパーパス アップリンク ポートがサポートされています。各アップリンク ポートはデュアル フロント エンド (RJ-45 コネクタおよび Small Form-factor Pluggable (SFP; 着脱可能小型フォーム ファクタ) モジュール コネクタ) を持つ1つのインターフェイスと見な されます。デュアル フロント エンドは冗長インターフェイスではありません。スイッチはペアのうちの1つのコネクタのみをアクティブにします。

デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、 media-type インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタま たは SFP モジュール コネクタを選択できます。デュアルパーパス アップリンクのデュプレックス設定 および速度設定については、「インターフェイス速度およびデュプレックス パラメータの設定」 (P.11-20) を参照してください。

各アップリンク ポートには、2 つの LED が付いています。1 つは RJ-45 ポートのステータスを示すも ので、もう 1 つは SFP モジュール ポートのステータスを示すものです。ポート LED は、いずれかのコ ネクタがアクティブのときに点灯します。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

Power over Ethernet (PoE) #- \Vdash

(注)

PoE がサポートされているのは、スイッチで LAN Base イメージが実行されている場合だけです。

PoE 対応スイッチ ポートは、次のような接続された装置に電力を自動的に供給します(スイッチが回路に電力が供給されていないことをスイッチが検知した場合)。

- シスコの先行標準装置(Cisco IP Phone および Cisco Aironet アクセス ポートなど)
- IEEE 802.3af に準拠した受電装置

受電装置が PoE スイッチ ポートと AC 電源にだけ接続している場合は、冗長電力を受電できます。

スイッチは受電装置の検出後、この装置の電力要件を決定し、装置への電力供給を許可または拒否しま す。また、スイッチは消費電力を監視およびポリシングすることで、装置の電力の消費をリアルタイム に検知できます。

ここでは、次の PoE 情報について説明します。

- 「サポート対象のプロトコルおよび規格」(P.11-5)
- 「受電装置の検出および初期電力割り当て」(P.11-6)
- 「電力管理モード」(P.11-7)
- 「電力モニタリングおよび電力ポリシング」(P.11-8)

サポート対象のプロトコルおよび規格

スイッチは PoE のサポートで次のプロトコルと規格を使用します。

- 電力の消費について CDP を使用:受電装置は、スイッチに消費している電力量を通知します。スイッチはこの電力消費に関するメッセージに応答しません。スイッチは、PoE ポートに電力を供給するか、このポートへの電力を取り除くだけです。
- シスコのインテリジェントな電力管理:受電装置およびスイッチは、電力ネゴシエーション CDP メッセージによって消費電力レベルを合意するためのネゴシエーションを行います。このネゴシ エーションにより、7Wより多くを消費する高電力のシスコ受電装置は、最も高い電力モードで動 作できるようになります。受電装置は、最初に低電力モードでブートして7W未満の電力を消費 し、ネゴシエーションを行って高電力モードで動作するための十分な電力を取得します。受電装置 が高電力モードに切り替わるのは、スイッチから確認を受信した場合に限られます。

高電力装置は、電力ネゴシエーション CDP をサポートしないスイッチで低電力モードによって動作できます。

シスコのインテリジェントな電力管理の機能には、電力消費に関して CDP との下位互換性がある ため、スイッチは、受信する CDP メッセージに従って応答します。CDP はサードパーティの受電 装置をサポートしません。このため、スイッチは、IEEE 分類を使用して装置の消費電力を判断し ます。

• IEEE 802.3a: この規格の主な機能は、受電装置の検出、電力の管理、切断の検出です。オプションとして受電装置の電力分類があります。詳細については、この規格を参照してください。

受電装置の検出および初期電力割り当て

スイッチは、PoE 対応ポートがシャットダウンの状態でなく、PoE はイネーブルになっていて(デフォルト)、接続した装置は AC アダプタから電力供給されていない場合、シスコの先行標準受電装置 または IEEE 準拠の受電装置を検出します。

装置の検出後、スイッチは、次のように装置のタイプに応じて電力要件を判断します。

• シスコの先行標準受電装置は、スイッチから検出された時点では自身の電力要件を提供しないので、スイッチはパワーバジェットの初期割り当てとして 15.4 W を割り当てます。

初期電力割り当ては、受電装置が要求する最大電力量です。スイッチは、受電装置を検出および電力供給する場合、この電力を最初に割り当てます。スイッチが受電装置から CDP メッセージを受信し、受電装置が CDP 電力ネゴシエーション メッセージを通じてスイッチと電力レベルをネゴシエートしたときに、初期電力割り当てが調整される場合があります。

 スイッチは検出した IEEE 装置を消費電力クラス内で分類します。スイッチは、パワーバジェット に使用可能な電力量に基づいて、ポートに通電できるかどうかを決定します。表 11-1 に、各種レベルの一覧を示します。

Class	スイッチから要求される最大電力レベル
0 (クラス ステータスは不明)	15.4 W
1	4 W
2	7 W
3	15.4 W
4(将来の使用のために予約)	クラス0として取り扱う

表 11-1 IEEE 電力分類

スイッチは電力要求を監視および追跡して必要な場合にだけ電力供給を許可します。スイッチは自身の パワーバジェット(PoEのスイッチで使用可能な電力量)を追跡します。電力の供給許可または拒否 がポートで行われると、スイッチはパワーアカウンティング計算を実行し、パワーバジェットを最新 に保ちます。

電力がポートに適用されると、スイッチは CDP を使用して、接続されたシスコの受電装置の*実際の*電 力消費要件を判断し、必要に応じてパワーバジェットを調整します。これは、サードパーティの PoE 装置には適用されません。スイッチは要件を処理して電力の供給を許可または拒否します。要求が許可 されると、スイッチはパワーバジェットを更新します。要求が拒否された場合は、スイッチはポート の電力がオフに切り替わっていることを確認し、syslog メッセージを生成して LED を更新します。受 電装置はより多くの電力について、スイッチとのネゴシエーションを行うこともできます。

不足電圧、過電圧、オシレータ障害、または短絡状態による障害をスイッチが検出した場合、ポートへの電源をオフにし、syslog メッセージを生成し、パワーバジェットと LED を更新します。

電力管理モード

スイッチでは、次の PoE モードがサポートされます。

 auto:接続されている装置で電力が必要であるかどうか、スイッチが自動的に検出します。ポート に接続されている受電装置をスイッチが検出し、スイッチに十分な電力がある場合、スイッチは電 力を供給してパワーバジェットを更新し、先着順でポートの電力をオンに切り替えて LED を更新 します。LED の詳細については、ハードウェア インストレーション ガイドを参照してください。

すべての受電装置用としてスイッチに十分な電力がある場合は、すべての受電装置が起動します。 スイッチに接続された受電装置すべてに対し十分な電力が利用できる場合、すべての装置に電力を 供給します。使用可能な PoE がない場合、または他の装置が電力供給を待機している間に装置の 接続が切断されて再接続した場合、どの装置へ電力を供給または拒否されるかが判断できなくなり ます。

許可された電力がシステムのパワー バジェットを超えている場合、スイッチは電力を拒否し、 ポートへの電力がオフになっていることを確認したうえで syslog メッセージを生成し、LED を更 新します。電力供給が拒否されたあと、スイッチは定期的にパワー バジェットを再確認し、継続 して電力要求の許可を試みます。

スイッチにより電力を供給されている装置が、さらに壁面コンセントに接続している場合、スイッ チは装置に電力を供給し続ける場合があります。このとき、装置がスイッチから受電しているか、 AC 電源から受電しているかにかかわらず、スイッチは引き続き装置へ電力を供給していることを 報告し続ける場合があります。

受電装置が取り外された場合、スイッチは切断を自動的に検出し、ポートから電力を取り除きま す。非受電装置を接続しても、その装置に障害は発生しません。

ポートで許可される最大ワット数を指定できます。受電装置の IEEE クラス最大ワット数が設定さ れている最大値より大きい場合、スイッチはそのポートに電力を供給しません。スイッチが受電装 置に電力供給したが、受電装置が設定の最大値より多くの電力を CDP メッセージによってあとで 要求した場合、スイッチはポートの電力を取り除きます。その受電装置に割り当てられていた電力 は、グローバル パワー バジェットに送られます。ワット数を指定しない場合、スイッチは最大値 の電力を供給します。任意の PoE ポートで auto 設定を使用してください。auto モードがデフォル ト設定です。

static:スイッチは、受電装置が接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電装置からの CDP メッセージによって調節されることはありません。これは、電力があらかじめ割り当てられていることから、最大ワット数以下の電力を使用するすべての受電装置が固定ポートに接続されている場合に電力が保証されるためです。ポートはもう先着順方式ではなくなります。

ただし、受電装置の IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。受電装置が最大ワット数を超えた量を要求していることを CDP メッセージを通じてスイッチ が認識すると、その受電装置がシャットダウンされます。

ワット数を指定しない場合、スイッチは最大数をあらかじめ割り当てます。スイッチは、受電装置 を検出した場合に限り、ポートに電力を供給します。優先順位が高いインターフェイスには、 static 設定を使用してください。

• never:スイッチは受電装置の検出をディセーブルにして、電力が供給されていない装置が接続されても、PoE ポートに電力を供給しません。このモードは、PoE 対応ポートに電力を適用することがなく、そのポートをデータ専用とする場合にだけ使用してください。

PoE ポートの設定の詳細については、「**PoE** ポートの電力管理モードの設定」(P.11-24) を参照してください。

電力モニタリングおよび電力ポリシング

リアルタイムの消費電力のポリシングをイネーブルにした場合、受電装置が最大割り当て(カットオフ 電力値)を超えて電力を消費すると、スイッチはアクションを開始します。

PoE がイネーブルの場合、スイッチは受電装置のリアルタイムの消費電力を検出します。接続されている受電装置のリアルタイム消費電力をスイッチが監視することを*電力モニタリング*または*電力検知と*呼びます。スイッチは*電力ポリシング*機能を使用して、使用電力にポリシングも行います。

電力モニタリングは、シスコのインテリジェントな電力管理および CDP ベースの消費電力に対して下 位互換性があります。電力モニタリングはこれらの機能とともに動作して、PoE ポートが受電装置に 電力を供給できるようにします。PoE 機能の詳細については、「受電装置の検出および初期電力割り当 て」(P.11-6)を参照してください。

スイッチは次のようにして、接続されている装置のリアルタイム消費電力を検知します。

- 1. スイッチは、個々のポートでリアルタイム消費電力を監視します。
- **2.** スイッチは、ピーク時の消費電力を含め、消費電力を記録します。スイッチは、SNMP MIB、 CISCO-POWER-ETHERNET-EXT-MIB を使用してこの情報を報告します。
- 電力ポリシングがイネーブルの場合、スイッチはリアルタイムの消費電力を装置に割り当てられた 最大電力と比較して、消費電力をポリシングします。カットオフ電力とも呼ばれる、PoE ポートで の最大消費電力の詳細については、「PoE ポートでの最大電力割り当て(カットオフ電力)」 (P.11-9)を参照してください。

装置がポートで最大電力割り当て以上の電力を使用すると、スイッチは、スイッチ コンフィギュ レーションに基づいて、ポートへの電力をオフにするか、受電装置に電力を供給しながら syslog メッセージを生成して LED (ポート LED はオレンジ色で点滅)を更新することができます。デ フォルトでは、すべての PoE ポートで消費電力のポリシングはディセーブルになっています。

PoEの errdisable ステートからのエラー回復がイネーブルの場合、指定の時間の経過後、スイッチ は PoE ポートを errdisable ステートから自動的に回復させます。

エラー回復がディセーブルの場合、shutdown および no shutdown インターフェイス コンフィ ギュレーション コマンドを使用して、手動で PoE ポートをイネーブルにできます。

4. ポリシングがディセーブルの場合、受電装置が PoE ポートに割り当てられた最大電力より多くの 量を消費し、スイッチに悪影響を与える可能性がある場合でも、アクションは実行されません。

PoE ポートでの最大電力割り当て(カットオフ電力)

電力ポリシングがイネーブルの場合、スイッチは次の順序でいずれかの値を PoE ポートでのカットオ フ電力とします。

- power inline consumption default wattage グローバル コンフィギュレーション コマンドまたはイ ンターフェイス コンフィギュレーション コマンドを入力する場合、スイッチがポート用に確保す るユーザ定義の電力レベル
- **2.** power inline auto max *max-wattage* または power inline static max *max-wattage* インターフェイ ス コンフィギュレーション コマンドを入力する場合、ポートで許可される電力を制限するユーザ 定義の電力レベル
- 3. CDP パワー ネゴシエーションまたは IEEE 分類を使用してスイッチが設定した装置の消費電力
- 4. スイッチが設定したデフォルトの消費電力 (デフォルト値は 15.4 W)

power inline consumption default *wattage* または **power inline [auto | static max]** *max-wattage* コマンドを入力することにより、カットオフ電力値を手動で設定するには、前述の一覧の1番目または2番目の方法を使用します。手動でカットオフ電力値を設定していない場合、スイッチが CDP パワー ネゴシエーションまたは装置の IEEE 分類を使用して、自動的に値を決定します。これが前述の3番めの方式となります。スイッチがこれらの方式のうち、どの方式を使用しても値を決定できない場合、15.4Wというデフォルト値を使用します(一覧の4番めの方式)。

電力消費値

ポートの初期電力割り当ておよび最大電力割り当てを設定することができます。ただし、これらの値 は、スイッチが PoE ポートの電力をオンまたはオフにするときを指定するために設定する値です。最 大電力割り当ては、受電装置の実際の電力と同じではありません。スイッチによって電力ポリシング に使用される実際のカットオフ電力値は、設定済みの電力値と同等ではありません。

電力ポリシングがイネーブルの場合、スイッチは、スイッチポートで、受電装置の消費電力を超える 消費電力ポリシングを行います。最大電力割り当てを手動で設定する場合、スイッチポートと受電装 置間のケーブルでの電力損失を考慮する必要があります。カットオフ電力とは、受電装置の定格消費電 力とケーブル上での最悪時の電力損失を合計したものです。

受電装置による PoE ポートでの実際の消費電力量は、カットオフ電力値に較正係数の 500 mW(0.5 W)を加えたものになります。実際のカットオフ値は近似値で、設定値ごとに設定値のパーセンテージという割合で異なります。たとえば、設定済みのカットオフ電力が 12 W の場合、実際のカットオフ値は 11.4 W で、設定値より 0.05% 小さくなっています。

スイッチの PoE がイネーブルの場合、電力ポリシングをイネーブルにすることをお勧めします。たと えば、ポリシングがディセーブルで、power inline auto max 6300 インターフェイス コンフィギュ レーション コマンドを使用してカットオフ値を設定すると、PoE ポートに設定される最大電力割り当 ては 6.3 W (6300 mW)です。装置が 6.3 W までの電力を必要とする場合、スイッチはポートに接続 されている装置に電力を供給します。CDP によるパワー ネゴシエーション実施後の値または IEEE 分 類値が設定済みカットオフ値を超えると、スイッチは接続されている装置に電力を供給しなくなりま す。スイッチは PoE ポートで電力をオンにしてから、装置のリアルタイム消費電力のポリシングを行 わないため、この装置は最大割り当て量を超えて電力を消費できることになり、スイッチと他の PoE ポートに接続されている装置に悪影響が生じる場合があります。

スイッチは内部電源装置 Cisco Redundant Power System 2300 (RPS 2300) をサポートしており、受電装置が使用可能な総電力量は電源装置の設定によって異なります。

 電源装置を取り外して低電力の新しい電源装置に交換すると、スイッチは受電装置に対して十分な 電力を供給できなくなり、autoモードでポート番号の降順に従って PoE ポートへの電力供給を拒 否します。これでもまだ十分な電力がない場合、スイッチは、staticモードでポート番号の降順に 従って PoE ポートへの電力供給を拒否します。 新しい電源装置の電力が前の電源装置より大きく、スイッチが大電力を使用できる場合、スイッチ は static モードでポート番号の昇順に従って PoE ポートへの電力供給を許可します。これでもまだ 使用可能な電力がある場合、スイッチは、ポート番号の昇順に従って auto モードで PoE ポートへの電力供給を許可します。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。

図 11-1の構成では、VLAN 20 のホスト A が VLAN 30 のホスト B にデータを送信する場合、データ はホスト A からスイッチを経由してルータへ送られたあと、再びスイッチに戻ってからホスト B へ送 られる必要があります。



図 11-1 レイヤ 2 スイッチによる VLAN の接続

インターフェイス コンフィギュレーション モードの使用方 法

スイッチは、次のインターフェイス タイプをサポートします。

- 物理ポート:スイッチポート
- VLAN:スイッチ仮想インターフェイス
- ポート チャネル: EtherChannel インターフェイス

インターフェイス範囲も設定できます(「インターフェイス範囲の設定」(P.11-12)を参照)。

物理インターフェイス(ポート)を設定するには、インターフェイスのタイプ、モジュール番号、およ びスイッチ ポート番号を指定し、インターフェイス コンフィギュレーション モード を開始します。

- タイプ: スイッチでのサポートに応じたポート タイプ。予想されるタイプには、10/100 Mb/s イー サネットにはファスト イーサネット (fastethernet または fa)、10/100/1000 Mb/s イーサネット ポートにはギガビット イーサネット (gigabitethernet または gi)、10,000 Mb/s には 10 ギガビット イーサネット (tengigabitethernet または te)、Small Form-factor Pluggable (SFP) モジュールに はギガビット イーサネット インターフェイスです。
- モジュール番号:スイッチのモジュールまたはスロット番号(常に0)。
- ポート番号:スイッチ上のインターフェイス番号。ポート番号は常に1で始まり、スイッチに向かって左のポートから順に番号が付けられています。たとえば、fastethernet0/1またはgigabitethernet0/1のようになります。複数のインターフェイスタイプがある場合は(10/100ポートおよび SFP モジュール ポートなど)、ポート番号は2番めのインターフェイスタイプであるgigabitethernet0/1から再開します。10/100/1000ポートとSFP モジュール ポートのあるスイッチの場合、SFP モジュール ポートの番号は10/100/1000ポートのあとに連続して付けられます。

スイッチを確認することで物理インターフェイスを識別できます。**show** 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。以降、この章では、主に物理インターフェイスの設定手順について説明します。

インターフェイスの設定手順

以下の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

ステップ1 特権 EXEC プロンプトに configure terminal コマンドを入力します。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#

ステップ 2 interface グローバル コンフィギュレーション コマンドを入力します。

ギガビット イーサネット ポート1 でのインターフェイス タイプおよびインターフェイス番号の識別方 法の例は、次のとおりです。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)#



インターフェイス タイプとインターフェイス番号の間に入れるスペースはオプションです。

ステップ3 各 interface コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。入力するコマンドによって、そのインターフェイスで稼動するプロトコ ルとアプリケーションが定義されます。別のインターフェイス コマンドまたは end を入力して特権 EXEC モードに戻ると、コマンドが収集されてインターフェイスに適用されます。

> また、interface range または interface range macro グローバル コンフィギュレーション コマンドを 使用すると、一定範囲のインターフェイスを設定することもできます。ある範囲内で設定したインター フェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければ なりません。

ステップ4 インターフェイスを設定してから、「インターフェイスのモニタおよびメンテナンス」(P.11-31) に示した show 特権 EXEC コマンドで、そのステータスを確認してください。

show interfaces 特権 EXEC コマンドを使用して、スイッチ上のまたはスイッチ用に設定されたすべて のインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定し たインターフェイスのレポートが出力されます。

インターフェイス範囲の設定

interface range グローバル コンフィギュレーション コマンドを使用して、同じコンフィギュレーショ ンパラメータを持つ複数のインターフェイスを設定できます。インターフェイス レンジ コンフィギュ レーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンド パラメー タはその範囲内のすべてのインターフェイスに対するものと見なされます。

同じパラメータでインターフェイス範囲を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface range { <i>port-range</i> macro <i>macro_name</i> }	設定するインターフェイス範囲(VLAN または物理ポート)を指 定し、インターフェイス コンフィギュレーション モードを開始し ます。
		 interface range コマンドを使用すると、最大 5 つのポート範囲または定義済みマクロを 1 つ設定できます。
		 macro 変数については、「インターフェイス レンジ マクロの 設定および使用方法」(P.11-14)を参照してください。
		 カンマで区切った port-range では、各エントリに対応するインターフェイス タイプを入力し、カンマの前後にスペースを含めます。
		 ハイフンで区切った port-range では、インターフェイス タイ プの再入力は不要ですが、ハイフンの前後にスペースを入力 する必要があります。
ステップ 3		この時点で、通常のコンフィギュレーション コマンドを使用し て、範囲内のすべてのインターフェイスにコンフィギュレーショ ンパラメータを適用します。各コマンドは、入力されたとおりに 実行されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces [interface-id]	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

interface range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項に留意 してください。

- スイッチでのポート タイプに応じた port-range の有効なエントリは次のとおりです。
 - vlan vlan-ID, VLAN ID $\ddagger 1 \sim 4094_{\circ}$



コマンドラインインターフェイスには複数の VLAN を設定するオプションが表示され ますが、これらのオプションはサポートされていません。

- モジュールは常に0です。
- fastethernet module/{first port} {last port}、モジュールは常に 0。
- gigabitethernet module/{first port} {last port}、モジュールは常に 0。
- port-channel port-channel-number port-channel-number, port-channel-number $t = 1 6_{\circ}$



ポート チャネルを指定して interface range コマンドを使用する場合は、先頭および最後のチャネル番号をアクティブなポート チャネルにする必要があります。

interfacerange コマンドを使用するときは、先頭のインターフェイス番号とハイフンの間にスペースが必要です。

たとえば、interface range gigabitethernet 0/1 - 4 は有効な範囲ですが、interface range gigabitethernet0/1-4 は無効な範囲です。

- interface range コマンドが機能するのは、interface vlan コマンドで設定された VLAN インターフェイスに限られます。show running-config 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。show running-config コマンドで表示されない VLAN インターフェイスに interface range コマンドを使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ(すべてがファスト イーサネット ポート、 すべてがギガビット イーサネット ポート、すべてが EtherChannel ポート、またはすべてが VLAN)でなければなりません。ただし、1 つのコマンド内で複数のレンジを組み合わせることが できます。

次の例では、interface range グローバル コンフィギュレーション コマンドを使用して、ポート1~2 の速度を 100 Mb/s に設定する方法を示します。

Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)# speed 100

この例では、カンマを使用して別のインターフェイス タイプ ストリングを追加し、ファスト イーサ ネット ポート1~3と、ギガビット イーサネット ポート1および2の両方をイネーブルにし、フロー 制御ポーズ フレームを受信できるようにします。

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 3, gigabitethernet0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

インターフェイス レンジ モードで複数のコンフィギュレーション コマンドを入力した場合、各コマン ドは入力した時点で実行されます。インターフェイス レンジ モードを終了したあとで、コマンドが バッチ処理されるわけではありません。コマンドの実行中にインターフェイス レンジ モードを終了す ると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コ マンド プロンプトが再表示されるのを待ってから、インターフェイス レンジ コンフィギュレーション モードを終了してください。

インターフェイス レンジ マクロの設定および使用方法

インターフェイス レンジ マクロを作成すると、設定するインターフェイスの範囲を自動的に選択でき ます。interface range macro グローバル コンフィギュレーション コマンドで macro キーワードを使 用するには、まず define interface-range グローバル コンフィギュレーション コマンドでマクロを定 義する必要があります。

インターフェイス レンジマクロを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	define interface-range macro_name interface-range	インターフェイス レンジ マクロを定義して NVRAM(不揮発性 RAM)に保存します。
		 macro_name は、最大 32 文字の文字列です。
		 マクロには、カンマで区切ったインターフェイスを5つまで 含めることができます。
		 それぞれの interface-range は、同じポート タイプで構成され ていなければなりません。
ステップ 3	interface range macro macro_name	<i>macro_name</i> の名前でインターフェイスレンジマクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。
		ここで、通常のコンフィギュレーション コマンドを使用して、定 義したマクロ内のすべてのインターフェイスに設定を適用できま す。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config include define	定義済みのインターフェイス レンジ マクロの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マクロを削除するには、no define interface-range *macro_name* グローバル コンフィギュレーション コマンドを使用します。

define interface-range グローバル コンフィギュレーション コマンドを使用するときは、次の注意事項 に留意してください。

- スイッチでのポート タイプに応じた interface-range の有効なエントリは次のとおりです。
 - vlan vlan-ID, VLAN ID は 1 \sim 4094.



コマンドライン インターフェイスには複数の VLAN を設定するオプションが表示され ますが、これらのオプションはサポートされていません。

- fastethernet module/{first port} {last port}、モジュールは常に 0。
- gigabitethernet module/{first port} {last port}、モジュールは常に 0。
- port-channel port-channel-number port-channel-number, port-channel-number $\lg 1 \sim 6_{\circ}$



ポート チャネルを指定して interface range コマンドを使用する場合は、先頭および最 後のチャネル番号をアクティブなポート チャネルにする必要があります。

- interface-range を入力するときは、最初のインターフェイス番号とハイフンの間にスペースを入れます。
 - たとえば、gigabitethernet0/1 4 は有効な範囲ですが、gigabitethernet0/1-4 は無効な範囲です。
- VLAN インターフェイスは、interface vlan コマンドで設定しておかなければなりません。show running-config 特権 EXEC コマンドを使用すると、設定されている VLAN インターフェイスが表示されます。show running-config コマンドで表示されない VLAN インターフェイスを interface-range として使用することはできません。
- ある範囲内のすべてのインターフェイスは、同じタイプ(すべてがファストイーサネットポート、 すべてがギガビットイーサネットポート、すべてが EtherChannel ポート、またはすべてが VLAN)でなければなりません。ただし、1つのマクロ内で複数のインターフェイスタイプを組み 合わせることができます。

次に、enet_list という名前のインターフェイス範囲マクロを定義して、ポート1および2を含め、マクロ設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 2
Switch(config)# end
Switch# show running-config | include define
Switch# define interface-range enet_list gigabitethernet0/1 - 2
```

次に、複数のタイプのインターフェイスを含むマクロ macrol を作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macrol fastethernet0/1 - 2, gigabitethernet0/1 - 2
Switch(config)# end
```

次に、インターフェイス レンジ マクロ enet_list に対するインターフェイス レンジ コンフィギュレー ション モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

次に、インターフェイス レンジ マクロ enet list を削除し、処理を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

イーサネット インターフェイスの設定

ここでは、次の設定情報について説明します。

- 「イーサネットインターフェイスのデフォルト設定」(P.11-16)
- 「デュアルパーパス アップリンク ポートのタイプの設定」(P.11-17)
- 「インターフェイス速度およびデュプレックス モードの設定」(P.11-19)
- 「IEEE 802.3x フロー制御の設定」(P.11-22)
- 「インターフェイスでの Auto-MDIX の設定」(P.11-23)
- 「PoE ポートの電力管理モードの設定」(P.11-24)
- 「PoE ポートに接続された装置のパワー バジェット」(P.11-26)
- 「電力ポリシングの設定」(P.11-28)
- 「インターフェイスに関する記述の追加」(P.11-29)

イーサネット インターフェイスのデフォルト設定

表 11-2 は、イーサネット インターフェイスのデフォルト設定を示しています。表に示されている VLAN パラメータの詳細については、第 13 章「VLAN の設定」を参照してください。また、ポートへ のトラフィック制御の詳細については、第 23 章「ポート単位のトラフィック制御の設定」を参照してく ださい。

機能	デフォルト設定
VLAN 許容範囲	VLAN 1 \sim 4094
デフォルト VLAN(アクセス	VLAN 1
ホート用)	
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1
VLAN トランキング	Switchport mode dynamic auto (DTP をサポート)
ポート イネーブル ステート	すべてのポートがイネーブル
ポート記述	未定義
速度	自動ネゴシエーション
デュプレックス モード	自動ネゴシエーション
フロー制御	フロー制御は receive: off に設定されます。送信パケットでは常 にオフです。
EtherChannel (PAgP)	すべてのイーサネット ポートでディセーブル。第 36 章 「EtherChannel およびリンクステート トラッキングの設定」
ポート ブロッキング(不明マルチ キャストおよび不明ユニキャスト トラフィック)	ディセーブル (ブロッキングされない)。「ポート ブロッキングの 設定」(P.23-8) を参照してください。
ブロードキャスト、マルチキャス ト、およびユニキャスト ストーム 制御	ディセーブル「ストーム制御のデフォルト設定」(P.23-3)を参 照してください。

表 11-2 レイヤ2 イーサネット インターフェイスのデフォルト設定
機能	デフォルト設定
保護ポート	ディセーブル 「保護ポートの設定」(P.23-7)を参照してください。
ポートセキュリティ	ディセーブル 「ポート セキュリティのデフォルト設定」 (P.23-12)を参照してください。
PortFast	ディセーブル 「オプションのスパニング ツリー機能のデフォル ト設定」(P.18-11) を参照してください。
Auto-MDIX	 イネーブル (注) 受電装置がクロス ケーブルでスイッチに接続されている 場合、スイッチは、IEEE 802.3af に完全には準拠してい ない、Cisco IP Phone やアクセス ポイントなどの準規格 の受電をサポートしていない場合があります。これは、 スイッチ ポート上で Automatic Medium-Dependent Interface Crossover (Auto-MIDX) がイネーブルかどう かは関係ありません。
Power over Ethernet (PoE)	イネーブル (auto)。
キープアライブ メッセージ	SFP モジュールでディセーブル。他のすべてのポートでイネーブ ル。

表 11-2 レイヤ2 イーサネット インターフェイスのデフォルト設定 (続き)

デュアルパーパス アップリンク ポートのタイプの設定

一部の 2960 スイッチでは、デュアルパーパス アップリンク ポートがサポートされています。デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、media-type インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。詳細については、「デュアルパーパス アップリンクポート」(P.11-4)を参照してください。

速度およびデュプレックスの設定が行えるようにアクティブにするデュアルパーパス アップリンクを選 択するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するデュアルパーパス アップリンク ポートを指定し、イン
		ターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	media-type {auto-select rj45 sfp}	インターフェイスとデュアルパーパス アップリンク ポートのタイ
		プを選択します。キーワードの意味は次のとおりです。
		 auto-select:スイッチが動的にタイプを選択します。リンクがアップの状態になると、アクティブなリンクがダウンの状態になるまで、スイッチによりその他のタイプがディセーブル化されます。アクティブなリンクがダウンの状態になると、いずれかのリンクがアップの状態になるまで、スイッチにより両方のタイプがイネーブル化されます。auto-select モードでは、スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます(デフォルト)。インストールされている SFP モジュールのタイプによって、スイッチで自動的に選択が行えない場合もあります。詳細については、この手順のあとの説明を参照してください。
		 rj45:スイッチが SFP モジュール インターフェイスをディ セーブル化します。このポートに SFP モジュールを接続する 場合、RJ-45 側がダウンしている、または接続していない場 合でも、リンクを確立することはできません。このモードで は、デュアルパーパス ポートは 10/100/1000BASE-TX イン ターフェイスと同様の動作をします。このインターフェイス タイプに対応した速度およびデュプレックスの設定が可能で す。
		 sfp:スイッチが RJ-45 インターフェイスをディセーブル化します。この RJ-45 ポートにケーブルを接続している場合、 SFP モジュール側がダウンしている、または SFP モジュールが接続していない場合でも、リンクを確立することはできません。インストールされている SFP モジュールのタイプに基づいて、このインターフェイスタイプに対応した速度およびデュプレックスの設定が可能です。
		速度およびデュプレックスの詳細については、「速度とデュプレックスモードの設定時の注意事項」(P.11-19)を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces <i>interface-id</i> transceiver properties	設定値を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、media-type auto interface または no media-type インターフェイス コ ンフィギュレーション コマンドを使用します。

スイッチにより両方のタイプが速度およびデュプレックスの自動ネゴシエーションに設定されます(デフォルト)。auto-select を設定した場合、speed および duplex インターフェイス コンフィギュレー ション コマンドによる設定は行えません。

スイッチの電源を ON にした場合、または shutdown および no shutdown インターフェイス コンフィ ギュレーション コマンドでデュアルパーパス アップリンク ポートをイネーブル化した場合、SFP モ ジュール インターフェイスが選択されます。これ以外の場合、最初にアップの状態になったリンクの タイプに基づいて、アクティブなリンクが選択されます。 このスイッチと 100BASE-x (-x は -BX、-FX、-FE、-LX のいずれか) SFP モジュールを組み合わせ ると、次のように動作します。

- 100BASE-x SFP モジュールがモジュール スロットに搭載されていて、RJ-45 側にリンクがない場合、スイッチにより RJ-45 インターフェイスがディセーブル化され、SFP モジュール インターフェイスが選択されます。ケーブルが接続されていない場合や、SFP モジュール側にリンクがない場合でも、このようになります。
- 100BASE-x SFP モジュールが搭載されていて、RJ-45 側にリンクがある場合、このリンクを使用して動作が続行します。リンクがダウンの状態になると、スイッチにより RJ-45 側がディセーブル化され、SFP モジュール インターフェイスが選択されます。
- 100BASE-*x* SFP モジュールを取り外すと、スイッチにより再び自動的にタイプが選択され (auto-select)、再び RJ-45 側がイネーブル化されます。

100BASE-FX-GE SFP モジュールの場合、この機能はありません。

インターフェイス速度およびデュプレックス モードの設定

サポートされるポート タイプに応じて、スイッチのイーサネット インターフェイスは、全二重または 半二重モードのいずれかで、10、100、1000、または 10,000 Mb/s で動作します。全二重モードの場 合、2 つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モー ドで動作します。これは、各ステーションがトラフィックを受信するか、送信するかのどちらか一方し かできないことを意味します。

スイッチ モデルには、ファスト イーサネット(10/100 Mb/s)ポート、ギガビット イーサネット (10/100/1000 Mb/s) ポート、10 ギガビット モジュール ポート、および SFP モジュールをサポートす る SFP モジュール スロットの組み合わせが含まれます。

ここでは、インターフェイス速度とデュプレックス モードの設定手順について説明します。

- 「速度とデュプレックス モードの設定時の注意事項」(P.11-19)
- 「インターフェイス速度およびデュプレックス パラメータの設定」(P.11-20)

速度とデュプレックス モードの設定時の注意事項

インターフェイス速度およびデュプレックス モードを設定するときには、次の注意事項に留意してく ださい。

- ファストイーサネット(10/100 Mbps)ポートは、すべての速度およびデュプレックスオプションをサポートします。
- ギガビット イーサネット(10/100/1000 Mbps) ポートは、すべての速度オプションとデュプレックスオプション(自動、半二重、全二重)をサポートします。ただし、1000 Mbps で稼動させているギガビット イーサネット ポートは、半二重モードをサポートしません。
- SFP モジュール ポートの場合、次の SFP モジュール タイプによって速度とデュプレックスの CLI (コマンドライン インターフェイス) オプションが変わります。
 - 1000 BASE-x (xには、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポートは、speed インターフェイス コンフィギュレーション コマンドで nonegotiate キーワードを サポートします。デュプレックス オプションはサポートされません。
 - 1000BASE-T SFP モジュール ポートは、10/100/1000 Mbps ポートと同一の速度とデュプレックスオプションをサポートします。

- 100BASE-x (xには、BX、CWDM、LX、SX、ZX が適宜入ります) SFP モジュール ポート は、100 Mbps のみサポートします。これらのモジュールは、全二重および半二重オプション をサポートしますが、自動ネゴシエーションをサポートしません。

スイッチでサポートされる SFP モジュールについては、各製品のリリース ノートを参照してくだ さい。

- 回線の両側で自動ネゴシエーションがサポートされる場合は、できるだけデフォルトの auto ネゴシエーションを使用してください。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で auto 設定を使用しないでください。
- STP がイネーブルの場合にポートを再設定すると、スイッチがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯し ます。



インターフェイス速度とデュプレックス モードの設定を変更すると、再設定時にシャットダウンが 発生し、インターフェイスが再びイネーブルになることがあります。

インターフェイス速度およびデュプレックス パラメータの設定

物理インターフェイスの速度およびデュプレックス モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。
ステップ 3	speed {10 100 1000 auto [10 100 1000] nonegotiate}	インターフェイスに対する適切な速度パラメータを入力します。 • インターフェイスの速度を指定するには、10、100、または 1000 を入力します。1000 キーワードを使用できるのは、 10/100/1000 Mbps ポートに対してだけです。
		 インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、autoを入力します。autoキーワードと一緒に 10、100、または1000 キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。
		 nonegotiate キーワードを使用できるのは、SFP モジュール ポートに対してだけです。SFP モジュール ポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポー トしていないデバイスに接続されている場合は、ネゴシエー トしないように設定できます。
		速度の設定の詳細については、「速度とデュプレックス モードの 設定時の注意事項」(P.11-19)を参照してください。

	コマンド	目的
ステップ 4	duplex {auto full half}	インターフェイスのデュプレックス パラメータを入力します。
		半二重モードをイネーブルにします(10 または 100Mbps のみで 動作するインターフェイスの場合)。1000 Mbps で動作するイン ターフェイスには半二重モードを設定できません。
		デュプレックスの設定の詳細については、「速度とデュプレックス モードの設定時の注意事項」(P.11-19)を参照してください。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id	インターフェイス速度およびデュプレックス モード設定を表示し ます。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの速度およびデュプレックス設定(自動ネゴシエーション)に戻すに は、no speed および no duplex インターフェイス コンフィギュレーション コマンドを使用します。す べてのインターフェイス設定をデフォルトに戻すには、default interface *interface-id* インターフェイ ス コンフィギュレーション コマンドを使用します。

次に、10/100Mbps ポートでインターフェイスの速度を 10 Mbps に、デュプレックス モードを半二重 に設定する例を示します。

Switch# configure terminal Switch(config)# interface fasttethernet0/3 Switch(config-if)# speed 10 Switch(config-if)# duplex half

次に、10/100/1000 Mbps ポートで、インターフェイスの速度を 100 Mbps に設定する例を示します。

Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# speed 100

IEEE 802.3x フロー制御の設定

フロー制御により、接続しているイーサネット ポートは、輻輳しているノードがリンク動作をもう 方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あ るポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズ フレームを送信 することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通 知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、 輻輳時のデータ パケット損失が防止されます。



スイッチのポートは、ポーズ フレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスのポーズ フレームを受信(receive)する能力を on、off、または desired に設定します。デフォルトの状態は off です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイス、 または必要ではないがフロー制御パケットを送信できる接続デバイスに対して動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- receive on (または desired): ポートはポーズ フレームを送信できませんが、ポーズ フレームを 送信する必要のある、または送信できる接続デバイスと組み合わせて使用できます。ポーズ フ レームの受信は可能です。
- receive off:フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側のデバイスもポーズフレームの送受信を行いません。

(注)

コマンドの設定と、その結果生じるローカルおよびリモート ポートでのフロー制御解決の詳細につい ては、このリリースのコマンド リファレンスに記載された flowcontrol インターフェイス コンフィ ギュレーション コマンドを参照してください。

インターフェイス上でフロー制御を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	
configure terminal	グローバル コンフィギュレーション モードを開始します。
interface interface-id	設定する物理インターフェイスを指定し、インターフェイン コンフィギュレーション モードを開始します。
flowcontrol {receive} {on off desired}	ポートのフロー制御モードを設定します。
end	特権 EXEC モードに戻ります。
show interfaces interface-id	インターフェイス フロー制御の設定を確認します。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

フロー制御をディセーブルにする場合は、flowcontrol receive off インターフェイス コンフィギュレー ション コマンドを使用します。

次に、ポート上のフロー制御をオンにする例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# flowcontrol receive on Switch(config-if)# end

インターフェイスでの Auto-MDIX の設定

インターフェイス上の Auto-MDIX がイネーブルに設定されている場合、インターフェイスが必要な ケーブル接続タイプ(ストレートまたはクロス)を自動的に検出し、接続を適切に設定します。 Auto-MDIX 機能を使用せずにスイッチを接続する場合、サーバ、ワークステーション、またはルータ などのデバイスの接続にはストレート ケーブルを使用し、他のスイッチやリピータの接続にはクロス ケーブルを使用する必要があります。Auto-MDIX がイネーブルの場合、他のデバイスとの接続にはど

す。ケーブル接続の詳細については、『Hardware Installation Guide』を参照してください。 Auto-MDIX はデフォルトでイネーブルです。Auto-MDIX をイネーブルに設定する場合、Auto-MDIX 機能が正しく動作するようにインターフェイスの速度およびデュプレックスを auto に設定する必要が あります。

ちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行いま

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mb/s インターフェイスでサポートされます。 1000BASE-SX または 1000BASE-LXSFP モジュール インターフェイスではサポートされていません。

表 11-3 に、Auto-MDIX の設定およびケーブル接続ごとのリンク ステートを示します。

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい 場合	ケーブル接続が正しく ない場合
オン	オン	リンク アップ	リンク アップ
オン	オフ	リンク アップ	リンク アップ
オフ	オン	リンク アップ	リンク アップ
オフ	オフ	リンク アップ	リンク ダウン

表 11-3 リンク状態と Auto-MDIX の設定

インターフェイス上で Auto-MDIX を設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
speed auto	接続されたデバイスと速度の自動ネゴシエーションを行うようにイン ターフェイスを設定します。
duplex auto	接続されたデバイスとデュプレックス モードの自動ネゴシエーション を行うようにインターフェイスを設定します。
mdix auto	インターフェイス上で Auto-MDIX をイネーブルにします。
end	特権 EXEC モードに戻ります。
show controllers ethernet-controller <i>interface-id</i> phy	インターフェイスで Auto-MDIX の動作ステートを確認します。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
	コマンド configure terminal interface interface-id speed auto duplex auto mdix auto end show controllers ethernet-controller interface-id phy copy running-config startup-config

Auto-MDIX をディセーブルにするには、no mdix auto インターフェイス コンフィギュレーション コ マンドを使用します。 次に、ポート上の Auto-MDIX をイネーブルにする例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# speed auto Switch(config-if)# duplex auto Switch(config-if)# mdix auto Switch(config-if)# end

PoE ポートの電力管理モードの設定



PoE コマンドは、スイッチで LAN Base イメージが実行されている場合にだけサポートされます。

ほとんどの場合、デフォルトの設定(自動モード)の動作は適切に行われ、プラグアンドプレイ動作が 提供されます。それ以上の設定は必要ありません。しかし、PoE ポートの優先順位を上げたり、PoE ポートをデータ専用にしたり、最大ワット数を指定して高電力受電装置をポートで禁止したりする場合 は、次の手順を実行します。



PoE 設定を変更するとき、設定中のポートでは電力が低下します。新しい設定、その他の PoE ポート の状態、パワーバジェットの状態により、そのポートの電力は再びアップしない場合があります。た とえば、ポート1が自動でオンの状態になっていて、そのポートを固定モードに設定するとします。ス イッチはポート1から電力を取り除き、受電装置を検出してポートに電力を再び供給します。ポート1 が自動でオンの状態になっていて、最大ワット数を10Wに設定した場合、スイッチはポートから電力 を取り除き、受電装置を再び検出します。スイッチは、受電装置がクラス1、クラス2、またはシスコ 専用受電装置のいずれかの場合に、ポートに電力を再び供給します。

電力管理モードを PoE 対応ポートで設定するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	<pre>power inline {auto [max max-wattage] never static [max max-wattage]}</pre>	ポートに PoE モードを設定します。キーワードの意味は次のとおり です。
		• auto:受電装置検出をイネーブルにします。十分な電力がある 場合は、装置の検出後に PoE ポートに電力を自動的に割り当て ます。これがデフォルトの設定です。
		 (任意) max max-wattage: ポートで許可する電力を制限します。 指定できる範囲は 4000 ~ 15400 ミリワットです。値を指定しな い場合は、最大電力まで供給できます(15400 ミリワット)。
		 never:装置検出とポートへの電力供給をディセーブルにします。
		 ポートにシスコの受電装置が接続されている場合は、power inline never コマンドでポートを設定しないでください。問題のあるリンクアップが発生し、ポートが errdisable ステートになることがあります。
		 static:受電装置検出をイネーブルにします。スイッチが受電装置を検出する前に、ポートへの電力を事前に割り当てます(確保します)。スイッチは、装置が接続されていなくてもこのポートに電力を予約し、装置の検出時に電力が供給されることを保証します。
		スイッチは、自動モードに設定されたポートに電力を割り当てる前 に、固定モードに設定されたポートに PoE を割り当てます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show power inline [interface-id]	スイッチまたは指定されたインターフェイスの PoE ステータスを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

show power inline ユーザ EXEC コマンドの出力については、このリリースのコマンド リファレンス を参照してください。PoE 関連の詳細については、「PoE スイッチ ポートのトラブルシューティング」 (P.37-13) を参照してください。音声 VLAN の設定の詳細については、第15章「音声 VLAN の設定」 を参照してください。

PoE ポートに接続された装置のパワー バジェット

シスコの受電装置が PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol (CDP) を使用して*実際に*装置が消費する電力量を決定して、それに応じてパワーバジェットを調整します。 CDP プロトコルはシスコの受電装置で動作し、IEEE サードパーティの受電装置には適用されません。こ の装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じてパワーバジェッ トを調整します。受電装置が Class 0 (クラスステータスは不明)または Class 3 である場合、実際に 必要な電力量に関係なく、スイッチはポート用に 15,400 ミリワットの電力を確保します。受電装置が 実際の電力消費量よりも高いクラスであるか、または電力分類(デフォルトで Class 0)をサポートし ない場合、スイッチは IEEE クラス情報を使用してグローバル パワーバジェットを追跡するので、少 しの装置にしか電力を供給しません。

power inline consumption wattage コンフィギュレーション コマンドを使用することで、IEEE 分類で 指定されたデフォルトの電力要件を無効にできます。IEEE 分類で指定された電力と実際に装置が必要 とする電力の差は、追加の装置が使用するためグローバル パワー バジェットに入れられます。した がって、スイッチのパワー バジェットを拡張してもっと効率的に使用できます。

たとえば、スイッチが各 PoE ポートで 15,400 ミリワットの電力を確保した場合、接続できる Class0 の受電装置は 24 台だけです。Class0 の装置の電力要件が実際には 5000 ミリワットである場合、消費 ワット数を 5000 ミリワットに設定すると、最大 48 台の装置を接続できます。24 ポートまたは 48 ポート スイッチで利用できる PoE 総出力電力は 370,000 ミリワットです。



慎重にスイッチのパワー バジェットを計画し、電源装置がオーバーサブスクライブ状態にならない ようにしてください。

(注)

手動でパワーバジェットを設定する場合、スイッチと受電装置の間のケーブルでの電力消失を考慮す る必要があります。

power inline consumption default *wattage* または **no power inline consumption default** グローバル コンフィギュレーション コマンドを入力する、あるいは power inline consumption wattage または *no* **power inline consumption** インターフェイス コンフィギュレーション コマンドを入力すると、次の注 意メッセージが表示されます。

%CAUTION: Interface interface-id: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty.Take precaution not to oversubscribe the power supply. It is recommended to enable power policing if the switch supports it. Refer to documentation.

電力供給が最大 20 パーセントのサブスクライブ過剰になると、スイッチは動作しますが、信頼性が低下します。電力供給 20 パーセントを超えてサブスクライブされると、短絡保護回路が始動しスイッチ はシャットダウンします。

IEEE 電力分類の詳細については、「Power over Ethernet (PoE) ポート」(P.11-5) を参照してください。

スイッチの各 PoE ポートに接続された受電装置へのパワー バジェット量を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	(任意) CDP をディセーブルにします。

	コマンド	目的
ステップ 3	power inline consumption default	スイッチの各 PoE ポートに接続された受電装置の消費電力を設定し
	wattage	ます。各デバイスで指定できる範囲は 4000 ~ 15400 ミリワットで
		す。デフォルト値は 15400 秒です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show power inline consumption	消費電力のステータスを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトに戻すには、no power inline consumption default グローバル コンフィギュレー ション コマンドを使用します。

特定の PoE ポートに接続された受電装置へのパワー バジェット量を設定するには、特権 EXEC モード で次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	(任意) CDP をディセーブルにします。
ステップ 3	interface interface-id	設定する物理ポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。
ステップ 4	power inline consumption wattage	スイッチの PoE ポートに接続された受電装置の消費電力を設定しま す。各デバイスで指定できる範囲は 4000 ~ 15400 ミリワットです。 デフォルト値は 15400 秒です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show power inline consumption	消費電力のステータスを表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no power inline consumption インターフェイス コンフィギュレーショ γ コマンドを使用します。

show power inline consumption 特権 EXEC コマンドの出力の詳細については、このリリースのコマ ンド リファレンスを参照してください。

電力ポリシングの設定

デフォルトでは、スイッチは接続されている受電装置の消費電力をリアルタイムで監視します。消費電 カに対するポリシングを行うようにスイッチを設定できます。デフォルトではポリシングはディセーブ ルです。

スイッチが使用するカットオフ電力値、消費電力値、および接続されている受電装置の実際の消費電力 の詳細については、「電力モニタリングおよび電力ポリシング」を参照してください。

PoE ポートに接続されている受電装置のリアルタイム消費電力ポリシングをイネーブルにするには、 特権 EXEC モードで、次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	設定する物理ポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。	
ステップ 3	power inline police [action log]	ポートでリアルタイム消費電力が最大電力割り当てを超えるときに、 次のいずれかのアクションを実行するようにスイッチを設定します。	
		 PoE ポートをシャットダウンし、このポートへの電力供給をオフ にし、error-dsabled ステートにする: power inline police コマ ンドを入力します。 	
		 (注) errdisable detect cause inline-power グローバル コンフィ ギュレーション コマンドを使用すると、PoE errdisable の原 因についてエラー検出をイネーブルにできます。errdisable recovery cause inline-power interval interval グローバル コ ンフィギュレーション コマンドを使用すると、PoE errdisable ステートから回復するためのタイマーをイネーブ ルにすることもできます。 	
		 ポートに電力を供給しながら syslog メッセージを生成する: power inline police action log コマンドを入力します。 	
		action log キーワードを入力しない場合、デフォルトのアクションに よってポートがシャットダウンされ、errdisable ステートになりま す。	
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。	
ステップ 5	errdisable detect cause inline-power	(任意) PoE errdisable ステートからのエラー回復をイネーブルにし、 PoE 回復メカニズム変数を設定します。	
	errdisable recovery cause inline-power	interval <i>interval</i> では、errdisable ステートから回復する時間を秒単 位で指定します。指定できる範囲は 30 ~ 86400 です。	
	および	デフォルトでは、回復間隔は 300 秒です。	
	errdisable recovery interval interval		
ステップ 6	exit	特権 EXEC モードに戻ります。	
ステップ 7	show power inline police	電力モニタリング ステータスを表示し、エラー回復設定を確認しま	
	show errdisable recovery	す。	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

リアルタイム消費電力のポリシングをディセーブルにするには、no power inline police インターフェ イス コンフィギュレーション コマンドを使用します。PoE errdisable の原因についてエラー回復を ディセーブルにするには、no errdisable recovery cause inline-power グローバル コンフィギュレー ション コマンドを使用します。

show power inline police 特権 EXEC コマンドの出力の詳細については、このリリースのコマンド リファレンスを参照してください。

インターフェイスに関する記述の追加

インターフェイスの機能に関する記述を追加できます。記述は、特権 EXEC コマンド show configuration、show running-config、および show interfaces の出力に表示されます。 インターフェイスに関する記述を追加するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	記述を追加するインターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。
ステップ 3	description string	インターフェイスに関する記述を追加します(最大 240 文字)。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id description	設定を確認します。
	または	
	show running-config	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

記述を削除するには、no description インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに記述を追加して、その記述を確認する例を示します。

Switch# config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet0/2 Switch(config-if)# description Connects to Marketing Switch(config-if)# end Switch# show interfaces gigabitethernet0/2 description Interface Status Protocol Description Gi0/2 admin down down Connects to Marketing

システム MTU の設定

すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送ユニット (MTU; Maximum Transmission Unit) サイズは、1500 バイトです。10 または 100 Mbps で動作するすべてのインター フェイスで MTU サイズを増やすには、system mtu グローバル コンフィギュレーション コマンドを使用します。また、system mtu jumbo グローバル コンフィギュレーション コマンドを使用すると、す べてのギガビット イーサネット インターフェイス上でジャンボ フレームをサポートするように MTU サイズを増やすことができます。

system mtu コマンドはギガビット イーサネット ポートには影響せず、system mtu jumbo コマンドは 10/100 ポートには影響しません。system mtu jumbo コマンドを設定していない場合、system mtu コ マンドの設定はすべてのギガビット イーサネット インターフェイスに適用されます。

個々のインターフェイスに MTU サイズを設定することはできません。すべての 10/100 インターフェ イスまたはすべてのギガビット イーサネット インターフェイスに対して設定されます。システムまた はジャンボ MTU サイズを変更した場合は、スイッチをリセットしなければ、新しい設定は有効になり ません。

スイッチの CPU が受信できるフレーム サイズは、system mtu または system mtu jumbo コマンドで 入力した値に関係なく、1998 バイトに制限されています。通常、転送されたフレームは CPU によって 受信されませんが、場合によっては、制御トラフィック、SNMP(簡易ネットワーク管理プロトコル)、 または Telnet へ送信されたトラフィックなどのパケットが CPU へ送信されることがあります。



レイヤ2ギガビットイーサネットインターフェイスが、10/100インターフェイスより大きいサイズの フレームを受け取るように設定されている場合、レイヤ2ギガビットイーサネットインターフェイス に着信するジャンボフレームとレイヤ210/100インターフェイスで発信されるジャンボフレームは廃 棄されます。

すべての 10/100 またはギガビット イーサネット インターフェイスで MTU サイズを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し ます。
ステップ 2	system mtu bytes	(任意) 10 または 100 Mb/s で動作するスイッチのす べてのインターフェイスに対して MTU サイズを変 更します。
		指定できる範囲は、1500 ~ 1998 バイトです。デ フォルトは 1500 バイトです。
ステップ 3	system mtu jumbo bytes	(任意) スイッチのすべてのギガビット イーサネット インターフェイスに対して MTU サイズを変更します。
		指定できる範囲は 1500 ~ 9000 バイトです。デフォ ルトは 1500 バイトです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	コンフィギュレーション ファイルに設定を保存しま す。
ステップ 6	reload	OS(オペレーティング システム)をリロードしま す。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

スイッチのリロード後、show system mtu 特権 EXEC コマンドを入力することによって、設定値を確認できます。

次に、ギガビット イーサネット ポートの最大パケット サイズを 1800 バイトに設定する例を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

次に、ギガビットイーサネットインターフェイスを範囲外の値に設定しようとした場合に表示される 応答の例を示します。

Switch(config) # system mtu jumbo 25000

% Invalid input detected at '^' marker.

インターフェイスのモニタおよびメンテナンス

ここでは、インターフェイスのモニタおよびメンテナンスについて説明します。

- 「インターフェイス ステータスのモニタ」(P.11-31)
- 「インターフェイスおよびカウンタのクリアとリセット」(P.11-32)
- 「インターフェイスのシャットダウンおよび再起動」(P.11-33)

インターフェイス ステータスのモニタ

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバー ジョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を 表示できます。表 11-4 に、このようなインターフェイス モニタ コマンドの一部を示します (特権 EXEC プロンプトに show? コマンドを入力すると、すべての show コマンドのリストが表示されま す)。これらのコマンドについては、『Cisco IOS Interface Command Reference, Release 12.2』で詳し く説明しています。これには、Cisco.com のホームページ (Documentation > Cisco IOS Software > 12.2 Mainline > Command References) からアクセス可能です。

表 11-4 インターフェイス用の show コマンド

コマンド	目的
<pre>show interfaces [interface-id]</pre>	(任意) すべてのインターフェイスまたは特定のインターフェイスの ステータスおよび設定を表示します。
show interfaces interface-id status [err-disabled]	(任意) インターフェイスのステータス、または errdisable ステート にあるインターフェイスの一覧を表示します。
<pre>show interfaces [interface-id] switchport</pre>	(任意) スイッチング ポートの管理上および動作上のステータスを表示します。
show interfaces [interface-id] description	(任意) 1 つのインターフェイスまたはすべてのインターフェイスに 関する記述とインターフェイスのステータスを表示します。
<pre>show ip interface [interface-id]</pre>	(任意) IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。

表 11-4 インターフェイス用の show コマンド (続き)

コマンド	目的
show interface [interface-id] stats	(任意)インターフェイスのスイッチング パスによる入出力パケット を表示します。
show interfaces transceiver properties	(任意) インターフェイスの速度およびデュプレックス設定を表示し ます。
<pre>show interfaces [interface-id] [{transceiver properties detail}] module number]</pre>	SFPモジュールに関する物理および動作ステータスを表示します。
<pre>show running-config interface [interface-id]</pre>	インターフェイスに対応する RAM 上の実行コンフィギュレーション を表示します。
show version	ハードウェア構成、ソフトウェアのバージョン、コンフィギュレー ション ファイルの名前とソース、ブート イメージを表示します。
show controllers ethernet-controller <i>interface-id</i> phy	インターフェイスの Auto-MDIX 動作ステートを表示します。
<pre>show power inline [interface-id]</pre>	スイッチまたはインターフェイスの PoE ステータスを表示します。
show power inline police	電力ポリシングのデータを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 11-5 に、カウンタのクリアとインターフェイスのリセットに使用できる特権 EXEC モードの clear コマンドを示します。

表 11-5 インターフェイス用の clear コマンド

コマンド	目的
clear counters [interface-id]	インターフェイスのカウンタをクリアします。
clear interface interface-id	インターフェイスのハードウェア ロジックをリセットします。
clear line [number console 0 vty number]	非同期シリアル回線に関するハードウェア ロジックをリセットします。

show interfaces 特権 EXEC コマンドによって表示されたインターフェイス カウンタをリセットするに は、clear counters 特権 EXEC コマンドを使用します。オプションの引数が特定のインターフェイス 番号から特定のインターフェイス タイプのみをクリアするように指定する場合を除いて、clear counters コマンドは、インターフェイスから現在のインターフェイス カウンタをすべてクリアします。



clear counters 特権 EXEC コマンドは、SNMP を使用して取得されたカウンタをクリアしません。 **show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能がディセーブ ルになり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、す べてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。 ルーティング アップデートには、インターフェイス情報は含まれません。

インターフェイスをシャットダウンするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開
		始します。
ステップ 2	interface {vlan vlan-id} {{fastethernet	設定するインターフェイスを選択します。
	gigabitethernet } <i>interface-id</i> } { port-channel <i>port-channel-number</i> }	
ステップ 3	shutdown	インターフェイスをシャットダウンします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。

インターフェイスを再起動するには、no shutdown インターフェイス コンフィギュレーション コマン ドを使用します。

インターフェイスがディセーブルになっていることを確認するには、**show interfaces** 特権 EXEC コマ ンドを使用します。ディセーブルになっているインターフェイスは、出力に *administratively down* と 表示されます。





Auto SmartPort マクロの設定

『Catalyst 2960 Switch Command Reference』には、コマンド構文および使用方法が記載されています。

- 「Auto SmartPort マクロおよびスタティック SmartPort マクロの概要」(P.12-2)
- 「Auto SmartPort の設定」(P.12-3)
- 「スタティック SmartPort マクロの設定」(P.12-18)
- 「Auto SmartPort マクロおよびスタティック SmartPort マクロの表示」(P.12-21)

Auto SmartPort マクロおよびスタティック SmartPort マ クロの概要

Auto SmartPort マクロは、ポートで検出されたデバイス タイプに基づいてポートを動的に設定します。 スイッチは、ポートで新しいデバイスを検出すると、そのポートに適切な Auto SmartPort マクロを適 用します。ポートにリンクダウン イベントがあると、スイッチはマクロを削除します。たとえば、 Cisco IP Phone をポートに接続すると、Auto SmartPort は自動的に IP Phone マクロを適用します。IP Phone マクロが適用されると、遅延に影響されやすい音声トラフィックを正しく処理できるように QoS (Quality Of Service)、セキュリティ機能、および専用の音声 VLAN がイネーブルになります。 Auto SmartPort では、デバイスからマクロへのマッピングにイベント トリガーが使用されます。

スイッチ ソフトウェアに組み込まれた Auto SmartPort マクロは、CLI コマンドの集まりです。1 つの ポート上で検出された CISCO PHONE イベントは、スイッチに

CISCO_PHONE_AUTO_SMARTPORT でコマンドを適用させます。言語自動化および変数置換のための BASH と同様の言語構文である、Cisco IOS シェルのスクリプト機能を使用してユーザ定義のマクロを作成することもできます。

Auto SmartPort マクロはスタティック SmartPort マクロとは異なります。スタティック SmartPort マク ロでは、ポートに接続されているデバイスに基づいて手動で適用するポート設定が提供されます。スタ ティック SmartPort マクロを適用すると、マクロ内の CLI コマンドが既存のポート設定に追加されま す。ポートにリンクダウン イベントがあると、スイッチはスタティック マクロ設定を削除しません。

Auto SmartPort はイベントを使用して、イベントのマクロを送信元ポートにマッピングします。接続 されたデバイスから受信した Cisco Discovery Protocol (CDP) メッセージに基づくイベント トリガー が最も一般的です。デバイスが検出されると、CDP イベント トリガーが呼び出されます。これは、 Cisco IP Phone、Autonomous アクセス ポイントや Lightweight アクセス ポイントを含む Cisco 無線ア クセス ポイント、Cisco スイッチ、または Cisco ルータ、および Cisco IP Video Surveillance Camera に該当します。

シスコおよびサードパーティのデバイスの追加イベント トリガーは、ユーザ定義の MAC アドレス グ ループ、MAC Authentication Bypass (MAB; MAC 認証バイパス) メッセージ、802.1x 認証メッセー ジ、および Link Layer Discovery Protocol (LLDP) メッセージです。

LLDP は一連のアトリビュートをサポートし、これらを使用して隣接するデバイスを検出します。アト リビュートには Type、Length、および Value があり、これらを TLV と呼びます。LLDP をサポートす るデバイスは、TLV を使用して情報を送受信します。このプロトコルは、設定情報、デバイス機能、 およびデバイス ID のような詳細情報をアドバタイズします。Auto SmartPort は、LLDP システム機能 TLV をイベント トリガーとして使用します。Auto SmartPort の LLDP システム機能 TLV アトリ ビュート設定の詳細については、第 26章「LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定」を参照してください。

ネットワーク プリンタ、LLDP、レガシー Cisco Digital Media Player のような、CDP、MAB、または 802.1x 認証をサポートしないデバイスの場合は、MAC Operationally Unique Identifier (OUI) に基づ くトリガーで MAC アドレス グループを設定できます。MAC アドレスを、組み込みマクロ、または対 象となる設定を含むユーザ定義のマクロにマッピングします。

ユーザ定義マクロ ファイルのリモート サーバ ロケーションを指定できます。その後、複数のスイッチ がネットワーク全体で使用するために 1 組の Auto SmartPort マクロ ファイルの更新とメンテナンスを おこなえます。

Auto SmartPort マクロの持続性機能を使用すると、リンクダウン イベント検出の有無に関係なく、マ クロ設定をスイッチ ポートに適用し続けられます。この機能を使用して、スイッチ上で Auto SmartPort マクロ設定をスタティックに設定できます。これにより、スイッチがリンクアップ イベント およびリンクダウン イベントを持つとき、または EnergyWise を設定されたネットワーク内の参加エン ティティであるときに複数のシステム ログおよび設定変更通知イベントを除去できます。

Auto SmartPort および Cisco Medianet

Cisco Medianet を使用すると、各種のビデオ アプリケーションのためのネットワーク インフラストラ クチャでのインテリジェントなサービスが可能になります。Medianet のサービスの1 つとして、Auto SmartPort での Cisco Digital Media Player および Cisco IP Video Surveillance Camera の自動プロビ ジョニングがあります。スイッチは、CDP、802.1x、MAB、LLDP、および MAC アドレスを使用す ることによって、シスコおよびサードパーティのビデオ デバイスを識別します (図 12-1)。スイッチ は、適用可能な Auto SmartPort マクロを使用して、デバイスに適切な VLAN および QoS の設定をイ ネーブルにします。スイッチは、組み込み型の MAC アドレス グループを使用して、4400 または 23ac00 の OUI に基づいてレガシー Cisco DMP を検出することもします。任意のビデオ デバイスのカ スタム ユーザ定義マクロも作成できます。





Auto SmartPort の設定

- 「Auto SmartPort のデフォルト設定」(P.12-4)
- 「Auto SmartPort 設定時の注意事項」(P.12-5)
- 「Auto SmartPort のイネーブル化」(P.12-6)
- 「Auto SmartPort のデフォルト パラメータ値の設定」(P.12-6)
- 「Auto SmartPort の MAC アドレス グループの設定」(P.12-8)
- 「Auto SmartPort マクロの永続性の設定」(P.12-9)
- 「Auto SmartPort 組み込みマクロ オプションの設定」(P.12-10)
- 「ユーザ定義のイベントトリガーの作成」(P.12-13)
- 「Auto SmartPort ユーザ定義マクロの設定」(P.12-16)

Auto SmartPort のデフォルト設定

- Auto SmartPort はグローバルにディセーブルにされ、インターフェイス単位でイネーブルにされます。
- CDP fallback はグローバルにディセーブルにされ、インターフェイス単位でイネーブルにされます。
- Cisco IOS シェルはイネーブルにされます。
- Auto SmartPort マクロはデフォルトで、表 12-1 に示されるデバイスに対して ASP がイネーブルに されているときに使用されます。

表 12-1 Auto SmartPort 組み込みマクロ

マクロ名	説明
CISCO_PHONE_AUTO_ SMARTPORT	このマクロは、Cisco IP 電話の IP 電話マクロに適用されます。QoS、ポート セキュリティ、 ストーム制御、DHCP スヌーピング、およびスパニング ツリー保護をイネーブルにします。 また、インターフェイスへのアクセスおよび音声 VLAN の設定もします。
CISCO_SWITCH_AUTO_ SMARTPORT	このマクロは、シスコ スイッチのスイッチ マクロに適用されます。QoS および 802.1Q カプ セル化とのトラッキングをイネーブルにします。また、インターフェイス上のネイティブ VLAN も設定します。
CISCO_ROUTER_AUTO_ SMARTPORT	このマクロは、シスコ ルータのルータ マクロに適用されます。QoS、802.1Q カプセル化と のトラッキング、およびスパニング ツリー BPDU 保護をイネーブルにします。
CISCO_AP_AUTO_ SMARTPORT	このマクロは、Cisco AP のワイヤレス アクセス ポイントに適用されます。QoS および 802.1Q カプセル化とのトラッキングをイネーブルにします。また、インターフェイス上のネ イティブ VLAN も設定します。
CISCO_LWAP_AUTO_ SMARTPORT	このマクロは、Cisco 軽量ワイヤレス アクセス ポイントの軽量ワイヤレス アクセス ポイント マクロに適用されます。QoS、ポート セキュリティ、ストーム制御、DHCP スヌーピング、 およびスパニング ツリー保護をイネーブルにします。インターフェイスの VLAN へのアクセ スを設定し、不明のユニキャスト パケットからのネットワーク保護を提供します。
CISCO_IPVSC_AUTO_ SMARTPORT	このマクロは、Cisco IP Video Surveillance Camera の IP カメラ マクロに適用されます。QoS trust、ポート セキュリティ、およびスパニング ツリー保護をイネーブルにします。インター フェイスの VLAN へのアクセスを設定し、不明のユニキャスト パケットからのネットワーク 保護を提供します。
CISCO_DMP_AUTO_ SMARTPORT	このマクロは、Cisco Digital Media Player の digital media player マクロに適用されます。 QoS trust、ポート セキュリティ、およびスパニング ツリー保護をイネーブルにします。イン ターフェイスの VLAN へのアクセスを設定し、不明のユニキャスト パケットからのネット ワーク保護を提供します。

Auto SmartPort 設定時の注意事項

- 組み込みマクロは、削除することも変更することもできません。ただし、ユーザ定義のマクロを同じ名前で作成すると、組み込みマクロを無効にすることができます。元の組み込みマクロを復元するには、ユーザ定義のマクロを削除します。
- macro auto device および macro auto execute の両方のグローバル コンフィギュレーション コマンドをイネーブルにすると、最後に実行されたコマンドで指定されたパラメータがスイッチに適用されます。スイッチでアクティブになるコマンドは、1 つだけです。
- Auto SmartPort マクロの適用時にシステムで衝突が発生しないようにするには、802.1x 認証を除くすべてのポート設定を削除します。
- スイッチで Auto SmartPort をイネーブルする場合は、ポート セキュリティを設定しないでください。
- マクロが元のコンフィギュレーションと競合する場合は、マクロは元のコンフィギュレーション コマンドの一部に適用されないか、またはアンチマクロはそれらを削除しません (アンチマクロ は、マクロをリンクダウン イベントで削除するマクロに適用される部分です)。

たとえば、802.1x 認証がイネーブルになっている場合は、switchport-mode access 設定を削除できません。この場合は、switchport-mode 設定を削除する前に 802.1x 認証を削除する必要があります。

- Auto SmartPort マクロを適用するときには、ポートを EtherChannel のメンバーにできません。
 EtherChannels を使用する場合は、no macro auto processing インターフェイス コンフィギュレー ション コマンドを使用して、EtherChannels のメンバーであるインターフェイス上の Auto SmartPort をディセーブルにします。
- 組み込みマクロのデフォルトのデータ VLAN は VLAN 1 です。組み込みマクロのデフォルトの データ VLAN は VLAN 2 です。(VLAN 1 は、すべてのマクロのデフォルト データ VLAN です。 VLAN 2 は、すべてのマクロのデフォルト音声データ VLAN です。)スイッチが、異なるアクセ ス、ネイティブ、または音声 VLAN を使用する場合は、macro auto device または macro auto execute グローバル コンフィギュレーション コマンドを使用して、目的の非デフォルト値を設定 します。
- デフォルトマクロのデフォルトパラメータ値、現在値、および各マクロに設定可能なパラメータ リストを表示するには、show macro auto device 特権 EXEC コマンドを使用します。また、show shell functions 特権 EXEC コマンドを使用すると、組み込みマクロのデフォルト値を表示できます
- 802.1x 認証または MAB の場合は、他社製のデバイスを検出するための Cisco Attribute-Value (AV; 属性と値)のペア auto-smart-port=event trigger をサポートするように RADIUS サーバを 設定します。
- ネットワークプリンタのような、CDP、MAB、または 802.1x 認証をサポートしない固定型のデバイスの場合は、MAC OUI に基づくトリガーで MAC アドレス グループを設定し、そのグループを、目的の設定を含むユーザ定義マクロにマッピングします。
- スイッチが Auto SmartPort をサポートするのは、直接接続されたデバイス上だけです。ハブのような複数のデバイスの接続はサポートされません。複数のデバイスを接続すると、適用されているマクロは最初に検出されたデバイスに関連付けられたものになります。
- ポート上で認証がイネーブルになっている場合は、認証に失敗するとスイッチは MAC アドレスを 無視します。
- マクロ内と対応するアンチマクロ内では、CLI コマンドの順序が異なる場合があります。
- Auto SmartPort はどのグローバル コンフィギュレーションも実行しません。インターフェイス レベルで Auto SmartPort マクロが何らかのグローバル コンフィギュレーションを必要とする場合は、 手動でグローバル コンフィギュレーションを追加する必要があります。

Auto SmartPort のイネーブル化

スイッチ上で Auto SmartPort マクロをグローバルにイネーブルにするには、次の手順に従います。この手順は必須です。特定のポートで Auto SmartPort マクロをディセーブルにするには、**no auto global** processing インターフェイス コンフィギュレーション コマンドを使用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto global processing	スイッチで Auto SmartPort をグローバルにイネーブルにしま
		す。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	Auto SmartPort がイネーブルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

イベント トリガー、組み込みマクロ、および組み込みマクロのデフォルト値を表示するには、show macro auto device、show shell *functions*、および show shell *triggers* 特権 EXEC コマンドを使用しま す。

次の例では、Auto SmartPort をスイッチではイネーブルにし、特定のインターフェイスではディセーブルにする方法を示します。

Switch(config) # macro auto global processing Switch(config) # interface interface_id Switch(config-if) # no macro auto processing

Auto SmartPort のデフォルト パラメータ値の設定

イベント トリガーから組み込みマクロへのマッピングは、スイッチで自動的に実行されます。次の手順に従うと、Auto SmartPort マクロのデフォルト パラメータ値をスイッチ固有の値に置換できます。 この手順は任意です。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show macro auto device	マクロのデフォルト パラメータ値を表示します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	macro auto device {access-point ip-camera lightweight-ap media-player phone router switch} [parameter=value]	指定したマクロのデフォルトパラメータ値を置き換えます。それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します(例:[<name1>=<value1> <name2>=<value2>])。各デフォルトパラメータ値のデフォルト値が表示されます。</value2></name2></value1></name1>
		• access-point NATIVE_VLAN=1
		• ip-camera ACCESS_VLAN=1
		 lightweight-ap ACCESS_VLAN=1
		• media-player ACCESS_VLAN=1
		 phone ACCESS_VLAN=1 VOICE_VLAN=2
		• router NATIVE_VLAN=1
		• switch NATIVE_VLAN=1
		(注) このテキストストリングが組み込みマクロ定義のテキスト ストリングと一致する必要があるため、正しいパラメータ名 (たとえば、VOICE_VLAN)を入力しなければなりません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show macro auto device	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no macro auto device {macro name} parameter=value グローバル コン フィギュレーション コマンドを使用します。

次に、IP 電話マクロのパラメータ値を表示する例、およびデフォルト音声 VLAN を 20 に変更する例 を示します。デフォルト値を変更する場合は、その値は、マクロがすでに適用されているインターフェ イスには適用されません。設定された値は、次のリンクアップイベントで適用されます。正確なテキ ストストリングが VOICE_VLAN に使用されたことに注意してください。エントリでは大文字と小文 字が区別されます。

```
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
```

```
Switch# configure terminal
Switch(config)# macro auto device phone VOICE_VLAN=20
Switch(config)# end
Switch# show macro auto device phone
Device:phone
Default Macro:CISCO_PHONE_AUTO_SMARTPORT
Current Macro:CISCO_PHONE_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN VOICE_VLAN
Defaults Parameters:ACCESS_VLAN=1 VOICE_VLAN=2
Current Parameters:voice_vlan=20
```

Auto SmartPort の MAC アドレス グループの設定

CDP または LLDP のような近接ディスカバリ プロトコルをサポートしないプリンタなどのデバイスの 場合は、Auto SmartPort に MAC アドレスに基づくトリガー コンフィギュレーションを使用します。 この手順は任意であり、次の手順に従う必要があります。

- macro auto mac-address グローバル コンフィギュレーション コマンドを使用して、MAC アドレ スに基づくトリガーを設定します。
- macro auto execute グローバル コンフィギュレーション コマンドを使用して、MAC アドレスト リガーを、組み込みマクロまたはユーザ定義マクロに関連付けます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto mac-address-group name	グループ名を指定し、MAC アドレス コンフィギュレーションモー ドを開始します。
ステップ 3	[mac-address list list] [oui [list list range word size number]]	スペースで区切られた MAC アドレスのリストを設定します。 Operationally Unique Identifier (OUI) list または range を指定し ます。OUI は MAC アドレスの最初の 3 バイトで示され、これによ り製品のメーカー名が識別されます。OUI を指定すると、近接ディ スカバリ プロトコルをサポートしないデバイスを認識できます。
		 list: OUI リストを、スペースで区切られた 16 進数で入力します。 range: OUI 開始範囲を 16 進数で入力します。サイズ (1-5) を入力して連続したアドレスを作成します。
ステップ 4	macro auto execute <i>address_trigger</i> built-in <i>macro name</i>	MAC アドレスのグループを、組み込みマクロまたはユーザ定義マ クロにマッピングします。
		MAC アドレスのトリガーが、65 秒のホールド タイムの後にイン ターフェイスに適用されます。このホールド タイムによって、CDP または LLDP のような近接ディスカバリ プロトコルを MAC アドレ スの代わりに使用できます。
ステップ 5	exit	コンフィギュレーション モードに戻ります。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show macro auto address-group	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アドレス グループを削除するには、no macro auto mac-address-group *name* グローバル コンフィ ギュレーション コマンドを使用します。マクロ トリガー、および macro auto execute グローバル コ ンフィギュレーション コマンドを使用して定義されたマクロにマッピングされている任意の関連付け られたトリガーを削除するには、no macro auto mac-address-group *name* と入力します。no macro auto execute mac-address-group を入力すると、トリガーからマクロへのマッピングだけが削除され ます。

次に、*address_trigger* と呼ばれる MAC アドレス グループのイベント トリガーを作成する例、および エントリを確認する例を示します。

Switch# configure terminal Switch(config)# macro auto address-group mac address_trigger Switch(config-addr-grp-mac)# mac-address list 2222.3333.3334 22.33.44 a.b.c

```
Switch(config-addr-grp-mac)# oui list 455555 233244
Switch(config-addr-grp-mac)# oui range 333333 size 2
Switch(config-addr-grp-mac)# exit
Switch(config) # mac auto execute address-trigger builtin macro
Switch(config)# exit
Switch(config)# end
Switch(config) # macro auto execute mac-address-trigger builtin CISCO_PHONE_ATUO_SMARTPORT
Switch(config) # end
Switch# show running configuration | include macro
macro auto mac-address-group address trigger
mac auto mad-address-group hel
mac auto execute mad-address-trigger builtin CISCO PHONE AUTO SMARTPORT
macro description CISCO_DMP EVENT
mac description CISCO SWITCH EVENT
1
<output truncated>
```

Auto SmartPort マクロの永続性の設定

スイッチで Auto SmartPort をイネーブルにする場合は、デフォルトで、マクロ コンフィギュレーショ ンがリンクアップ イベントで適用され、リンクダウン イベントで削除されるようになっています。マ クロの永続性機能をイネーブルにすると、コンフィギュレーションは、リンクアップで適用され、リン クダウンで削除されます。適用されたコンフィギュレーションは、スイッチ上のリンクアップ イベン トまたはリンクダウン イベントに関係なく、そのままになります。マクロの永続性機能は、実行中の コンフィギュレーション ファイルを保存すると再起動後も設定されたままになります。

Auto SmartPort マクロをリンクダウン イベント後もスイッチでアクティブのままにするには、次の手順に従います。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto sticky	Auto SmartPort マクロ コンフィギュレーションがリンクダウン イ ベントでインターフェイスにそのまま適用されるようにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show macro auto	設定を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

特権 EXEC モードで次の手順を実行します。

Auto SmartPort マクロの永続性機能をディセーブルにするには、no macro auto sticky グローバル コンフィギュレーション コマンドを使用します。

次に、Auto SmartPort の auto-sticky 機能をイネーブルにする例を示します。

Switch(config) # macro auto sticky

Auto SmartPort 組み込みマクロ オプションの設定

この手順を使用すると、イベント トリガーを組み込みマクロにマッピングし、組み込みマクロ デフォ ルト パラメータ値を、スイッチに固有の値に置換できます。マクロのデフォルト パラメータ値を*置き 換える*必要がある場合は、**macro auto device** グローバル コンフィギュレーション コマンドを使用し ます。次の手順のコマンドは、すべて任意です。

特権 EXEC モード

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto execute event trigger builtin built-in macro name [parameter=value] [parameter=value]	イベント トリガーから組み込みマクロへのマッピングを定義します。
		イベントトリガーを指定します。
		CISCO_DMP_EVENT
		CISCO_IPVSC_EVENT
		CISCO_PHONE_EVENT
		CISCO_SWITCH_EVENT
		CISCO_ROUTER_EVENT
		CISCO_WIRELESS_AP_EVENT
		CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
		• WORD: ユーザ定義のイベント トリガーを適用します。
		builtin <i>組み込みマクロ名</i> を指定します。
		それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力 します(例:[<name1>=<value1> <name2>=<value2>])。デフォル ト値は、入力すべきとおりに正確に表示されます。</value2></name2></value1></name1>
		 CISCO_DMP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。
		 CISCO_IPVSC_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。
		 CISCO_PHONE_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 および VOICE_VLAN=2 を指 定します。
		 CISCO_SWITCH_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。
		 CISCO_ROUTER_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。
		 CISCO_AP_AUTO_SMARTPORT パラメータ値 NATIVE_VLAN=1 を指定します。
		 CISCO_LWAP_AUTO_SMARTPORT パラメータ値 ACCESS_VLAN=1 を指定します。

	コマンド	目的
ステップ 3	remote <i>url</i>	リモート マクロ ファイルのリモート サーバ ロケーションを指定しま す。
		 スタンドアロン スイッチまたはスタック マスターのローカル フ ラッシュ ファイル システムの構文: flash:
		 スタック メンバーのローカル フラッシュ ファイル システムの構 文: flash member number:
		 FTPの構文: ftp:[[//username[:password]@location]/directory]/filename
		• HTTP サーバの構文: http://[[username:password]@]{hostname host-ip}[/directory]/filename
		 セキュア HTTP サーバの構文: https://[[username:password]@]{hostname host-ip}[/directory]/filename
		 NVRAM の構文: nvram://[[username:password]@][/directory]/filename
		 Remote Copy Protocol (RCP; リモート コピー プロトコル)の構 文:rcp:[[//username@location]/directory]/filename
		 Secure Copy Protocol (SCP) の構文: scp:[[//username@location]/directory]/filename
		 TFTP の構文: tftp: [[//location]/directory]/filename
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。

次の例では、該当するスイッチに Cisco スイッチと Cisco IP Phone を接続するための 2 つの組み込み Auto SmartPort マクロを使用する方法を示します。次の例では、トランク インターフェイスのデフォ ルトの音声 VLAN、アクセス VLAN、およびネイティブ VLAN を変更します。

```
Switch# configure terminal
\texttt{Switch}\,(\texttt{config})\,\#!\,!!\,\texttt{the next command modifies the access and voice vlans}
Switch(config)#!!!for the built in Cisco IP phone auto smartport macro
Switch (config) # macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!!the next command modifies the Native vlan used for inter switch trunks
Switch (config) # macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE VLAN=10
Switch(config)#
Switch (config) #!!!the next command enables auto smart ports globally
Switch(config)# macro auto global processing cdp-fallback
Switch(config)#
Switch(config) # exit
{\tt Switch}\# {\tt !!!here's} the running configuration of the interface connected
Switch# !!!to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface gigabitethernet0/1
```

```
Building configuration...

Current configuration : 284 bytes

!

interface GigabitEthernet0/1

switchport trunk encapsulation dot1q

switchport trunk native vlan 10

switchport mode trunk

srr-queue bandwidth share 10 10 60 20

queue-set 2

priority-queue out

mls qos trust cos

auto qos voip trust

macro description CISCO_SWITCH_EVENT

end
```

次に、ネイティブ VLAN 5 の設定のリモート マクロを設定する例を示します。

- a. macro.txt ファイル内のリモート マクロを設定します。
- **b.** マクロ ファイルのリモート ロケーションを指定するには、macro auto execute コンフィギュレー ション コマンドを使用します。

```
if [[ $LINKUP -eq YES ]]; then
    conf t
           interface $INTERFACE
                 macro description $TRIGGER
                 auto qos voip trust
                  switchport trunk encapsulation dotlq
                  switchport trunk native vlan $NATIVE VLAN
                 switchport trunk allowed vlan ALL
                  switchport mode trunk
            exit
   end
else
   conf t
           interface $INTERFACE
                no macro description
                 no auto qos voip trust
                no switchport mode trunk
                no switchport trunk encapsulation dot1q
                no switchport trunk native vlan $NATIVE_VLAN
                 no switchport trunk allowed vlan ALL
          exit
   end
```

Switch(config)# macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt NATIVE_VLAN=5

```
Switch# show running configuration | include macro
macro auto execute CISCO_SWITCH_EVENT remote tftp://<ip_address>/macro.txt
NATIVE_VLAN=5
Switch#
```

ユーザ定義のイベント トリガーの作成

MAB または 802.1x 認証を使用して Auto SmartPort マクロを実行させる場合、RADIUS サーバによっ て送信される Cisco アトリビュート値ペア (auto-smart-port=event trigger) に対応するイベント トリ ガーを作成する必要があります。この手順は任意です。

特権 EXEC モード

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	shell trigger identifier description	イベント トリガー。の ID および説明を指定します。この ID を指定 する場合は、文字間にスペースやハイフンを入れないでください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show shell triggers	スイッチのイベント トリガーを表示します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

イベント トリガーを削除するには、no shell trigger *identifier* グローバル コンフィギュレーション コ マンドを使用します。

次に、RADIUS_MAB_EVENT と呼ばれるユーザ定義のイベント トリガーを組み込みマクロ CISCO_AP AUTO_SMARTPORT にマッピングしてデフォルト VLAN を VLAN 10 に置き換える例、 およびエントリを確認する例を示します。

- a. デバイスを MAB 対応のスイッチ ポートに接続します。
- **b.** RADIUS サーバで、アトリビュート値ペアを auto-smart-port=RADIUS_MAB_EVENT に設定 します。
- **c.** スイッチ上で、イベントトリガー RADIUS MAB EVENT を作成します。
- **d.** スイッチは、アトリビュート値ペアが RADIUS_MAB_EVENT であるとの RADIUS サーバから の応答を認識し、マクロ CISCO AP AUTO SMARTPORT を適用します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config) # !!!create a user defined trigger and map
Switch(config)# !!!a system defined macro to it
Switch(config)# !!!first create the trigger event
Switch(config) # shell trigger RADIUS MAB EVENT MAC AuthBypass Event
Switch(config)#
Switch(config) #!!!map a system defined macro to the trigger event
Switch(config) # macro auto execute RADIUS_MAB_EVENT builtin ?
_ CISCO_DMP_AUTO_SMARTPORT
_ CISCO_IPVSC_AUTO_SMARTPORT
 CISCO_AP_AUTO_SMARTPORT
 CISCO LWAP AUTO SMARTPORT
 CISCO PHONE AUTO SMARTPORT
 CISCO ROUTER AUTO SMARTPORT
 CISCO SWITCH AUTO SMARTPORT
LINE
       <cr>
Switch(config) # macro auto execute RADIUS_MAB_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=10
Switch(config) # exit
Switch# show shell triggers
User defined triggers
_____
Trigger Id: RADIUS MAB EVENT
Trigger description: MAC AuthBypass Event
```

```
Trigger environment:
Trigger mapping function: CISCO_AP_SMARTPORT
<output truncated>
```

次の例では、**show shell** *triggers* 特権 EXEC コマンドを使用して、スイッチ ソフトウェアにイベント トリガーを表示する方法を示します。

Switch# show shell triggers

User defined triggers

Built-in triggers ------Trigger Id: CISCO_DMP_EVENT Trigger description: Digital media-player device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$ACCESS_VLAN=(1), The value in the parenthesis is a default value Trigger mapping function: CISCO_DMP_AUTO_SMARTPORT

Trigger Id: CISCO_IPVSC_EVENT Trigger description: IP-camera device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$ACCESS_VLAN=(1), The value in parenthesis is a default value Trigger mapping function: CISCO_IP_CAMERA_AUTO_SMARTPORT

Trigger Id: CISCO_PHONE_EVENT Trigger description: IP-phone device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$ACCESS_VLAN=(1) and \$VOICE_VLAN=(2), The value in the parenthesis is a default value Trigger mapping function: CISCO PHONE AUTO SMARTPORT

Trigger Id: CISCO_ROUTER_EVENT Trigger description: Router device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$NATIVE_VLAN=(1), The value in the parenthesis is a default value Trigger mapping function: CISCO_ROUTER_AUTO_SMARTPORT

Trigger Id: CISCO_SWITCH_EVENT Trigger description: Switch device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$NATIVE_VLAN=(1), The value in the parenthesis is a default value Trigger mapping function: CISCO_SWITCH_AUTO_SMARTPORT

Trigger Id: CISCO_WIRELESS_AP_EVENT Trigger description: Autonomous ap device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$NATIVE_VLAN=(1), The value in the parenthesis is a default value Trigger mapping function: CISCO AP AUTO SMARTPORT

Trigger Id: CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT Trigger description: Lightweight-ap device event to apply port configuration Trigger environment: Parameters that can be set in the shell - \$NATIVE_VLAN=(1), The value in the parenthesis is a default value Trigger mapping function: CISCO_LWAP_AUTO_SMARTPORT

次の例では、show shell functions 特権 EXEC コマンドを使用して、スイッチ ソフトウェアに組み込み マクロを表示する方法を示します。

Switch# **show shell functions** #User defined functions:

#Built-in functions: function CISCO_AP_AUTO_SMARTPORT () { if [[\$LINKUP -eq YES]]; then

```
conf t
           interface $INTERFACE
               macro description $TRIGGER
               switchport trunk encapsulation dotlq
               switchport trunk native vlan $NATIVE VLAN
               switchport trunk allowed vlan ALL
               switchport mode trunk
                switchport nonegotiate
               auto qos voip trust
               mls qos trust cos
            exit
       end
    fi
   if [[ $LINKUP -eq NO ]]; then
        conf t
           interface $INTERFACE
               no macro description
               no switchport nonegotiate
               no switchport trunk native vlan $NATIVE VLAN
               no switchport trunk allowed vlan ALL
               no auto qos voip trust
               no mls qos trust cos
               if [[ $AUTH ENABLED -eq NO ]]; then
                   no switchport mode
                    no switchport trunk encapsulation
                fi
            exit
       end
   fi
}
function CISCO SWITCH AUTO SMARTPORT () {
   if [[ $LINKUP -eq YES ]]; then
       conf t
            interface $INTERFACE
               macro description $TRIGGER
               auto qos voip trust
               switchport trunk encapsulation dotlq
               switchport trunk native vlan $NATIVE VLAN
                switchport trunk allowed vlan ALL
               switchport mode trunk
            exit
       end
   else
         conf t
             interface $INTERFACE
                no macro description
                no auto qos voip trust
                 no switchport mode trunk
                no switchport trunk encapsulation dotlq
                 no switchport trunk native vlan $NATIVE VLAN
                 no switchport trunk allowed vlan ALL
             exit
         end
   fi
}
<output truncated>
```

Auto SmartPort ユーザ定義マクロの設定

Cisco IOS シェルは、ユーザ定義の Auto SmartPort マクロを設定する基本スクリプト機能を提供しま す。これらのマクロは複数行を含むことができ、任意の CLI コマンドを含むことができます。変数の 置換、条件、機能、およびマクロ内のトリガーも定義できます。この手順は任意です。

ユーザ定義イベント トリガーをユーザ定義マクロにマッピングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	macro auto execute event trigger [parameter=value] {function contents}	イベント トリガーにマッピングするユーザ定義のマクロを指定します。 { <i>function contents</i> }:トリガーに関連付けるユーザ定義のマクロを指定 します。マクロの内容は、波カッコで囲んで入力します。左波カッコで Cisco IOS シェル コマンドを開始し、右波カッコでコマンドのグループ 化を終了します。
		 (任意) parameter=value: \$ で始まるデフォルト値を置き換えて、それ ぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します (例: [<name1>=<value1> <name2>=<value2>])。</value2></name2></value1></name1>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、Media Player と呼ばれるユーザ定義のイベント トリガーをユーザ定義のマクロにマッピ ングする方法を示します。

- a. Media Player を 802.1x または MAB 対応のスイッチ ポートに接続します。
- **b.** RADIUS サーバで、アトリビュート値ペアを auto-smart-port=MP_EVENT に設定します。
- **C.** スイッチで、イベント トリガー MP_EVENT を作成し、次のようにユーザ定義マクロ コマンドを 入力します。
- **d.** スイッチは、アトリビュート値ペアが MP_EVENT であるとの RADIUS サーバからの応答を認識 し、このイベント トリガーに関連付けられているマクロを適用します。

```
Switch(config) # shell trigger MP EVENT mediaplayer
Switch(config) # macro auto execute MP EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
 interface $INTERFACE
  macro description $TRIGGER
   switchport access vlan 1
   switchport mode access
  switchport port-security
   switchport port-security maximum 1
   switchport port-security violation restrict
   switchport port-security aging time 2
   switchport port-security aging type inactivity
   spanning-tree portfast
   spanning-tree bpduguard enable
   exit
fi
if [[ $LINKUP -eq NO ]]; then
conf t
```

```
interface $INTERFACE
    no macro description $TRIGGER
     no switchport access vlan 1
    if [[ $AUTH_ENABLED -eq NO ]]; then
      no switchport mode access
    fi
    no switchport port-security
     no switchport port-security maximum 1
    no switchport port-security violation restrict
    no switchport port-security aging time 2
    no switchport port-security aging type inactivity
     no spanning-tree portfast
    no spanning-tree bpduguard enable
     exit
fi
```

```
Switch(config)# end
```

}

コマンド	説明
{	コマンドのグループ化を開始します。
}	コマンドのグループ化を終了します。
[[条件構成体として使用します。
]]	条件構成体として使用します。
else	条件構成体として使用します。
-eq	条件構成体として使用します。
fi	条件構成体として使用します。
if	条件構成体として使用します。
then	条件構成体として使用します。
-Z	条件構成体として使用します。
\$	\$ 文字で始まる変数が、パラメータ値に置き換えられます。
#	コメント テキストを入力するには、#文字を使用します。

表 12-2 サポートされている Cisco IOS シェルのキーワ	ノード
------------------------------------	-----

表 12-3 サポートされていない Cisco IOS シェルの予約済キーワード

コマンド	説明
	パイプライン
case	条件構成体
esac	条件構成体
for	ループ構成体
function	シェル関数
in	条件構成体
select	条件構成体
time	パイプライン
until	ループ構成体
while	ループ構成体

スタティック SmartPort マクロの設定

- 「スタティック SmartPort のデフォルト設定」(P.12-18)
- 「スタティック SmartPort 設定時の注意事項」(P.12-18)
- 「スタティック SmartPort マクロの適用」(P.12-19)

スタティック SmartPort のデフォルト設定

スイッチに、イネーブルにされているスタティック SmartPort マクロはありません。

表 12-4 デフォルト スタティック SmartPort マクロ

	=× an
マクロ名	at 43
cisco-global	Rapid PVST+、ループガード、リンク ステート障害用のダイナミック ポート エラー回復をイネーブル
	にするには、このグローバル コンフィギュレーション マクロを使用します。
cisco-desktop	PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、ネットワーク セキュリティと信頼
	性を高めるために、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-phone	Cisco IP Phone を装備した PC などのデスクトップ デバイスをスイッチ ポートに接続する場合、このイ
	ンターフェイス コンフィギュレーション マクロを使用します。このマクロは、cisco-desktop マクロの
	拡張機能で、同じセキュリティ機能と復元力機能を提供します。ただし、遅延に影響されやすい音声ト
	ラフィックを適切に処理するために、専用音声 VLAN が追加されています。
cisco-switch	ー アクセス スイッチとディストリビューション スイッチを接続する場合。または Small Form-factor
	Pluggable (SFP) を使用して接続したアクセス スイッチの間で このインターフェイス コンフィギュ
	レーション マクロを使用します。
cisco-router	
	します.
cisco-wireless	スイッチとリイヤレス アクセス ホイントを接続する場合、このインターフェイス コンフィギュレー
	ション マクロを使用します。

1. シスコのデフォルト SmartPort マクロは、スイッチで稼動するソフトウェアのバージョンによって異なります。

スタティック SmartPort 設定時の注意事項

- スイッチまたはスイッチインターフェイスにマクロをグローバルに適用しても、インターフェイスの既存の設定はすべて維持されます。これは、差分設定に適用する場合に役立ちます。
- 構文エラーまたは設定エラーが原因でコマンドが失敗した場合でも、マクロは引き続き残りのコマンドを適用します。マクロを適用およびデバッグして、構文エラーまたは設定エラーを検出するには、macro global trace macro-name グローバル コンフィギュレーション コマンド、またはmacro trace macro-name インターフェイス コンフィギュレーション コマンドを使用できます。
- 特定のインターフェイスタイプ固有の CLI コマンドもあります。設定を受け入れないインター フェイスにマクロを適用すると、マクロは構文チェックまたは設定チェックに失敗し、スイッチは エラーメッセージを返します。
- インターフェイス範囲へのマクロの適用は、単一インターフェイスへのマクロの適用と同じです。 インターフェイス範囲を使用すると、インターフェイス範囲内の各インターフェイスへマクロが順 番に適用されます。1つのインターフェイスでマクロコマンドの実行に失敗しても、マクロは残り のインターフェイス上に適用されます。
スイッチまたはスイッチ インターフェイスにマクロを適用すると、マクロ名が自動的にスイッチ またはインターフェイスに追加されます。show running-config ユーザ EXEC コマンドを使用し て、適用されたコマンドおよびマクロ名を表示できます。

スタティック SmartPort マクロの適用

スタティック SmartPort を適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show parser macro	スイッチ ソフトウェアに組み込まれたシスコのデフォルト スタティッ ク SmartPort マクロを表示します。
ステップ 2	show parser macro name macro-name	適用する特定のマクロを表示します。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	<pre>macro global {apply trace} macro-name [parameter {value}] [parameter {value}] [parameter {value}]</pre>	マクロに定義されている個々のコマンドをスイッチに適用するには、 macro global apply <i>macro-name</i> を入力します。マクロを適用およびデ バッグして、構文エラーまたは設定エラーを検出するには、macro global trace <i>macro-name</i> を指定します。
		parameter value キーワードを使用して、マクロに必要な値を追加しま す。 \$ で始まるキーワードには、一意のパラメータ値が必要です。
		macro global apply macro-name? コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
		(任意)スイッチに固有の一意のパラメータ値を指定します。最高3つのキーワードと値の組み合わせを入力できます。パラメータキーワードの照合では、大文字と小文字が区別されます。キーワードがすべて照合できた場合、それに対応する値に置き換えられます。
ステップ 5	interface interface-id	(任意) インターフェイス コンフィギュレーション モードを開始し、マ クロを適用するインターフェイスを指定します。
ステップ 6	default interface interface-id	(任意)指定のインターフェイスからすべての設定情報を消去します。
ステップ 7	macro {apply trace} macro-name [parameter {value}] [parameter {value}] [parameter {value}]	マクロに定義されている個々のコマンドをポートに適用するには、 macro global apply <i>macro-name</i> を入力します。マクロを適用およびデ バッグして、構文エラーまたは設定エラーを検出するには、macro global trace <i>macro-name</i> を指定します。
		parameter <i>value</i> キーワードを使用して、マクロに必要な値を追加しま す。 \$ で始まるキーワードには、一意のパラメータ値が必要です。
		macro global apply macro-name?コマンドを使用すると、マクロで必要な値を一覧表示できます。キーワード値を入力せずにマクロを適用した場合、コマンドは無効となり、マクロは適用されません。
		(任意) スイッチに固有の一意のパラメータ値を指定します。最高3つのキーワードと値の組み合わせを入力できます。パラメータキーワードの照合では、大文字と小文字が区別されます。キーワードがすべて照合できた場合、それに対応する値に置き換えられます。
ステップ 8	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	show running-config interface <i>interface-id</i>	マクロがインターフェイスに適用されたことを確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マクロに含まれる各コマンドの no バージョンを入力したときにだけ、スイッチで適用されたグローバ ルマクロ設定を削除できます。default interface *interface-id* インターフェイス コンフィギュレーショ ン コマンドを入力すれば、ポート上のマクロが適用された設定を削除できます。

次に、cisco-desktop マクロを表示してそのマクロを適用し、インターフェイスのアクセス VLAN ID を 25 に設定する例を示します。

```
Switch# show parser macro cisco-desktop
```

```
Macro name : cisco-desktop
Macro type : default
```

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

```
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1
```

```
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Auto SmartPort マクロおよびスタティック SmartPort マ クロの表示

Auto SmartPort およびスタティック SmartPort のマクロを表示するには、表 12-5 の特権 EXEC コマン ドを 1 つ以上使用します。

コマンド	目的
show macro auto	Auto SmartPort マクロに関する情報を表示します。
show parser macro	すべてのスタティック SmartPort マクロを表示します。
show parser macro name macro-name	特定のスタティック SmartPort マクロを表示します。
show parser macro brief	スタティック SmartPort マクロ名を表示します。
show parser macro description [interface <i>interface-id</i>]	すべてのインターフェイスまたは指定されたインターフェイスのス タティック SmartPort マクロ説明を表示します。
show shell	Auto SmartPort のイベント トリガーおよびマクロに関する情報を表示します。

表 12-5 Auto SmartPort およびスタティック SmartPort マクロの表示コマンド



снарте 13

VLAN の設定

この章では、Catalyst 2960 スイッチでの標準範囲 VLAN (VLAN ID 1 ~ 1005) および拡張範囲 VLAN (VLAN ID 1006 ~ 4094) の設定手順について説明します。VLAN メンバシップ モード、 VLAN コンフィギュレーション モード、VLAN トランク、および VLAN Membership Policy Server (VMPS; VLAN メンバシップ ポリシー サーバ) からの動的 VLAN 割り当てについても説明します。



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

この章で説明する内容は、次のとおりです。

- 「VLAN の概要」(P.13-2)
- 「標準範囲 VLAN の設定」(P.13-5)
- 「拡張範囲 VLAN の設定」(P.13-11)
- 「VLAN の表示」(P.13-14)
- 「VLAN トランクの設定」(P.13-14)
- 「VMPS の設定」(P.13-24)

VLAN の概要

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーション などで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じアトリビュー トをすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンドステーションも グループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブ ロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンドステーションだけに転送およ びフラッディングが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に割り当て られていないステーション宛てのパケットは、ルータまたはフォールバック ブリッジングをサポート するスイッチを経由して転送しなければなりません(図 13-1を参照)。VLAN はそれぞれが独立した 論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ MIB(管理情報ベース)情報があ り、スパニング ツリーの独自の実装をサポートできます。第16章「STP の設定」を参照してくださ い。

<u>《</u> (注)

VLAN を作成する前に、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル)を使用し てネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。VTP の詳 細については、第 14 章「VTP の設定」を参照してください。

図 13-1 に、論理的に定義されたネットワークにセグメント化された VLAN の例を示します。



図 13-1 論理的に定義されたネットワークとしての VLAN

VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれる すべてのエンド ステーションは同一の VLAN に所属させます。スイッチ上のインターフェイスの VLAN メンバシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチ インター フェイスを VLAN に割り当てた場合、これをインターフェイス ベース(またはスタティック) VLAN メンバシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバック ブリッジングする必要があります。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレント モードで VLAN をサポートしま す。VLAN は、1 ~ 4094 の番号で識別します。VLAN ID 1002 ~ 1005 は、トークンリングおよび Fiber Distributed Data Interface (FDDI) VLAN 専用です。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN (VLAN ID 1 ~ 1005) だけをサポート します。これらのバージョンでは、1006 ~ 4094 の VLAN ID を作成する場合は、スイッチを VTP ト ランスペアレント モードにする必要があります。Cisco IOS Release 12.2(52)SE 以降では VTP バー ジョン 3 をサポートします。VTP バージョン 3 は、VLAN 範囲全体 (VLAN 1 ~ 4094) をサポート します。拡張範囲 VLAN (VLAN 1006 ~ 4094) は、VTP バージョン 3 でだけサポートされます。拡 張 VLAN がドメインに設定されている場合は、VTP バージョン 3 から VTP バージョン 2 に変換でき ません。

(注)

スイッチが LAN Lite イメージを実行中の場合は、最大 64 の VLAN をサポートできます。

スイッチは合計 255 (標準範囲および拡張範囲)の VLAN をサポートしますが、スイッチのハード ウェアの使用状況は、設定済み機能の個数に左右されます。

スイッチは、最大 128 のスパニング ツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus (PVST+) または Rapid PVST+ をサポートします。VLAN ごとに 1 つずつスパニング ツリー インス タンスを使用できます。スパニング ツリー インスタンス数および VLAN 数の詳細については、「標準 範囲 VLAN 設定時の注意事項」(P.13-6) を参照してください。スイッチは、イーサネット ポート経由 の VLAN トラフィックの送信方式として IEEE 802.1Q トランキングのみをサポートします。



スイッチが LAN Lite イメージを実行中の場合は、最大 64 のスパニング ツリー インスタンスをサポー トできます。

VLAN ポート メンバシップ モード

VLAN に所属するポートは、メンバシップ モードを割り当てることで設定します。メンバシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。 表 13-1 に、各種メンバシップ モード、およびそれぞれのメンバシップと VTP の特性を示します。

表 13-1 ポートのメンバシップ モードとその特性

メンバシップ モード	VLAN メンバシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。 詳細については、「VLAN へのスタティック アクセス ポートの 割り当て」(P.13-10)を参照してください。	VTP は必須ではありません。VTP を使 用して情報をグローバルに伝播させない 場合は、VTP モードをトランスペアレン トに設定します。VTP に加入するには、 2 台めのスイッチのトランク ポートに接 続されたスイッチ上に、トランク ポート が少なくとも1 つなければなりません。
トランク (IEEE 802.1Q)	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべて の VLAN のメンバーです。ただし、メンバシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リス トを変更して、リストに指定したトランク ポート上の VLAN へ のフラッディング トラフィックを阻止することもできます。 トランク ポートの設定については、「トランク ポートとしての イーサネット インターフェイスの設定」(P.13-16) を参照して ください。	VTP を推奨しますが、必須ではありませ ん。VTP は、ネットワーク全体にわたっ て VLAN の追加、削除、名前変更を管 理することにより、VLAN 設定の整合性 を維持します。VTP はトランク リンク を通じて他のスイッチと VLAN コン フィギュレーション メッセージを交換し ます。
ダイナミック アクセス	ダイナミックアクセス ポートは 1 つの VLAN (VLAN ID が 1 ~ 4094) にのみ所属し、VMPS によって動的に割り当てられま す。VMPS には Catalyst 5000 または Catalyst 6500 シリーズ ス イッチを使用できますが、たとえば、Catalyst 2960 スイッチは 使用できません。Catalyst 2960 スイッチが、VMPS クライアン トです。 同一スイッチ上でダイナミックアクセス ポートとトランク ポー トを使用できますが、ダイナミックアクセス ポートは別のス イッチではなく、エンド ステーションまたはハブに接続する必 要があります。 設定情報については、「VMPS クライアント上のダイナミックア クセス ポートの設定」(P.13-28) を参照してください。	VTP は必須です。 VMPS およびクライアントを同じ VTP ドメイン名で設定してください。 VTP に加入するには、2 台めのスイッチ のトランク ポートに、スイッチ上のトラ ンク ポートが少なくとも1 つ接続されて いる必要があります。
音声 VLAN	音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データトラフィックに別の VLAN を使用するように設定されたアクセス ポートです。 音声 VLAN ポートの詳細については、第15章「音声 VLAN の 設定」を参照してください。	VTP は不要です。VTP は音声 VLAN に 対して無効です。

アクセスモードとトランクモード、および機能の定義の詳細については、表 13-4 (P.13-15) を参照 してください。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理 します。詳細については、「MAC アドレス テーブルの管理」(P.6-22)を参照してください。

標準範囲 VLAN の設定

標準範囲 VLAN は、VLAN ID が 1 ~ 1005 の VLAN です。スイッチが VTP サーバまたは VTP トラ ンスペアレント モードの場合、VLAN データベース内の VLAN 2 ~ 1001 の設定を追加、変更、また は削除できます (VLAN ID 1 および 1002 ~ 1005 は自動作成され、削除できません)。

VTP バージョン 1 および 2 では、拡張範囲 VLAN (ID が 1006 ~ 4094 の VLAN) を作成する場合は スイッチを VTP トランスペアレント モードにする必要があります。ただし、これらの拡張範囲 VLAN は VLAN データベースに格納されません。VTP バージョン 3 は、VTP サーバ モードおよびトランス ペアレント モードで拡張範囲 VLAN をサポートします。「拡張範囲 VLAN の設定」(P.13-11) を参照 してください。

VLAN ID 1 ~ 1005 の設定はファイル *vlan.dat* (VLAN データベース) に書き込まれます。この設定 を表示するには、**show vlan** 特権 EXEC コマンドを入力します。*vlan.dat* ファイルはフラッシュ メモ リに保存されます。



vlan.dat ファイルを手動で削除しようとすると、VLAN データベースの不整合が生じる可能性があ ります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応す るコマンド リファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、第 14 章「VTP の設定」を参照してください。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバシップ モード の定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行 コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、show running-config 特権 EXEC コマンドを使用します。

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ (イーサネット、FDDI、FDDI Network Entity Title [NET]、TrBRF または TrCRF、 トークンリング、トークンリング Net)
- VLAN ステート (アクティブまたはサスペンド)
- VLAN のMaximum Transmission Unit (MTU; 最大伝送ユニット)
- Security Association Identifier (SAID)
- Token Ring Bridge Relay Function (TrBRF; トークンリング ブリッジ リレー機能) VLAN のブ リッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- Token Ring Concentrator Relay Function (TrCRF; トークンリング コンセントレータ リレー機能) VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号



ここでは、これらのパラメータの大部分の設定手順について説明しません。VLAN 設定を制御するコ マンドおよびパラメータの詳細については、このリリースに対応するコマンド リファレンスを参照し てください。

■標準範囲 VLAN の設定

ここでは、標準範囲 VLAN の設定情報について説明します。

- 「トークンリング VLAN」 (P.13-6)
- 「標準範囲 VLAN 設定時の注意事項」(P.13-6)
- 「標準範囲 VLAN の設定」(P.13-7)
- 「イーサネット VLAN のデフォルト設定」(P.13-8)
- 「イーサネット VLAN の作成または変更」(P.13-8)
- 「VLAN の削除」(P.13-10)
- 「VLAN へのスタティック アクセス ポートの割り当て」(P.13-10)

トークンリング VLAN

このスイッチはトークンリング接続をサポートしていませんが、トークンリング接続を行っている Catalyst 5000 シリーズ スイッチなどのリモート デバイスを、サポート対象スイッチのうちの 1 台から 管理できます。VTP バージョン 2 が稼動しているスイッチは、次のトークンリング VLAN に関する情 報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

トークンリング VLAN の詳しい設定手順については、『Catalyst 5000 Series Software Configuration Guide』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- スイッチは、VTP クライアント、サーバ、およびトランスペアレント モードで 255 VLAN をサ ポートします。
- 標準範囲 VLAN は、1 ~ 1001 の番号で識別します。VLAN 番号 1002 ~ 1005 は、トークンリン グおよび FDDI VLAN 専用です。
- VLAN 1 ~ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレントの場合、VTP および VLAN 設定はスイッチの実行コンフィギュレーション ファイルにも格納されます。
- VTP バージョン1 および2 では、スイッチが VLAN ID 1006 ~ 4094 をサポートするのは、VTP トランスペアレント モード (VTP はディセーブル) だけです。これらは拡張範囲 VLAN であり、 設定オプションには制限があります。VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン3 は、拡張範囲 VLAN (VLAN 1006 ~ 4094) データベース伝播をサポートします。拡張 VLAN を設定している 場合は、VTP バージョン3 からバージョン1 または2 に変換できません。「拡張範囲 VLAN の設 定」(P.13-11) を参照してください。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードに しておく必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要 があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、 FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を 伝播します。

 スイッチは 128 のスパニング ツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニング ツリー インスタンス数よりも多い場合、スパニング ツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニング ツリーはディ セーブルになります。スイッチ上の使用可能なスパニング ツリー インスタンスをすべて使い切っ てしまったあとに、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパ ニング ツリーが稼動しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォル トの許可リスト (すべての VLAN を許可するリスト)が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニング ツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定すること により、このような可能性を防ぐことができます。

スイッチ上の VLAN の数がサポートされているスパニング ツリー インスタンスの最大数を超える 場合、スイッチ上に IEEE 802.1s Multiple STP(MSTP)を設定して、複数の VLAN を単一のス パニング ツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 17章「MSTP の設定」を参照してください。

標準範囲 VLAN の設定

VLAN を vlan global コンフィギュレーションコマンドで設定するには、VLAN ID を入力します。新 規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変 更します。デフォルトの VLAN 設定を使用するか(表 13-2を参照)、複数のコマンドを入力して VLAN を設定できます。このモードで使用できるコマンドの詳細については、このリリースのコマン ドリファレンスに記載されている vlan グローバル コンフィギュレーション コマンドを参照してくだ さい。設定を終了したら、VLAN コンフィギュレーション モードを終了して、設定を有効にする必要 があります。VLAN 設定を表示するには、show vlan 特権 EXEC コマンドを入力します。

VLAN ID 1 ~ 1005 の設定は、常に VLAN データベースに保存されます(vlan.dat ファイル)。VTP モードがトランスペアレントの場合、それらの設定もスイッチの実行コンフィギュレーション ファイ ルに格納されます。copy running-config startup-config 特権 EXEC コマンドを使用して、スタート アップ コンフィギュレーション ファイルに設定を保存できます。VLAN 設定を表示するには、show vlan 特権 EXEC コマンドを入力します。

VLAN および VTP 情報(拡張範囲 VLAN 設定情報を含む)をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランス ペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ)、スタートアップ コ ンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベー ス内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベー スと一致しない場合、最初の 1005 の VLAN のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン1および2では、VTP モードがサーバの場合、最初の1005のVLAN だけのドメイン名およびVLAN 設定にはVLAN データベース情報が使用されます。VTP バージョン3は、VLAN 1006~4094もサポートします。

イーサネット VLAN のデフォルト設定

表 13-2 にイーサネット VLAN のデフォルト設定を示します。

(注)

スイッチがサポートするのは、イーサネット インターフェイスだけです。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、 他のスイッチに対する VTP グローバル アドバタイズにのみ設定します。

表 13-2 イーサネット VLAN のデフォルト値および範囲

パラメータ	デフォルト	範囲
VLAN ID	1	$1 \sim 4094$
		(注) 拡張範囲 VLAN (VLAN ID 1006 ~ 4094) は、VTP バージョン 3 の場合 だけ VLAN データベースに保存され ます。
VLAN 名	<i>VLANxxxx</i> 。 <i>xxxx</i> は VLAN ID 番号に等しい 4 桁の 数字(先行ゼロを含む)です。	範囲なし
IEEE 802.10 SAID	100001 (100000 と VLAN ID の和)	$1 \sim 4294967294$
MTU サイズ	1500	$1500 \sim 18190$
トランスレーショナル ブリッジ1	0	$0 \sim 1005$
トランスレーショナル ブリッジ 2	0	$0 \sim 1005$
VLAN ステート	アクティブ	アクティブ、サスペンド
リモート SPAN	ディセーブル	イネーブル、ディセーブル

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN には、1 ~ 1001 の 4 桁の一意の ID が設定されていま す。VLAN ID 1002 ~ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。

(注)

VTP バージョン1および2では、スイッチがVTP トランスペアレントモードの場合、1006を超える VLAN ID を割り当てることができますが、それらは VLAN データベースに追加されません。「拡張範 囲 VLAN の設定」(P.13-11)を参照してください。

VLAN の追加時に指定されるデフォルトパラメータの一覧は、「標準範囲 VLAN の設定」(P.13-5)を 参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan vlan-id	VLAN ID を入力して、VLAN コンフィギュレーション モードを開 始します。新規の VLAN ID を入力して VLAN を作成するか、また は既存の VLAN ID を入力してその VLAN を変更します。
		 (注) このコマンドで指定できる VLAN ID 範囲は 1 ~ 4094 です。 1005 を超える VLAN ID(拡張範囲 VLAN)を追加する手 順については、「拡張範囲 VLAN の設定」(P.13-11)を参照 してください。
ステップ 3	name vlan-name	(任意) VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた vlan-id が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	mtu mtu-size	(任意)MTU サイズ(または他の VLAN 特性)を変更します。
ステップ 5	remote-span	(任意) リモート Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) セッションに対する RSPAN VLAN として、VLAN を 設定します。リモート SPAN の詳細は、第 27 章「SPAN および RSPAN の設定」を参照してください。
		(注) RSPAN を使用するには、スイッチが LAN Base イメージを 実行している必要があります。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	<pre>show vlan {name vlan-name id vlan-id}</pre>	設定を確認します。
ステップ 8	copy running-config startup config	(任意) スイッチが VTP トランスペアレント モードである場合、 VLAN 設定は実行コンフィギュレーション ファイルと VLAN デー タベースに保存されます。この場合、スイッチのスタートアップ コ ンフィギュレーション ファイルに設定が保存されます。

イーサネット VLAN を作成または変更するには、特権 EXEC モードで次の手順を実行します。

VLAN 名をデフォルトの設定に戻すには、no name、no mtu または no remote-span コマンドを使用 します。

次に、イーサネット VLAN 20 を作成し、test20 という名前を付け、VLAN データベースに追加する例 を示します。

Switch# configure terminal Switch(config)# vlan 20 Switch(config-vlan)# name test20 Switch(config-vlan)# end

VLANの削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのスイッチ から VLAN を削除した場合、そのスイッチ上に限り VLAN が削除されます。

メディア タイプが異なるデフォルトの VLAN を削除することはできません。たとえば、イーサネット VLAN 1、および FDDI またはトークンリング VLAN の 1002 ~ 1005 を削除することはできません。

注意

VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになりま す。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に(非アクティブで) 対応付けられたままです。

スイッチ上で VLAN を削除するには、特権 EXEC モードで次の手順を実行します。

_	コマンド	目的
-	configure terminal	グローバル コンフィギュレーション モードを開始します。
-	no vlan vlan-id	VLAN ID を入力して、VLAN を削除します。
_	end	特権 EXEC モードに戻ります。
	show vlan brief	VLAN が削除されたことを確認します。
_	copy running-config startup config	(任意) スイッチが VTP トランスペアレント モードである場合、 VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタート アップ コンフィギュレーション ファイルに設定が保存されます。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって (VTP トランスペアレント モード)、VTP に VLAN 設定情報 をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバー スイッチのポートを VLAN に割り当てる場合、最初に rcommand 特権 EXEC コマ ンドを使用して、そのクラスタ メンバー スイッチにログインします。



存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます(「イーサネット VLAN の作成または変更」(P.13-8)を参照)。

VLAN データベース内の VLAN にポートを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	VLAN に追加するインターフェイスを入力します。
ステップ 3	switchport mode access	ポート(レイヤ 2 アクセス ポート)の VLAN メンバシップ モー ドを定義します。
ステップ 4	switchport access vlan vlan-id	VLAN にポートを割り当てます。有効な VLAN ID は 1 ~ 4094 です。

	コマンド	目的
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface <i>interface-id</i>	インターフェイスの VLAN メンバシップ モードを確認します。
ステップ 7	show interfaces interface-id switchport	表示された Administrative Mode および Access Mode VLAN フィールドの設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、**default interface** *interface-id* インターフェイス コン フィギュレーション コマンドを使用します。

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet0/1 Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan 2 Switch(config-if)# end

拡張範囲 VLAN の設定

VTP バージョン 1 およびバージョン 2 では、スイッチが VTP トランスペアレント モード (VTP が ディセーブル)の場合、拡張範囲 VLAN (1006 ~ 4094)を作成できます。VTP バージョンは、サー バモードまたはトランスペアレント モードで拡張範囲 VLAN をサポートします。サービス プロバイ ダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応 できます。拡張範囲 VLAN ID は、VLAN ID が許可されている任意の switchport コマンドで使用でき ます。

VTP バージョン1 または2 では、拡張範囲 VLAN の設定は VLAN データベースには格納されません。 ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファ イルに格納されます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。VTP バージョン 3 で作成された拡 張範囲 VLAN は、VLAN データベースに保存されます。



スイッチは 4094 の VLAN ID をサポートしますが、実際にサポートされる VLAN の数については、 「サポートされる VLAN」(P.13-3) を参照してください。

ここでは、拡張範囲 VLAN の設定情報について説明します。

- 「VLAN のデフォルト設定」(P.13-12)
- 「拡張範囲 VLAN 設定時の注意事項」(P.13-12)
- 「拡張範囲 VLAN の作成」(P.13-12)

VLAN のデフォルト設定

表 13-2 (P.13-8) にイーサネット VLAN のデフォルト設定を示します。拡張範囲 VLAN については MTU サイズおよびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォル ト状態のままでなければなりません。

(注)

リモート SPAN をサポートするには、スイッチが LAN Base イメージを実行している必要があります。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、スイッチが VTP バージョン 3 を実行していない場合は VLAN データ ベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。
- VTP バージョン1および2では、拡張範囲のVLANを作成する場合は、スイッチをVTPトランスペアレントモードにする必要があります。VTPモードがサーバまたはクライアントの場合、エラーメッセージが生成され、拡張範囲VLANが拒否されます。VTPバージョン3は、サーバモードおよびトランスペアレントモードで拡張範囲VLANをサポートします。
- VTP バージョン1または2では、グローバルコンフィギュレーションモードで、VTP モードをトランスペアレントに設定できます。「VTP モードの設定」(P.14-11)を参照してください。VTPトランスペアレントモードでスイッチが起動するように、この設定をスタートアップコンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン3で拡張範囲 VLAN を作成する場合は、VTPバージョン1または2に変更できません。
- 拡張範囲 VLAN では、STP はデフォルトでイネーブルになりますが、no spanning-tree vlan vlan-id グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッ チ上に最大数のスパニング ツリー インスタンスが存在している場合に、VLAN を新規作成する と、この VLAN 上でスパニング ツリーはディセーブルになります。スイッチ上の VLAN の数が スパニング ツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s MSTP を設定 して、複数の VLAN を単一のスパニング ツリー インスタンスにマッピングすることを推奨しま す。MSTP の詳細については、第 17 章「MSTP の設定」を参照してください。
- スイッチは合計 255(標準範囲および拡張範囲)の VLAN をサポートしますが、スイッチのハードウェアの使用状況は、設定済み機能の個数に左右されます。拡張範囲 VLAN を作成するときに、使用できるハードウェア リソースが不足していると、エラーメッセージが生成され、拡張範囲 VLAN が拒否されます。

拡張範囲 VLAN の作成

グローバル コンフィギュレーション モードで拡張範囲 VLAN を作成するには、vlan グローバル コン フィギュレーション コマンドを入力し、1006 ~ 4094 の VLAN ID を指定します。拡張範囲 VLAN は イーサネット VLAN のデフォルトの特性を備えており (表 13-2を参照)、MTU サイズおよび RSPAN 設定だけが変更できるパラメータです。すべてのパラメータのデフォルト値については、コマンド リ ファレンスに記載された vlan グローバル コンフィギュレーション コマンドの説明を参照してくださ い。VTP バージョン 1 または 2 では、スイッチが VTP トランスペアレント モードでない場合に拡張範 囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラー メッセージが生 成され、拡張範囲 VLAN が作成されません。 VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチの 実行コンフィギュレーション ファイルに保存されます。拡張範囲 VLAN 設定をスイッチのスタート アップ コンフィギュレーション ファイルに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。VTP バージョン 3 は、拡張範囲 VLAN を VLAN データベースに保存 します。

拡張範囲 VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	vtp mode transparent	スイッチを VTP トランスペアレント モードに設定し、VTP をディ セーブルにします。	
		(注) この手順は、VTP バージョン3では不要です。	
ステップ 3	vlan vlan-id	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ~ 4094 です。	
ステップ 4	mtu mtu-size	(任意) MTU サイズを変更して、VLAN を変更します。	
		(注) CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、mtu <i>mtu-size</i> コマンドおよび remote-span コマンドだけです。	
ステップ 5	remote-span	(任意) RSPAN VLAN として VLAN を設定します。「RSPAN VLAN としての VLAN の設定」(P.27-18)を参照してください。	
		RSPAN をサポートできるのは、スイッチで LAN Base イメージが実 行されている場合だけです。	
ステップ 6	end	特権 EXEC モードに戻ります。	
ステップ 7	show vlan id vlan-id	VLAN が作成されたことを確認します。	
ステップ 8	copy running-config startup config	スイッチのスタートアップ コンフィギュレーション ファイルに設定 を保存します。拡張範囲 VLAN 設定を保存するには、VTP トランス ペアレント モード設定および拡張範囲 VLAN 設定をスイッチのス タートアップ コンフィギュレーション ファイルに保存する必要があ ります。これらを保存しないと、スイッチをリセットした場合に、 スイッチがデフォルトで VTP サーバ モードになり、拡張範囲 VLAN ID は保存されません。	
		(注) VTP バージョン 3 では、VLAN コンフィギュレーションは VLAN データベースにも保存されます。	

拡張範囲 VLAN を削除するには、no vlan vlan-id グローバル コンフィギュレーション コマンドを使用 します。

スタティック アクセス ポートを拡張範囲 VLAN に割り当てる手順は、標準範囲 VLAN の手順と同じ です。「VLAN へのスタティック アクセス ポートの割り当て」(P.13-10) を参照してください。

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する 例を示します。

Switch(config)# vtp mode transparent Switch(config)# vlan 2000 Switch(config-vlan)# end Switch# copy running-config startup config

VLAN の表示

拡張範囲 VLAN を含む、スイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。VLAN ステータス、ポート、および設定情報も表示されます。 表 13-3 に、VLAN をモニタするための特権 EXEC コマンドを示します。

表 13-3 VLAN モニタ コマンド

コマンド	目的
show interfaces [vlan <i>vlan-id</i>]	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [id vlan-id]	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。

show コマンド オプションおよび出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

VLAN トランクの設定

ここでは、次の概要について説明します。

- 「トランキングの概要」(P.13-14)
- 「レイヤ2イーサネットインターフェイス VLAN のデフォルト設定」(P.13-16)
- 「トランクポートとしてのイーサネットインターフェイスの設定」(P.13-16)
- 「トランク ポートの負荷分散の設定」(P.13-21)

トランキングの概要

トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーキング デバ イス (ルータ、スイッチなど)の間のポイントツーポイント リンクです。イーサネット トランクは 1 つ のリンクを介して複数の VLAN トラフィックを搬送するので、VLAN をネットワーク全体に拡張できま す。スイッチでは、IEEE 802.1Q カプセル化がサポートされています。

トランクを設定できるのは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対 してです。EtherChannel の詳細については、第 36 章「EtherChannel およびリンクステート トラッキ ングの設定」を参照してください。

イーサネット トランク インターフェイスは、表 13-4に示すトランキング モードをサポートしていま す。インターフェイスをトランキングまたは非トランキングとして設定したり、近接インターフェイス とトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシ エーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、PPP(ポイントツーポイント プロトコル)である Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)によって管理されます。ただし、一部のイン ターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合 があります。 この事態を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレー ムを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介してトランキングを行わない場合は、switchport mode access インターフェ イス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、switchport mode trunk および switchport nonegotiate インターフェイス コンフィギュレーション コマンドを使用 して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

表	13-4	レイヤ 2 インターフェイ	スモード
---	------	---------------	------

モード	機能
switchport mode access	インターフェイス(アクセス ポート)を永続的な非トランキング モードにして、リン クの非トランク リンクへの変換をネゴシエートします。インターフェイスは、近接イン ターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インター フェイスになります。
switchport mode dynamic auto	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェ イスは、近接インターフェイスが <i>trunk</i> または <i>desirable</i> モードに設定されている場合、 トランク インターフェイスになります。すべてのイーサネット インターフェイスのデ フォルトのスイッチポート モードは dynamic auto です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、近接インターフェイスが trunk、desirable、または auto モードに設定されている場合、トランク インターフェイスになります。
switchport mode trunk	インターフェイスを永続的なトランキング モードにして、近接リンクのトランク リン クへの変換をネゴシエートします。インターフェイスは、近接インターフェイスがトラ ンク インターフェイスでない場合でも、トランク インターフェイスになります。
switchport nonegotiate	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、イン ターフェイス スイッチポート モードが access または trunk の場合だけ使用できます。 トランク リンクを確立するには、手動で近接インターフェイスをトランク インター フェイスとして設定する必要があります。

IEEE 802.1Qの設定に関する考慮事項

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

 IEEE 802.1Q トランクを使用して接続しているシスコ製スイッチのネットワークでは、スイッチは トランク上で許容される VLAN ごとに1つのスパニング ツリー インスタンスを維持します。他社 製のデバイスは、すべての VLAN でスパニング ツリー インスタンスを1つサポートする場合があ ります。

IEEE 802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続する場合、シスコ製 スイッチは、トランクの VLAN のスパニング ツリー インスタンスを、他社製の IEEE 802.1Q ス イッチのスパニング ツリー インスタンスと結合します。ただし、各 VLAN のスパニング ツリー情 報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離されたシスコ製スイッチに よって維持されます。シスコ製スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ 間の単一トランク リンクとして扱われます。

IEEE 802.1Qトランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニング ツリー ループが発生する可能性があります。

 ネットワーク上のすべてのネイティブ VLAN についてスパニング ツリーをディセーブルにせず に、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニング ツリーをディセーブルにすると、 スパニング ツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニング ツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニング ツリーをディセーブルにすることを推奨します。また、ネットワークにルー プがないことを確認してから、スパニング ツリーをディセーブルにしてください。

レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

表 13-5 に、レイヤ2イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 13-5 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
インターフェイス モード	switchport mode dynamic auto
VLAN 許容範囲	VLAN 1 \sim 4094
プルーニングに適格な VLAN 範囲	VLAN 2 \sim 1001
デフォルト VLAN(アクセス ポート用)	VLAN 1
ネイティブ VLAN(IEEE 802.1Q トラ	VLAN 1
ンク用)	

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートは VTP アドバタイズを送受信するので、VTP を使用する場合は、スイッチ上で少なく とも1 つのトランク ポートが設定されており、そのトランク ポートが第2のスイッチのトランク ポー トに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズ を受信できません。

ここでは、次の設定情報について説明します。

- 「他の機能との相互作用」(P.13-16)
- 「トランクでの許可 VLAN の定義」(P.13-18)
- 「プルーニング適格リストの変更」(P.13-19)
- 「タグなしトラフィック用ネイティブ VLAN の設定」(P.13-20)

他の機能との相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートをセキュア ポートにすることはできません。
- トランクポートをまとめて EtherChannel ポート グループにすることはできますが、グループ内の すべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグ ループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラ メータのいずれかについて、設定を変更すると、入力した設定値がスイッチによってグループ内の すべてのポートに伝播されます。
 - 許可 VLAN リスト。
 - 各 VLAN の STP ポート プライオリティ。

- STP PortFast の設定値。

- トランクステータス。ポートグループ内の1つのポートがトランクでなくなると、すべての ポートがトランクでなくなります。
- PVST モードで設定するトランク ポートの数は 24 まで、MST モードで設定するトランク ポートの数は 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、 IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとして も、ポート モードは変更されません。
- ダイナミックモードのポートは、ネイバとトランクポートへの変更をネゴシエートする場合があります。ダイナミックポートでIEEE 802.1x をイネーブルにしようとすると、エラーメッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、ポートモードは変更されません。

トランク ポートの設定

ポートをトランク ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	トランクに設定するポートを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
ステップ 3	switchport mode {dynamic {auto desirable} trunk}	インターフェイスをレイヤ2トランクとして設定します(インター フェイスがレイヤ2アクセス ポートである場合、またはトランキン グモードを設定する場合に限り必要となります)。
		 dynamic auto: 近接インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これがデフォルトです。
		 dynamic desirable: 近接インターフェイスが trunk、desirable、 または auto モードに設定されている場合に、インターフェイス をトランク リンクとして設定します。
		 trunk: 近接インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシェートします。
ステップ 4	switchport access vlan vlan-id	(任意) インターフェイスがトランキングを停止した場合に使用する デフォルト VLAN を指定します。
ステップ 5	switchport trunk native vlan vlan-id	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces interface-id switchport	インターフェイスのスイッチポート設定を表示します。 Administrative Mode および Administrative Trunking Encapsulation フィールドに表示されます。
ステップ 8	show interfaces interface-id trunk	インターフェイスのトランク設定を表示します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、default interface interface-id インターフェイス コン フィギュレーション コマンドを使用します。トランキング インターフェイスのすべてのトランキング 特性をデフォルトにリセットするには、no switchport trunk インターフェイス コンフィギュレーショ ン コマンドを使用します。トランキングをディセーブルにするには、switchport mode access イン ターフェイス コンフィギュレーション コマンドを使用して、ポートをスタティック アクセス ポートと して設定します。

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、近接インターフェ イスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```

トランクでの許可 VLAN の定義

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トラン クですべての VLAN ID (1 ~ 4094) が許可されます。ただし、許可リストから VLAN を削除するこ とにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。 トランクが伝送するトラフィックを制限するには、switchport trunk allowed vlan remove vlan-list イ ンターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除し ます。



VLAN1は、すべてのシスコ製スイッチのすべてのトランクポートのデフォルトVLANです。以前 は、すべてのトランクリンクでVLAN1を必ずイネーブルにする必要がありました。VLAN1の最小 化機能を使用して、個々のVLANトランクリンクでVLAN1をディセーブルに設定できます。これに より、ユーザトラフィック(スパニングツリーアドバタイズなど)はVLAN1で送受信されなくなり ます。

スパニング ツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除し て個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol (CDP)、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)、DTP、および VTP など の管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、switchport trunk allowed の設定には 関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN に ついて同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの 許可リストにその VLAN が登録されている場合に、VLAN のメンバーになることができます。VTP が 新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録され ている場合、トランク ポートは自動的にその VLAN のメンバーになります。VTP が新しい VLAN を 認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートは その VLAN のメンバーにはなりません。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。
ステップ 3	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	switchport trunk allowed vlan {add	(任意) トランク上で許可される VLAN のリストを設定します。
	all except remove} vlan-list	add、all、except、および remove キーワードの使用方法について は、このリリースに対応するコマンド リファレンスを参照してくだ さい。
		<i>vlan-list</i> パラメータは、1 ~ 4094 の単一の VLAN 番号、または 2 つ の VLAN 番号(小さい方が先、ハイフンで区切る)で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、または ハイフンで指定した範囲の間には、スペースを入れないでください。
		デフォルトでは、すべての VLAN が許可されます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport	表示された <i>Trunking VLANs Enabled</i> フィールドの設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トランクの許可リストを変更するには、特権 EXEC モードで次の手順を実行します。

すべての VLAN の許可 VLAN リストをデフォルトに戻すには、no switchport trunk allowed vlan イ ンターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに専用の適格 リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必 要があります。VTP プルーニングをイネーブルにする方法については、「VTP プルーニングのイネー ブル化」(P.14-16)を参照してください。

トランク ポートのプルーニング適格リストから VLAN を削除するには、特権 EXEC モードで次の手順 を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	VLAN プルーニングを適用するトランク ポートを選択し、インター
		フェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3 switchpor except I [,vlan[,vla	<pre>switchport trunk pruning vlan {add except none remove} vlan-list</pre>	トランクからのプルーニングを許可する VLAN のリストを設定しま す (「VTP プルーニング」(P.14-6)を参照)。
	[,vlan[,vlan[,,,]]	add、except、none、および remove キーワードの使用方法について は、このリリースに対応するコマンド リファレンスを参照してくだ さい。
		連続していない VLAN ID は、カンマ(スペースなし)で区切りま す。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ~ 1001 です。拡張範囲 VLAN(VLAN ID 1006 ~ 4094)はプルーニングで きません。
		プルーニング不適格の VLAN は、フラッディング トラフィックを受 信します。
		デフォルトでは、プルーニングが許可される VLAN のリストには、 VLAN 2 ~ 1001 が含まれます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id switchport	表示された Pruning VLANs Enabled フィールドの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN のプルーニング適格リストをデフォルトに戻すには、no switchport trunk pruning vlan インターフェイス コンフィギュレーション コマンドを使用します。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。ネイティブ VLAN は、デフォルトでは VLAN 1 です。



ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定についての詳細は、「IEEE 802.1Q の設定に関する考慮事項」(P.13-15) を参照して ください。

IEEE 802.1Q トランクでネイティブ VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport trunk native vlan vlan-id	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。
		<i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
ステップ 4	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	show interfaces interface-id switchport	Trunking Native Mode VLAN フィールドの設定を確認します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

ネイティブ VLAN をデフォルト (VLAN 1) に戻すには、no switchport trunk native vlan インター フェイス コンフィギュレーション コマンドを使用します。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなし で送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信し ます。

トランク ポートの負荷分散の設定

負荷分散により、スイッチに接続しているパラレルトランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で1つのパラレルリンク以外のすべてのリンクをブ ロックします。負荷分散を行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラ フィックが分散されます。

トランク ポートで負荷分散を設定するには、STP ポート プライオリティまたは STP パス コストを使 用します。STP ポート プライオリティを使用して負荷分散を設定する場合には、両方の負荷分散リン クを同じスイッチに接続する必要があります。STP パス コストを使用して負荷分散を設定する場合に は、それぞれの負荷分散リンクを同一のスイッチにも、2 台の異なるスイッチにも接続できます。STP の詳細については、第 16 章「STP の設定」を参照してください。

STP ポート プライオリティによる負荷分散

同一スイッチ上の2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用 して、どのポートをイネーブルとし、どのポートをブロッキングステートとするかを判断します。パ ラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべ てのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い(値の小さい) トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの 低い(値の大きい)トランク ポートは、その VLAN に対してブロッキング ステートのままです。1つ のトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

図 13-2 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ~ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ~ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ~ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ~ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク1がVLAN8~10のトラフィックを伝送し、トランク2がVLAN 3~6のトラフィックを伝送します。アクティブトランクで障害が起きた場合には、プライオリティの 低いトランクが引き継ぎ、それらすべてのVLANのトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。



図 13-2 STP ポート プライオリティによる負荷分散

図 13-2 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	スイッチ A で、グローバル コンフィギュレーション モードを開 始します。
ステップ 2	vtp domain domain-name	VTP 管理ドメインを設定します。
		1~32 文字のドメイン名を使用できます。
ステップ 3	vtp mode server	スイッチAをVTPサーバとして設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show vtp status	スイッチ A および B の両方で、VTP 設定を確認します。
		表示された VTP Operating Mode および VTP Domain Name フィールドをチェックします。
ステップ 6	show vlan	スイッチ A のデータベースに VLAN が存在していることを確認 します。
ステップ 7	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 8	interface <i>interface-id_1</i>	トランクとして設定するインターフェイスを定義し、インター フェイス コンフィギュレーション モードを開始します。
ステップ 9	switchport mode trunk	ポートをトランク ポートとして設定します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	<pre>show interfaces interface-id_1 switchport</pre>	VLAN 設定を確認します。
ステップ 12		スイッチの2番めのポートに対して、スイッチA上でステップ7 ~10を実行します。
ステップ 13		スイッチ B でステップ 7 ~10 を繰り返し、スイッチ A で設定さ れたトランク ポートに接続するトランク ポートを設定します。
ステップ 14	show vlan	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。 スイッチ B が VLAN 設定を 学習したことを確認します。
ステップ 15	configure terminal	スイッチ A で、グローバル コンフィギュレーション モードを開 始します。
ステップ 16	interface <i>interface-id_1</i>	STP のポート プライオリティを設定するインターフェイスを定義 し、インターフェイス コンフィギュレーション モードを開始しま す。
ステップ 17	spanning-tree vlan 8-10 port-priority 16	VLAN 8 ~ 10 にポート プライオリティ 16 を割り当てます。

	コマンド	目的
ステップ 18	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 19	interface <i>interface-id_2</i>	STP のポート プライオリティを設定するインターフェイスを定義 し、インターフェイス コンフィギュレーション モードを開始しま す。
ステップ 20	spanning-tree vlan 3-6 port-priority 16	VLAN 3 ~ 6 にポート プライオリティ 16 を割り当てます。
ステップ 21	end	特権 EXEC モードに戻ります。
ステップ 22	show running-config	設定を確認します。
ステップ 23	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

STP パス コストによる負荷分散

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付 け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トラン クを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持し ます。

図 13-3 で、トランク ポート1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2~4は、トランクポート1で30というパスコストが割り当てられています。
- VLAN 8 ~ 10 は、トランク ポート1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8 ~ 10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2 ~ 4は、トランクポート2で100BASE-Tのデフォルトのパスコストである19のままです。

図 13-3 パス コストによってトラフィックが分散される負荷分散トランク



図 13-3 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	スイッチ A で、グローバル コンフィギュレーション モードを開始 します。
ステップ 2	interface interface-id_1	トランクとして設定するインターフェイスを定義し、インターフェ イス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	switchport mode trunk	ポートをトランク ポートとして設定します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5		スイッチA内の2番めのインターフェイスでステップ2~4を繰り 返します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。画面で、インターフェイスがトランク ポートと して設定されていることを確認してください。
ステップ 8	show vlan	トランク リンクがアクティブになると、スイッチ A がもう一方の スイッチから VTP 情報を受信します。 スイッチ A が VLAN 設定を 学習したことを確認します。
ステップ 9	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 10	interface <i>interface-id_l</i>	STP コストを設定するインターフェイスを定義し、インターフェイ ス コンフィギュレーション モードを開始します。
ステップ 11	spanning-tree vlan 2-4 cost 30	VLAN 2 ~ 4 のスパニング ツリー パス コストを 30 に設定します。
ステップ 12	end	グローバル コンフィギュレーション モードに戻ります。
ステップ 13		スイッチ A に設定したもう一方のトランク インターフェイスで、 ステップ 9 ~ 12 を繰り返し、VLAN 8、9、および 10 のスパニン グ ツリー パス コストを 30 に設定します。
ステップ 14	exit	特権 EXEC モードに戻ります。
ステップ 15	show running-config	設定を確認します。両方のトランクインターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 16	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VMPS の設定

VLAN Query Protocol (VQP) は、ダイナミックアクセス ポートをサポートする場合に使用します。 ダイナミックアクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC (メディア アクセス制御)送信元アドレスに基づいて VLAN を割り当てます。未知の MAC ア ドレスが検出されるたびに、スイッチはリモート VMPS に VQP クエリーを送信します。クエリーには 新たに検出された MAC アドレスとそのアドレスを検出したポートが含まれます。VMPS はそのポー トの VLAN 割り当てで応答します。このスイッチを VMPS サーバにすることはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信できます。

ここでは、次の情報について説明します。

- 「VMPS の概要」(P.13-25)
- 「VMPS クライアントのデフォルト設定」(P.13-26)
- 「VMPS 設定時の注意事項」(P.13-26)
- 「VMPS クライアントの設定」(P.13-27)
- 「VMPS のモニタ」 (P.13-30)
- 「ダイナミックアクセス ポート VLAN メンバシップのトラブルシューティング」(P.13-30)
- 「VMPS の設定例」(P.13-31)

VMPS の概要

クライアント スイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを 送信します。このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピン グを検索します。サーバの応答は、このマッピングと、サーバがオープン モードかセキュア モードか に基づいて行われます。セキュア モードの場合、サーバは不正なホストが検出されると、ポートを シャットダウンします。オープン モードでは、サーバはホストに対してポート アクセスを拒否するだ けです。

ポートが*未割り当て*の場合(つまり、VLAN 割り当てがまだ設定されていない場合)、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホスト へのアクセスを許可する VLAN 割り当て応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS はア クセス拒否応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS は ポートシャットダウン応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は成功応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブ ホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、アクセス拒否またはポート シャットダウン応答を送信します。

VMPS からアクセス拒否応答を受信した場合、スイッチはそのホスト MAC アドレスのトラフィック を双方向で引き続きブロックします。スイッチはポート宛のパケットを引き続きモニタし、新しいホス ト アドレスを検出すると VMPS にクエリーを送信します。VMPS からポートシャットダウン応答を受 信した場合、スイッチはそのポートをディセーブルにします。Network Assistant、CLI(コマンドライ ンインターフェイス)、または SNMP(簡易ネットワーク管理プロトコル)を使用して、ポートを手動 で再びイネーブルにする必要があります。

ダイナミックアクセス ポート VLAN メンバシップ

ダイナミックアクセス ポートが所属できるのは、VLAN ID が 1 ~ 4094 の 1 つの VLAN だけです。 リ ンクがアップになっても、VMPS によって VLAN が割り当てられるまで、このポートとの間でトラ フィック転送は行われません。VMPS は、ダイナミックアクセス ポートに接続した新しいホストの最 初のパケットから送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレ スを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。クライアント スイッチがまだ設定さ れていない場合は、スイッチは VMPS からトランク ポートで受信した最初の VTP パケットからのド メイン名を使用します。クライアント スイッチがすでに設定されている場合は、クエリー パケットに スイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。VMPS はパケット内のド メイン名が自身のドメイン名と一致することを確認したあと、要求を受け入れ、クライアントに割り当 てられた VLAN 番号を応答します。一致しない場合、(VMPS セキュア モードの設定に応じて) VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミックアクセス ポート上で複数のホスト(MAC アドレス)をアクティブにできますが、それら のホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数 が 20 を超えると、VMPS はダイナミックアクセス ポートをシャットダウンします。 ダイナミックアクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、 VLAN の所属から外れます。ポート経由でオンラインになるホストは VMPS によって VQP 経由で再 チェックされてから、ポートが VLAN に割り当てられます。

ダイナミックアクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。 スイッチ上のポートごとに、最大 20 の MAC アドレスを使用できます。ダイナミックアクセス ポート が一度に所属できる VLAN は 1 つだけですが、VLAN は検出された MAC アドレスに基づいてあとで 変更されることがあります。

VMPS クライアントのデフォルト設定

表 13-6 に、クライアント スイッチ上の VMPS およびダイナミック アクセス ポートのデフォルト設定 を示します。

表 13-6	VMPS クライアントおよびダイナミックアクセス ポートのデフォルト設定
--------	--------------------------------------

	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミックアクセス ポート VLAN メンバシップには、次の注意事項および制限事項があります。

- VMPS を設定してから、ポートをダイナミックアクセス ポートとして設定する必要があります。
- ポートをダイナミックアクセスポートとして設定すると、そのポートに対してスパニングツリーの PortFast 機能が自動的にイネーブルになります。PortFast モードにより、ポートをフォワーディングステートに移行させるプロセスが短縮されます。
- IEEE 802.1x ポートをダイナミックアクセス ポートとして設定することはできません。ダイナミックアクセス (VQP) ポートで IEEE 802.1x をイネーブルにしようとすると、エラーメッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。
- トランクポートをダイナミックアクセスポートにすることはできませんが、トランクポートに対して switchport access vlan dynamic インターフェイス コンフィギュレーション コマンドを入力することは可能です。その場合、スイッチの設定は維持され、あとにアクセスポートとして設定された場合には、その設定が適用されます。

ダイナミックアクセス設定を有効にするには、ポート上でトランキングをオフにしておく必要があ ります。

- ダイナミックアクセス ポートをモニタ ポートにすることはできません。
- セキュアポートをダイナミックアクセスポートにすることはできません。ポートをダイナミックにするには、ポート上でポートセキュリティをディセーブルにしておく必要があります。
- ダイナミックアクセス ポートを EtherChannel グループのメンバーにすることはできません。
- ポート チャネルをダイナミックアクセス ポートとして設定することはできません。

- VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。
- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。

VMPS クライアントの設定

ダイナミック VLAN を設定するには、VMPS(サーバ)を使用します。スイッチを VMPS クライアントにすることはできますが、VMPS サーバにすることはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。

(注)

スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

VMPS の IP アドレスを入力するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
vmps server <i>ipaddress</i> primary	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力 します。
vmps server ipaddress	(任意) セカンダリ VMPS サーバとして動作するスイッチの IP アドレ スを入力します。
	セカンダリ サーバのアドレスは、3 つまで入力できます。
nd	特権 EXEC モードに戻ります。
show vmps	表示された VMPS Domain Server フィールドの設定を確認します。
opy running-config tartup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



ダイナミックアクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。IP 接続が 可能かどうかをテストするには、VMPS の IP アドレスに ping を実行し、応答が得られるかどうかを確 認します。

VMPS クライアント上のダイナミックアクセス ポートの設定

クラスタ メンバー スイッチのポートをダイナミックアクセス ポートとして設定するには、最初に rcommand 特権 EXEC コマンドを使用して、そのクラスタ メンバー スイッチにログインします。

<u>/</u>]\ 注意

ダイナミックアクセス ポート VLAN メンバシップはエンド ステーション用、またはエンド ステー ションに接続されたハブ用です。他のスイッチにダイナミックアクセス ポートを接続すると、接続 が切断されることがあります。

VMPS クライアント スイッチにダイナミックアクセス ポートを設定するには、特権 EXEC モードで次 の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	エンド ステーションに接続するスイッチ ポートを指定し、イン ターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode access	ポートをアクセス モードにします。
ステップ 4	switchport access vlan dynamic	ポートをダイナミック VLAN メンバシップ適格として設定しま
		す。
		ダイナミックアクセス ポートは、エンド ステーションに接続され ている必要があります。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport	表示された Operational Mode フィールドの設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻すには、default interface *interface-id* インターフェイス コン フィギュレーション コマンドを使用します。インターフェイスをデフォルトのスイッチポート モード (dynamic auto) に戻すには、no switchport mode インターフェイス コンフィギュレーション コマン ドを使用します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、no switchport access vlan インターフェイス コンフィギュレーション コマンドを使用します。

VLAN メンバシップの再確認

スイッチが VMPS から受信したダイナミックアクセス ポート VLAN メンバシップの割り当てを確認 するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	vmps reconfirm	ダイナミックアクセス ポート VLAN メンバシップを再確認します。
ステップ 2	show vmps	ダイナミック VLAN の再確認ステータスを確認します。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信する VLAN メンバシップの情報を定期的に再確認します。再確認を実行する間隔は数字を使用して分単位で設定できます。

クラスタのメンバー スイッチを設定する場合、このパラメータはコマンド スイッチの再確認インター バルの設定値以上でなければなりません。メンバー スイッチにログインするには、最初に rcommand 特権 EXEC コマンドを使用する必要があります。

再確認インターバルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	vmps reconfirm minutes	ダイナミック VLAN メンバシップの再確認を行う間隔(分)を入力し ます。指定できる範囲は1~120です。デフォルト値は60分です。	
ステップ 3	end	特権 EXEC モードに戻ります。	
ステップ 4	show vmps	表示された <i>Reconfirm Interval</i> フィールドのダイナミック VLAN の再 確認ステータスを確認します。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

スイッチのデフォルト設定に戻すには、no vmps reconfirm グローバル コンフィギュレーション コマ ンドを使用します。

再試行回数の変更

スイッチが次のサーバにクエリーを送信する前に、VMPS との接続を試行する回数を変更するには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vmps retry count	再試行の回数を変更します。指定できる再試行回数の範囲は1~10で す。デフォルトは3です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vmps	表示された Server Retry Count フィールドの設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチのデフォルト設定に戻すには、no vmps retry グローバル コンフィギュレーション コマンド を使用します。

VMPS のモニタ

show vmps 特権 EXEC コマンドを使用して、VMPS に関する情報を表示できます。 スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP バージョン: VMPS との通信に使用する VQP のバージョン。スイッチは VQP バージョン1 を使用する VMPS にクエリーを送信します。
- 再確認インターバル:スイッチが VLAN と MAC アドレスの割り当てを再確認する間隔(分)
- サーバ再試行回数: VQP が VMPS にクエリーを再送信する回数。この回数すべてを試行しても応答が得られない場合、スイッチはセカンダリ VMPS へのクエリーを開始します。
- VMPS ドメイン サーバ:設定されている VLAN メンバシップ ポリシー サーバの IP アドレス。ス イッチは current と表示されているサーバにクエリーを送信します。primary と表示されている サーバは、プライマリ サーバです。
- VMPS 動作:最新の再確認の結果。再確認は、再確認インターバルが経過したときに自動的に行われますが、vmps reconfirm 特権 EXEC コマンドを入力するか、Network Assistant またはSNMP で同等の操作を行うことによって、強制的に再確認することもできます。

次に、show vmps 特権 EXEC コマンドの出力例を示します。

ダイナミックアクセス ポート VLAN メンバシップのトラブルシューティン グ

VMPS は次の状況でダイナミックアクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、なおかつホストのポートへの接続を許可しない場合。VMPS は ポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- ダイナミックアクセス ポート上のアクティブ ホストが 20 を超えた場合。

ディセーブルにされているダイナミックアクセス ポートを再びイネーブルにするには、shutdown イン ターフェイス コンフィギュレーション コマンドに続けて、no shutdown インターフェイス コンフィ ギュレーション コマンドを入力します。

VMPS の設定例

図 13-4 に、VMPS サーバ スイッチと、ダイナミック アクセス ポートを備えた VMPS クライアント ス イッチが含まれるネットワークの例を示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンドステーションはクライアント(スイッチB、スイッチI)に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。



図 13-4 ダイナミック ポート VLAN メンバシップの構成例

■ VMPS の設定


снартев 14

VTP の設定

この章では、Catalyst スイッチで、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) および VLAN データベースを使用して VLAN を管理する方法について説明します 2960。

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

この章で説明する内容は、次のとおりです。

- 「VTP の概要」(P.14-1)
- 「VTP の設定」(P.14-8)
- 「VTP のモニタ」 (P.14-18)

VTP の概要

VTP は、レイヤ2のメッセージプロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の 重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設 定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を 使用すると、1 台または複数のスイッチ上で中央集約的に設定変更を行い、その変更を自動的にネット ワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN 情報を他のスイッチに送信 することはできません。

VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境 で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のス イッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じ ます。

スイッチは 255 の VLAN をサポートしますが、設定済み機能の個数によって、スイッチ ハードウェア の使用が左右されます。VTP が新しい VLAN をスイッチに通知し、スイッチが使用可能な最大限の ハードウェア リソースをすでに使用している場合、スイッチはハードウェア リソース不足を伝える メッセージを送信して、VLAN をシャットダウンします。show vlan ユーザ EXEC コマンドの出力に、 サスペンド ステートの VLAN が示されます。



このスイッチは、LAN Lite イメージの実行中に最大 64 個の VLAN をサポートします。

VTP バージョン 1 およびバージョン 2 は、標準範囲の VLAN (VLAN ID 1 ~ 1005) だけをサポート します。Cisco IOS Release 12.2(52)SE 以降では VTP バージョン 3 をサポートします。VTP バージョ ン 3 は、VLAN 範囲全体 (VLAN 1 ~ 4094) をサポートします。拡張範囲 VLAN (VLAN 1006 ~ 4094) は、VTP バージョン 3 でだけサポートされます。拡張 VLAN がドメインに設定されている場合 は、VTP バージョン 3 から VTP バージョン 2 に変換できません。

(注)

VTP バージョン 3 をサポートするには、スイッチが LAN Base イメージを実行している必要があります。

ここでは、次の概要について説明します。

- 「VTP ドメイン」 (P.14-2)
- 「VTP モード」 (P.14-3)
- 「VTP アドバタイズ」(P.14-4)
- 「VTP バージョン 2」 (P.14-4)
- 「VTP バージョン 3」 (P.14-5)
- 「VTP プルーニング」 (P.14-6)

VTP ドメイン

VTP ドメイン (別名 VLAN 管理ドメイン) は、1 つのスイッチ、または同じ VTP ドメイン名を共有し て同一管理下にある相互接続された複数のスイッチで構成されます。スイッチは、1 つの VTP ドメイ ンにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。

デフォルトの設定では、トランクリンク(複数 VLAN のトラフィックを伝送するリンク)を介してド メインについてのアドバタイズを受信しないかぎり、またはユーザがドメイン名を設定しないかぎり、 スイッチは VTP 非管理ドメイン ステートです。管理ドメイン名を指定するか学習するまでは、VTP サーバ上で VLAN を作成または変更できません。また、VLAN 情報はネットワークを介して伝播され ません。

スイッチがトランク リンクを介して VTP アドバタイズを受信すると、スイッチは管理ドメイン名および VTP コンフィギュレーション リビジョン番号を継承します。そのあとスイッチは、別のドメイン名または古いコンフィギュレーション リビジョン番号が指定されたアドバタイズについては、すべて無視します。



VTP クライアント スイッチを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より *小さい*ことを確認してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーショ ンリビジョン番号が最大のスイッチの VLAN コンフィギュレーションを使用します。VTP ドメイ ン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバおよ び VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP コンフィギュレー ション リビジョン番号の確認手順およびリセット手順については、「VTP ドメインへの VTP クライ アント スイッチの追加」(P.14-17) を参照してください。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのスイッチに伝播さ れます。VTP アドバタイズは、IEEE 802.1Q を含め、すべての IEEE トランク接続に送信されます。 VTP は、複数の LAN タイプにわたり、固有の名前と内部インデックスの対応によって VLAN を動的 にマッピングします。このマッピングにより、ネットワーク管理者がデバイスを管理するための作業負 担が大幅に軽減されます。 VTP トランスペアレント モードでスイッチを設定した場合、VLAN の作成および変更は可能ですが、 その変更はドメイン内の他のスイッチには送信されません。また、変更が作用するのは、個々のスイッ チに限られます。ただし、スイッチがこのモードのときに設定を変更すると、変更内容がスイッチの実 行コンフィギュレーションに保存されます。この変更はスイッチのスタートアップ コンフィギュレー ション ファイルに保存することもできます。

ドメイン名およびパスワードの設定時の注意事項については、「VTP 設定時の注意事項」(P.14-8)を 参照してください。

VTP モード

サポート対象のスイッチを、表 14-1 に示す VTP モードのいずれかに設定できます。

表 14-1 VTP モード

VTP モード	説明
VTP サーバ	VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して 他のコンフィギュレーション パラメータ(VTP バージョンなど)を指定できます。VTP サーバは、 同一 VTP ドメイン内の他のスイッチに自身の VLAN 設定をアドバタイズし、トランク リンクを介し て受信したアドバタイズに基づいて、自身の VLAN 設定を他のスイッチと同期させます。
	VTP サーバ モードがデフォルトの設定です。
	(注) VTP サーバ モードでは、VLAN 設定は NVRAM に保存されます。スイッチがコンフィギュレーションを NVRAM に書き込んでいる間に障害を検出すると、VTP モードはサーバ モードからクライアント モードに自動的に移行します。この場合、スイッチは NVRAM が動作するまで VTP サーバ モードに戻ることができません。
VTP クライアント	VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信し ますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ド メインに含まれる、他のサーバ モードのスイッチで設定します。
	VTP バージョン 1 および 2 の VTP クライアント モードでは、VLAN 設定は NVRAM に保存されま せん。VTP バージョン 3 では、VLAN 設定はクライアント モードで NVRAM に保存されます。
VTP トランスペアレント	VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは自 身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期さ せることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転 送します。VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できま す。
	VTP バージョン1および2 では、拡張範囲 VLAN を作成するときは、スイッチを VTP トランスペアレント モードにする必要があります。VTP バージョン3 でも、クライアント モードまたはサーバモードでの拡張範囲 VLAN の作成をサポートしています。「拡張範囲 VLAN の設定」(P.13-11)を参照してください。
	スイッチが VTP トランスペアレント モードの場合、VTP および VLAN の設定は NVRAM に保存さ れますが、他のスイッチにはアドバタイズされません。このモードでは、VTP モードおよびドメイン 名はスイッチの実行コンフィギュレーションに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、copy running-config startup-config 特権 EXEC コマンドを使用します。
VTP オフ	VTP オフ モードでのスイッチの機能は、トランクを介して VTP アドバタイズを転送しないことを除 くと VTP トランスペアレント スイッチとしての機能と同じです。

VTP アドバタイズ

VTP ドメイン内の各スイッチは、専用のマルチキャスト アドレスに対して、それぞれのトランク ポートからグローバル コンフィギュレーション アドバタイズを定期的に送信します。このようなアドバタイズを受信した近接スイッチは、必要に応じて各自の VTP および VLAN 設定をアップデートします。

(注)

トランク ポートは VTP アドバタイズを送受信するので、スイッチ上で少なくとも1つのトランクポートが設定されており、そのトランク ポートが別のスイッチのトランク ポートに接続されていることを 確認する必要があります。そうでない場合、スイッチは VTP アドバタイズを受信できません。トラン クポートの詳細については「VLAN トランクの設定」(P.13-14)を参照してください。

VTP アドバタイズにより、次のグローバル ドメイン情報が配信されます。

- VTP ドメイン名
- VTP コンフィギュレーション リビジョン番号
- アップデート ID およびアップデート タイムスタンプ
- 各 VLAN の Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズを含む MD5 ダイ ジェスト VLAN コンフィギュレーション
- フレームフォーマット

VTP アドバタイズではさらに、設定されている各 VLAN について、次の VLAN 情報が配信されます。

- VLAN ID (ISL および IEEE 802.1Q)
- VLAN 名
- VLAN タイプ
- VLAN ステート
- VLAN タイプ固有のその他の VLAN 設定情報

VTP バージョン 3 では、VTP アドバタイズにはプライマリ サーバ ID、インスタンス番号、および開 始インデックスも含まれます。

VTP バージョン2

ネットワークで VTP を使用する場合、VTP のどのバージョンを使用するかを決定する必要がありま す。デフォルトでは、バージョン 1 の VTP が動作します。

VTP バージョン1でサポートされず、バージョン2でサポートされる機能は、次のとおりです。

- トークンリング サポート: VTP バージョン 2 は、Token Ring Bridge Relay Function (TrBRF; トークンリング ブリッジ リレー機能) および Token Ring Concentrator Relay Function (TrCRF; トークンリング コンセントレータ リレー機能) VLAN をサポートします。トークンリング VLAN の詳細については、「標準範囲 VLAN の設定」(P.13-5) を参照してください。
- 認識不能な Type-Length-Value (TLV)のサポート: VTP サーバまたは VTP クライアントは、 TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバモードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレントモード: VTP バージョン1の場合、VTP トランスペアレントスイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン2 がサポートするドメインは1つだけなので、VTP バージョン2 では、トランスペアレントモードの場合にはバージョンおよびドメイン名をチェックせずに、VTP メッセージを転送します。

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

・整合性検査: VTP バージョン2の場合、CLI (コマンドラインインターフェイス)、または SNMP (簡易ネットワーク管理プロトコル)を介して新しい情報が入力された場合に限り、VLAN 整合性 検査(VLAN 名、値など)を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージの MD5 ダイジェストが有効であれば、情報を受け入れます。

VTP バージョン3

VTP バージョン1または2でサポートされず、バージョン3でサポートされる機能は、次のとおりです。

- 拡張認証:認証を hidden または secret として設定できます。設定を hidden にしている場合、パスワード文字列からの秘密鍵は VLAN のデータベース ファイルに保存されますが、設定においてプレーン テキストで表示されることはありません。代わりに、パスワードに関連付けられている鍵が 16 進表記で実行コンフィギュレーションに保存されます。ドメインにテイクオーバー コマンドを入力するときは、パスワードを再入力する必要があります。キーワード secret を入力する場合、パスワードに秘密鍵を直接設定できます。
- 拡張範囲 VLAN (VLAN 1006 ~ 4094)のデータベース伝播のサポート。VTP バージョン1および2 で伝播する範囲は、VLAN 1 ~ 1005 だけです。拡張 VLAN を設定している場合は、VTP バージョン3 からバージョン1 または2 に変換できません。



VTP プルーニングは引き続き VLAN 1 ~ 1005 にだけ適用され、VLAN 1002 ~ 1005 は予約されたままで変更できません。

- プライベート VLAN のサポート。
- ドメインの任意のデータベースをサポートします。VTP 情報の伝播に加えて、バージョン3は Multiple Spanning Tree Protocol (MSTP) データベース情報を伝播できます。VTP プロトコルの 個別インスタンスが VTP を使用する各アプリケーションで実行されます。
- VTP プライマリ サーバと VTP セカンダリ サーバ。VTP プライマリ サーバは、データベース情報 をアップデートし、システムのすべての装置で受け入れられるアップデートを送信します。VTP セカンダリ サーバで実行できるのは、プライマリ サーバから NVRAM に受け取ったアップデート 済み VTP コンフィギュレーションのバックアップだけです。

デフォルトでは、すべての装置はセカンダリ サーバとしてアクティブになります。vtp primary 特権 EXEC コマンドを入力してプライマリ サーバを指定することができます。プライマリ サーバの ステータスは、管理者がドメインでテイクオーバー メッセージを発行する場合、データベースの アップデート用に必要となるだけです。プライマリ サーバがなくても VTP ドメインを動作させる ことはできます。プライマリ サーバのステータスは、スイッチにパスワードが設定されている場合でも、装置がリロードしたり、ドメインのパラメータが変更したりすると失われます。

トランク(ポート)単位で VTP をオンまたはオフにするオプション。[no] vtp インタフェイス コンフィギュレーション コマンドを使用すると、ポート単位で VTP をイネーブルまたはディセーブルにできます。トランク ポート上で VTP をディセーブルにすると、そのポートのすべての VTP インスタンスがディセーブルになります。VTP の設定を、MST データベースには off にする一方で、同じポートの VLAN データベースには on にすることはできません。

グローバルに VTP モードをオフに設定すると、システムのすべてのトランク ポートにこの設定が 適用されます。ただし、VTP インスタンス ベースでこのモードのオンまたはオフを指定すること はできます。たとえば、VLAN データベースには、スイッチを VTP サーバとして設定する一方 で、MST データベースには VTP を off に設定することができます。

■ VTP の概要

VTP プルーニング

VTP プルーニングを使用すると、トラフィックが宛先デバイスに到達するために使用しなければなら ないトランク リンクへのフラッディング トラフィックが制限されるので、使用可能なネットワーク帯 域幅が増えます。VTP プルーニングを使用しない場合、スイッチは受信側のスイッチで廃棄される可 能性があっても、VTP ドメイン内のすべてのトランク リンクに、ブロードキャスト、マルチキャスト、 および不明のユニキャスト トラフィックをフラッディングします。VTP プルーニングはデフォルトで ディセーブルです。

VTP プルーニングは、プルーニング適格リストに指定された VLAN トランク ポートへの不要なフラッ ディング トラフィックを阻止します。プルーニング適格リストに指定された VLAN だけが、プルーニ ングの対象になります。デフォルトでは、スイッチのトランク ポート上で VLAN 2 ~ 1001 がプルー ニング適格です。プルーニング不適格として設定した VLAN については、引き続きフラッディングが 行われます。VTP プルーニングはすべてのバージョンの VTP でサポートされます。

図 14-1 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ A のポート 1 およびスイッチ D のポート 2 は、Red という VLAN に割り当てられています。スイッチ A に接続されたホストからブロードキャストが送信された場合、スイッチ A は、このブロードキャスト をフラッディングします。Red VLAN にポートを持たないスイッチ C、E、F も含めて、ネットワーク 内のすべてのスイッチがこのブロードキャストを受信します。



図 14-1 VTP プルーニングを使用しない場合のフラッディング トラフィック

図 14-2 に、VTP プルーニングをイネーブルに設定したスイッチド ネットワークを示します。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されてい るリンク ポート (スイッチ B のポート 5、およびスイッチ D のポート 4) で、Red VLAN のトラ フィックがプルーニングされるからです。



図 14-2 VTP プルーニングによるフラッディング トラフィックの最適化

VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効にな ります。VLAN をプルーニング適格または不適格として設定する場合、影響を受けるのは、そのトラ ンク上の VLAN のプルーニングだけです(VTP ドメイン内のすべてのスイッチに影響するわけではあ りません)。

「VTP プルーニングのイネーブル化」(P.14-16)を参照してください。VTP プルーニングは、イネーブ ルにしてから数秒後に有効になります。VTP プルーニング不適格の VLAN からのトラフィックは、プ ルーニングの対象になりません。VLAN 1 および VLAN 1002 ~ 1005 は常にプルーニング不適格です。 これらの VLAN からのトラフィックはプルーニングできません。拡張範囲 VLAN (1005 を超える VLAN ID)もプルーニング不適格です。

VTP プルーニングは **VTP** トランスペアレント モードでは機能しないように設計されています。ネット ワーク内に **VTP** トランスペアレント モードのスイッチが 1 台または複数存在する場合は、次のいずれ かを実行する必要があります。

- ネットワーク全体の VTP プルーニングをオフにします。
- VTP トランスペアレント スイッチのアップストリーム側にあるスイッチのトランク上で、すべての VLAN をプルーニング不適格にすることによって、VTP プルーニングをオフにします。

インターフェイスに VTP プルーニングを設定するには、switchport trunk pruning vlan インターフェ イス コンフィギュレーション コマンドを使用します (「プルーニング適格リストの変更」(P.13-19) を 参照)。VTP プルーニングは、インターフェイスがトランキングを実行している場合に作用します。 VLAN プルーニングの適格性は、VTP ドメインで VTP プルーニングがイネーブルであるかどうか、特 定の VLAN が存在するかどうか、およびインターフェイスが現在トランキングを実行しているかどう かにかかわらず、設定できます。

VTP の設定

ここでは、次の設定情報について説明します。

- 「VTP のデフォルト設定」(P.14-8)
- 「VTP 設定時の注意事項」(P.14-8)
- 「VTP モードの設定」(P.14-11)
- 「VTP バージョンのイネーブル化」(P.14-14)
- 「VTP プルーニングのイネーブル化」(P.14-16)
- 「ポート単位の VTP の設定」(P.14-16)
- 「VTP ドメインへの VTP クライアント スイッチの追加」(P.14-17)

VTP のデフォルト設定

表 14-2 に、VTP のデフォルト設定を示します。

表 14-2 VTP のデフォルト設定

機能	デフォルト設定
VTP ドメイン名	ヌル
VTP モード (VTP バージョン 1 およびバー ジョン 2)	サーバ
VTPモード (VTPバージョン3)	このモードは、VTP バージョン 3 に変換する前のバー ジョン 1 または 2 のモードと同じです。
VTP バージョン	バージョン 1
MST データベース モード	トランスペアレント
VTP バージョン 3 のサーバ タイプ	セカンダリ
VTP パスワード	なし
VTP プルーニング	ディセーブル

VTP 設定時の注意事項

VTP パスワード、バージョン、VTP ファイル名、最新の VTP 情報を提供するインターフェイス、ド メイン名、およびモードを設定する場合、さらにプルーニングをディセーブルまたはイネーブルに設定 する場合には、vtp グローバル コンフィギュレーション コマンドを使用します。使用できるキーワー ドの詳細については、このリリースに対応するコマンド リファレンスに記載されているコマンドの説 明を参照してください。VTP 情報は VTP VLAN データベースに保存されます。VTP モードがトラン スペアレントである場合、VTP ドメイン名およびモードはスイッチの実行コンフィギュレーション ファイルにも保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイル に保存するには、copy running-config startup-config 特権 EXEC コマンドを入力します。スイッチを リセットした場合、VTP モードをトランスペアレントとして保存するには、このコマンドを使用する 必要があります。 スイッチのスタートアップ コンフィギュレーション ファイルに VTP 情報を保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップコンフィギュレーションおよび VLAN データベース内の VTP モードがトランス ペアレントであり、VLAN データベースとスタートアップコンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され(クリアされ)ます。スター トアップコンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップコンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベー スと一致しない場合、最初の 255 個の VLAN のドメイン名、VTP モード、および 設定には VLAN データベース情報が使用されます。

ドメイン名

VTP を初めて設定するときは、必ずドメイン名を割り当てる必要があります。また、VTP ドメイン内 のすべてのスイッチを、同じドメイン名で設定しなければなりません。VTP トランスペアレント モー ドのスイッチは、他のスイッチと VTP メッセージを交換しません。これらのスイッチについては VTP ドメイン名を設定する必要はありません。

(注)

NVRAM および DRAM の記憶域が十分にある場合は、VTP ドメイン内のすべてのスイッチを VTP サーバ モードにする必要があります。

注意

すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメインを設定しない でください。ドメインを設定すると、そのドメインの VLAN 設定を変更できなくなります。VTP ドメイン内の少なくとも1台のスイッチを VTP サーバ モードに設定してください。

パスワード

VTP ドメインのパスワードは設定できますが、必須ではありません。ドメインパスワードを設定する 場合は、すべてのドメインスイッチで同じパスワードを共有し、管理ドメイン内のスイッチごとにパ スワードを設定する必要があります。パスワードのないスイッチ、またはパスワードが不正なスイッチ は、VTP アドバタイズを拒否します。

ドメインに VTP パスワードを設定する場合、VTP 設定なしで起動したスイッチは、正しいパスワード を使用して設定しないかぎり、VTP アドバタイズを受信しません。設定後、スイッチは同じパスワー ドおよびドメイン名を使用した VTP アドバタイズを受信します。

VTP 機能を持つ既存のネットワークに新しいスイッチを追加した場合、その新しいスイッチに適切なパスワードを設定して初めて、スイッチはドメイン名を学習します。

注意

VTP ドメイン パスワードを設定したにもかかわらず、ドメイン内の各スイッチに管理ドメイン パ スワードを割り当てなかった場合には、管理ドメインが正常に動作しません。

VTP バージョン

実装する VTP バージョンを決定する場合は、次の注意事項に従ってください。

- VTP ドメイン内のすべてのスイッチは同じドメイン名を使用する必要がありますが、すべてが同じ VTP バージョンを実行する必要はありません。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 がディセーブルに設定されている場合、 VTP バージョン 2 対応スイッチは、VTP バージョン 1 を実行しているスイッチと同じ VTP ドメインで動作できます (デフォルトでは VTP バージョン 2 はディセーブルになっています)。
- VTP バージョン1を実行しているものの、VTP バージョン2に対応可能なスイッチが VTP バー ジョン3アドバタイズを受信すると、このスイッチは VTP バージョン2に自動的に移行します。
- VTP バージョン3を実行しているスイッチがVTP バージョン1を実行しているスイッチに接続すると、VTP バージョン1のスイッチはVTP バージョン2に移行し、VTP バージョン3のスイッチは、スケールダウンしたバージョンのVTP パケットを送信するため、VTP バージョン2スイッチは自身のデータベースをアップデートできます。
- VTP バージョン 3 を実行するスイッチは、拡張 VLAN を持つ場合はバージョン 1 または 2 に移行 できません。
- 同一VTPドメイン内のすべてのスイッチがバージョン2に対応可能な場合を除いて、スイッチ上でVTPバージョン2をイネーブルにしないでください。あるスイッチでバージョン2をイネーブルにすると、ドメイン内のすべてのバージョン2対応スイッチでバージョン2がイネーブルになります。バージョン1専用のスイッチがドメインに含まれている場合、そのスイッチはバージョン2対応スイッチとの間でVTP情報を交換できません。
- VTP バージョン1および2のスイッチはVTP バージョン3のアドバタイズを転送しないため、これらをネットワークエッジに配置することをお勧めします。
- 使用環境に TrBRF および TrCRF トークンリング ネットワークが含まれている場合に、トークン リング VLAN スイッチング機能を正しく動作させるには、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。トークンリングおよびトークンリング Net を実行する場合 は、VTP バージョン 2 をディセーブルにします。
- VTP バージョン1 およびバージョン2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094)の設定情報を 伝播しません。これらの VLAN は各装置で手動によって設定する必要があります。VTP バージョン3 は拡張範囲 VLAN をサポートします。拡張 VLAN を設定している場合、VTP バージョン3 から VTP バージョン2 に変換できません。
- VTP バージョン3装置のトランクポートがVTP バージョン2装置からのメッセージを受信した場合、この装置は、VLAN データベースをスケールダウンし、その特定のトランク上でVTP バージョン2フォーマットを使用して送信します。VTP バージョン3装置は、最初にそのトランクポートでVTP バージョン2パケットを受信しない限り、VTP バージョン2フォーマットのパケットを送信しません。
- VTP バージョン 3 装置が、あるトランク ポートで VTP バージョン 2 装置を検出した場合、両方の ネイバが同一トランク上で共存できるように、VTP バージョン 2 パケットだけでなく VTP バー ジョン 3 パケットの送信も継続します。
- VTP バージョン 3 装置は、VTP バージョン 2 またはバージョン 1 の装置からの設定情報は受け入 れません。
- VTP バージョン1またはバージョン2のリージョンで VTP バージョン3の2つの装置が通信に使用できるのはトランスペアレントモードだけです。
- VTP バージョン1にだけ対応する装置は、VTP バージョン3装置との相互運用はできません。

設定要件

VTP を設定する場合は、スイッチがドメイン内の他のスイッチと VTP アドバタイズを送受信できるように、トランク ポートを設定する必要があります。

詳細については、「VLAN トランクの設定」(P.13-14)を参照してください。

クラスタ メンバー スイッチの VTP を VLAN に設定する場合、rcommand 特権 EXEC コマンドを使 用して、そのメンバー スイッチにログインします。コマンドの詳細については、このリリースに対応 するコマンド リファレンスを参照してください。

VTP バージョン1および2では、スイッチに拡張範囲 VLAN を設定する場合、このスイッチは VTP トランスペアレント モードにする必要があります。VTP バージョン3でも、クライアント モードまた はサーバ モードでの拡張範囲 VLAN の作成をサポートしています。

VTP モードの設定

次のいずれかに VTP モードを設定できます。

- スイッチが VTP サーバ モードの場合には、VLAN 設定を変更し、その変更をネットワーク全体に 伝播できます。
- スイッチが VTP クライアントモードの場合には、そのスイッチの VLAN 設定を変更できません。 クライアント スイッチは、VTP ドメイン内の VTP サーバから VTP アップデート情報を受信し、 それに基づいて設定を変更します。
- スイッチを VTP トランスペアレント モードに設定すると、スイッチ上で VTP がディセーブルに なります。VTP トランスペアレント スイッチは VTP アップデートを送信せず、他のスイッチから 受信した VTP アップデートにも反応しません。ただし、VTP バージョン 2 が動作している VTP トランスペアレント スイッチでは、受信した VTP アドバタイズのトランク リンクに転送します。
- VTP オフモードは、VTP アドバタイズが転送されないことを除くと、VTP トランスペアレント モードと同じです。

次の注意事項に従ってください。

VTP バージョン1 およびバージョン2 では、拡張範囲 VLAN がスイッチ上に設定されている場合、VTP モードをクライアントまたはサーバに変更できません。エラーメッセージが表示され、設定が許可されません。VTP バージョン1 およびバージョン2 は、拡張範囲 VLAN (VLAN 1006 ~ 4094)の設定情報を伝播しません。これらの VLAN を各装置上に手動で設定する必要があります。



- (注) VTP バージョン1または2では、拡張範囲 VLAN (VLAN ID 1006~4094)を作成するには、 事前に vtp mode transparent グローバル コンフィギュレーション コマンドを使用して、VTP モードをトランスペアレントに設定する必要があります。VTP トランスペアレント モードで スイッチが起動するように、この設定をスタートアップ コンフィギュレーションに保存してく ださい。このようにしないと、スイッチのリセット時に拡張範囲 VLAN 設定が失われ、VTP サーバモード (デフォルト)で起動します。
- VTP バージョン 3 は拡張範囲 VLAN をサポートします。拡張 VLAN が設定されている場合は、 VTP バージョン 3 から VTP バージョン 2 に変換できません。

 スイッチを VTP クライアントモードに設定した場合、VLAN データベース ファイル (vlan.dat) は作成されません。そのままスイッチの電源をオフにすると、VTP 設定はデフォルトにリセット されます。スイッチが再起動されたあとも VTP 設定を VTP クライアントモードに維持するには、 VTP モードを設定する前に、VTP ドメイン名を設定する必要があります。

注意

すべてのスイッチが VTP クライアント モードで動作している場合は、VTP ドメイン名を設定しな いでください。ドメイン名を設定すると、そのドメインの VLAN 設定を変更できなくなります。し たがって、少なくとも1台のスイッチを VTP サーバとして設定してください。

VTP モードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vtp domain domain-name	VTP 管理ドメイン名を設定します。1~32 文字の名前を使用できま す。同一管理下にある VTP サーバ モードまたはクライアント モード のスイッチは、すべて同じドメイン名に設定する必要があります。
		サーバ モード以外にはこのコマンドは任意です。VTP サーバ モードに はドメイン名が必要です。スイッチで VTP ドメインにトランクを接続 している場合、スイッチはドメインの VTP サーバからドメイン名を学 習します。
		他の VTP パラメータを設定する前に、VTP ドメインを設定する必要が あります。
ステップ 3	vtp mode {client server transparent off} {vlan mst unknown}	スイッチを VTP モード(クライアント、サーバ、トランスペアレン ト、オフ)に設定します。
		(任意) データベースを次のように設定します。
		 vlan:何も設定されていない場合は VLAN データベースがデフォ ルトです。
		• mst:多重スパニング ツリー (MST) データベース。
		• unknown : データベース タイプは不明。
ステップ 4	vtp password password	(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用 できる文字数は 8 ~ 64 文字です。VTP パスワードを設定したにもかか わらず、ドメイン内の各スイッチに同じパスワードを割り当てなかっ た場合には、VTP ドメインが正常に動作しません。
		VTP バージョン 3 で使用可能なオプションについては、「VTP バー ジョン 3 のパスワードの設定」(P.14-13) を参照してください。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show vtp status	表示された VTP Operating Mode および VTP Domain Name フィールドの設定を確認します。
ステップ 7	copy running-config startup-config	(任意) スタートアップ コンフィギュレーション ファイルに設定を保 存します。
		 (注) スイッチの実行コンフィギュレーションに保存され、スタート アップ コンフィギュレーション ファイルにコピーできるのは、 VTP モードおよびドメイン名だけです。

設定したドメイン名は、削除できません。別のドメインにスイッチを再び割り当てるしかありません。

別のモードのスイッチを VTP サーバ モードに戻すには、no vtp mode グローバル コンフィギュレー ション コマンドを使用します。スイッチをパスワードがない状態に戻すには、no vtp password グロー バル コンフィギュレーション コマンドを使用します。

次に、ドメイン名が eng_group、パスワードが mypassword という VTP サーバとしてスイッチを設定 する例を示します。

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

VTP バージョン3のパスワードの設定

VTP バージョン3を使用する場合にパスワードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vtp password password [hidden secret]	(任意) VTP ドメイン用のパスワードを設定します。パスワードに使用 できる文字数は 8 ~ 64 文字です。
		 (任意) hidden:パスワード文字列から生成された秘密鍵が nvam:vlan.datファイルに保存されるようにするには、hidden を 入力します。VTP プライマリ サーバを設定してテイクオーバーを 設定しようとすると、パスワードの再入力を要求されます。
		 (任意) secret: パスワードを直接設定するには、secret を入力します。シークレットパスワードには 16 進数文字を 32 個含める必要があります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vtp password	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

パスワードをクリアするには、no vtp password グローバル コンフィギュレーション コマンドを入力 します。

次に、非表示のパスワードを設定方法とその表示方法の例を示します。

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

VTP バージョン3のプライマリ サーバの設定

VTP サーバを **VTP** プライマリ サーバ (バージョン 3 限定) として設定し、テイクオーバー操作を開始 するには、特権 **EXEC** モードの **VTP** サーバで次の手順を実行します。

	コマンド	目的
ステップ 1	vtp primary-server [vlan mst] [force]	スイッチの動作ステートをセカンダリ サーバ(デフォルト)からプラ イマリ サーバに変更し、その設定をドメインにアドバタイズします。 スイッチのパスワードが hidden に設定されている場合は、パスワード の再入力を要求されます。
		• (任意)vlan:テイクオーバー機能として VLAN データベースを 選択します。これがデフォルトです。
		 (任意) mst: テイクオーバー機能として Multiple Spanning Tree (MST; 多重スパニング ツリー) データベースを選択します。
		 (任意) force: force と入力すると、競合するサーバの設定が上書 きされます。force を入力しない場合、テイクオーバーの実行前に 確認を求められます。

次に、パスワードが非表示またはシークレットに設定されている場合に、VLAN データベースのプラ イマリ サーバ (デフォルト)としてスイッチを設定する方法の例を示します。

Do you want to continue (y/n) [n]? ${\boldsymbol{y}}$

VTP バージョンのイネーブル化

デフォルトで VTP バージョン 2 およびバージョン 3 はディセーブルになっています。



VTP バージョン 3 をサポートするには、スイッチが LAN Base イメージを実行している必要があります。

- あるスイッチ上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内の VTP バージョン 2 に対応可能なすべてのスイッチでバージョン 2 がイネーブルになります。VTP バージョン 3 をイ ネーブルにするには、各スイッチ上で手動によって設定する必要があります。
- VTP バージョン1および2では、VTP サーバまたはトランスペアレントモードのスイッチでだけ バージョンを設定できます。VTP バージョン3を実行するスイッチがクライアントモードの場合、 既存の拡張 VLAN や既存のプライベート VLAN がなく、パスワードが非表示に設定されていない ときであれば、バージョン2に変更できます。



同一 VTP ドメイン内のスイッチ上で、VTP バージョン 1 と VTP バージョン 2 は相互運用できません。VTP ドメイン内のすべてのスイッチが VTP バージョン 2 をサポートしている場合を除き、 VTP バージョン 2 をイネーブルにはしないでください。

- TrCRF および TrBRF トークンリング環境では、トークンリング VLAN スイッチング機能を正し く動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があり ます。トークンリングおよびトークンリング Net メディアの場合は、VTP バージョン 2 をディ セーブルにする必要があります。
- VTP バージョン 3 は、Cisco IOS Release 12.2(52) SE 以降でサポートされます。

注意

VTP バージョン 3 では、プライマリ サーバとセカンダリ サーバの両方がドメイン内の 1 つのイン スタンスに存在できます。

VTP バージョンを設定する場合の注意事項については、「VTP バージョン」(P.14-10) を参照してください。

VTP バージョンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vtp version {1 2 3}	スイッチで VTP バージョンをイネーブルにします。デフォルトは VTP バー ジョン 1 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vtp status	設定された VTP バージョンがイネーブルであることを確認します。
ステップ 5	copy running-config startup-config	(任意) スタートアップ コンフィギュレーション ファイルに設定を保存します。

デフォルトの VTP バージョン 1 に戻るには、no vtp version グローバル コンフィギュレーション コマ ンドを使用します。

VTP プルーニングのイネーブル化

プルーニングは、トラフィックが宛先デバイスに到達するために使用しなければならないトランク リ ンクだけにフラッディング トラフィックを制限することによって、使用可能な帯域幅を増やします。 VTP プルーニングをイネーブルにできるのは、スイッチが VTP サーバ モードの場合だけです。

VTP ドメイン内で VTP プルーニングをイネーブルにするには、特権 EXEC モードで次の手順を実行 します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vtp pruning	VTP 管理ドメインでプルーニングをイネーブルにします。
		プルーニングは、デフォルトではディセーブルに設定されています。VTP サーバモードの1台のスイッチ上に限ってプルーニングをイネーブルにする 必要があります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vtp status	表示された VTP Pruning Mode フィールドの設定を確認します。

VTP プルーニングをディセーブルにするには、no vtp pruning グローバル コンフィギュレーション コ マンドを使用します。

VTP バージョン1および2 では、VTP サーバでプルーニングをイネーブルにすると、その VTP ドメ イン全体でプルーニングがイネーブルになります。VTP バージョン3 では、ドメイン内の各スイッチ 上で手動によってプルーニングをイネーブルにする必要があります。

プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。デフォルトで は、トランク ポート上で VLAN 2 ~ 1001 がプルーニング適格です。専用の VLAN および拡張範囲 VLAN をプルーニングすることはできません。プルーニング適格の VLAN を変更する手順について は、「プルーニング適格リストの変更」(P.13-19) を参照してください。

ポート単位の VTP の設定

VTP バージョン 3 では、ポート単位で VTP をイネーブルまたはディセーブルにできます。VTP は、ト ランク モードのポート上でだけイネーブルにできます。VTP トラフィックの着信または発信はブロッ クされ、転送されません。

ポート上で VTP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	vtp	指定されたポート上で VTP をイネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface <i>interface-id</i>	ポートの変更を確認します。
ステップ 6	show vtp status	設定を確認します。

インターフェイス上で VTP をディセーブルにするには、no vtp インターフェイス コンフィギュレー ション コマンドを使用します。

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# vtp
Switch(config-if)# end

VTP ドメインへの VTP クライアント スイッチの追加

VTP クライアントを VTP ドメインに追加する前に、必ず VTP コンフィギュレーション リビジョン番号が VTP ドメイン内の他のスイッチのコンフィギュレーション リビジョン番号より 小さいことを確認 してください。VTP ドメイン内のスイッチは常に、VTP コンフィギュレーション リビジョン番号が最 大のスイッチの VLAN コンフィギュレーションを使用します。VTP バージョン 1 および 2 では、VTP ドメイン内のリビジョン番号よりも大きなリビジョン番号を持つスイッチを追加すると、VTP サーバ および VTP ドメインからすべての VLAN 情報が消去される場合があります。VTP バージョン 3 では、 VLAN 情報が消去されることはありません。

VTP ドメインに追加する*前に、*スイッチ上で VTP コンフィギュレーション リビジョン番号を確認およ びリセットするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	show vtp status	VTP コンフィギュレーション リビジョン番号をチェックします。
		番号が 0 の場合は、スイッチを VTP ドメインに追加します。
		番号が0より大きい場合は、次の手順に従います。
		a. ドメイン名を書き留めます。
		b. コンフィギュレーション リビジョン番号を書き留めます。
		C. 次のステップに進んで、スイッチのコンフィギュレーション リビジョン番号をリセットします。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vtp domain domain-name	ドメイン名を、ステップ1で表示された元の名前から新しい名前に変更します。
ステップ 4	end	スイッチの VLAN 情報が更新され、コンフィギュレーション リビジョン番号 が 0 にリセットされます。特権 EXEC モードに戻ります。
ステップ 5	show vtp status	コンフィギュレーション リビジョン番号が 0 にリセットされていることを確認 します。
ステップ 6	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 7	vtp domain domain-name	スイッチの元のドメイン名を入力します。
ステップ 8	end	スイッチの VLAN 情報が更新されて、特権 EXEC モードに戻ります。
ステップ 9	show vtp status	(任意)ドメイン名がステップ1のものと同じであり、コンフィギュレーション リビジョン番号が0であることを確認します。

コンフィギュレーション リビジョン番号をリセットしたあとに、スイッチを VTP ドメインに追加します。

<u>》</u> (注)

スイッチ上で VTP をディセーブルにし、VTP ドメイン内の他のスイッチに影響を与えることなく VLAN 情報を変更するには、vtp mode transparent グローバル コンフィギュレーション コマンドを使 用します。

VTP のモニタ

VTP の設定情報(ドメイン名、現在の VTP バージョン、VLAN 数)を表示することによって、VTP をモニタします。スイッチで送受信されたアドバタイズに関する統計情報を表示することもできます。 表 14-3 に、VTP アクティビティをモニタするための特権 EXEC コマンドを示します。

丰	11-3	VTD エータ	コマンド
衣	14-3	VIP T-2	コマント

コマンド	目的
show vtp counters	送受信された VTP メッセージに関するカウンタを表示します。
show vtp devices [conflict]	ドメイン内のすべての VTP バージョン 3 の装置の情報を表示します。 プライマリ サーバと競合する VTP バージョン 3 の装置が表示されま す。スイッチがトランスペアレント モードまたはオフ モードの場合、 show vtp devices コマンドで情報は表示されません。
show vtp interface [<i>interface-id</i>]	すべてのインターフェイスまたは指定したインターフェイスに関する VTP ステータスおよび設定情報を表示します。
show vtp password	VTP パスワードを表示します。表示されるパスワードの形式は、 hidden キーワードが入力されているか、または、暗号化がスイッチで イネーブル化されているかどうかによって異なります。
show vtp status	VTP スイッチの設定情報を表示します。



снарте 15

音声 VLAN の設定

この章では、Catalyst 2960 スイッチで音声 VLAN 機能を設定する方法について説明します。Catalyst 6500 ファミリー スイッチの一部のマニュアルでは、音声 VLAN を 補助 VLAN と表しています。

(注)

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

この章で説明する内容は、次のとおりです。

- 「音声 VLAN の概要」(P.15-1)
- 「音声 VLAN の設定」(P.15-3)
- 「音声 VLAN の表示」(P.15-8)

音声 VLAN の概要

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できま す。スイッチを Cisco 7960 IP Phone に接続すると、IP Phone はレイヤ 3 IP precedence およびレイヤ 2 Class of Service (CoS; サービス クラス) 値を使用して、音声トラフィックを送信します。どちらの 値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下す ることがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service (QoS) をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからの ネットワーク トラフィックを予測可能な方法で送信します。QoS の詳細については、第 33 章 「QoS の設定」を参照してください。

Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

Cisco IP Phone には、3 ポートの 10/100 スイッチが統合されています。図 15-1 を参照してください。 これらのポートは、次のデバイスへの接続専用です。

- ポート1は、スイッチまたは他の Voice over IP (VoIP) デバイスに接続します。
- ポート2は、IP Phoneのトラフィックを伝送する内部 10/100 インターフェイスです。
- ポート3(アクセスポート)は、PCまたは他のデバイスに接続します。

図 15-1 に、Cisco7960 IP Phone の接続方法の例を示します。



図 15-1 スイッチに接続された Cisco7960 IP Phone

Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定 できます。スイッチ上のアクセス ポートを設定して、Cisco Discovery Protocol (CDP) パケットを送 信させることができます。CDP には、接続する IP Phone に対して、次のいずれかの方法でスイッチに 音声トラフィックを送信するように指定します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし(レイヤ 2 CoS プライオリティ値なし)のアクセス VLAN による送信



いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値(音声トラフィックはデフォルトで 5、音声制御トラフィックは 3)を伝送します。

Cisco IP Phone のデータ トラフィック

スイッチは、Cisco IP Phone のアクセス ポートに接続されたデバイス(図 15-1を参照)から送られた、タグ付きデータトラフィック(IEEE 802.1Q または IEEE 802.1p フレーム タイプのトラフィック)を処理することもできます。スイッチ上のレイヤ 2 アクセス ポートが、CDP パケットを送信するように設定できます。CDP は、接続する IP Phone に、次のいずれかのモードで IP Phone 上のアクセスポートを設定するように指定します。

- trusted (信頼性がある) モードでは、Cisco IP Phone のアクセス ポート経由で受信したすべての トラフィックがそのまま IP Phone を通過します。
- untrusted (信頼性がない) モードでは、Cisco IP Phone のアクセス ポート経由で受信した IEEE 802.1Q および IEEE 802.1p フレームのすべてのトラフィックに、設定されたレイヤ 2 CoS 値を与 えます。デフォルトのレイヤ 2 CoS 値は 0 です。untrusted モードがデフォルトの設定です。

(注)

Cisco IP Phone に接続されたデバイスからのタグなしトラフィックは、IP Phone のアクセス ポートの 信頼状態に関係なく、そのまま IP Phone を通過します。

音声 VLAN の設定

ここでは、次の設定情報について説明します。

- 「音声 VLAN のデフォルト設定」(P.15-3)
- 「音声 VLAN 設定時の注意事項」(P.15-4)
- 「Cisco7960 IP Phone に接続するポートの設定」(P.15-5)

音声 VLAN のデフォルト設定

音声 VLAN 機能は、デフォルトではディセーブルに設定されています。

音声 VLAN 機能がイネーブルの場合、すべてのタグなしトラフィックはポートのデフォルトの CoS プ ライオリティに従って送信されます。

IEEE 802.1p または IEEE 802.1Q のタグ付きトラフィックでは、CoS 値が信頼されません。

音声 VLAN 設定時の注意事項

音声 VLAN の設定時の注意事項を次に示します。

 音声 VLAN 設定はスイッチのアクセス ポートだけでサポートされており、トランク ポートではサ ポートされていません。

(注)

- トランク ポートは、標準 VLAN と同様に、任意の数の音声 VLAN を伝送できます。音声 VLAN の設定は、トランク ポートでは不要です。
- IP Phone での通信が適切に行えるように、音声 VLAN はスイッチ上でアクティブになっている必要があります。VLAN が存在しているかどうかを確認するには、show vlan 特権 EXEC コマンドを使用します (リストで表示されます)。VLAN がリストになかった場合、音声 VLAN の作成方法について、第13章「VLAN の設定」を参照してください。
- Power Over Ethernet (PoE) スイッチは、シスコ先行標準の受電装置または IEEE 802.3af 準拠の 受電装置が AC 電源から電力を供給されてない場合に、それらの受電装置に自動的に電力を供給で きます。PoE インターフェイスの詳細については、「PoE ポートの電力管理モードの設定」 (P.11-24) を参照してください。
- 音声 VLAN をイネーブルにする前に、mls qos グローバル コンフィギュレーション コマンドを入 力してスイッチ上で QoS をイネーブルに設定し、さらに mls qos trust cos インターフェイス コン フィギュレーション コマンドを入力してポートの信頼状態を trust に設定しておくことを推奨しま す。Auto-QoS 機能を使用すると、これらは自動的に設定されます。詳細は、第 33 章「QoS の設 定」を参照してください。
- IP Phone にコンフィギュレーションを送信するために、Cisco IP Phone に接続するスイッチ ポート上で CDP をイネーブルにする必要があります (デフォルト設定では、CDP がすべてのスイッチインターフェイスでグローバルにイネーブルです)。
- 音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディ セーブルにしても、PortFast 機能は自動的にディセーブルになりません。
- Cisco IP Phone とその IP Phone に接続されたデバイスが同じ VLAN 上にある場合、両方とも同じ IP サブネットに属していなければなりません。次の条件が満たされている場合は、同じ VLAN 上 にあります。
 - 両方とも IEEE 802.1p またはタグなしフレームを使用する。
 - Cisco IP Phone が IEEE 802.1p フレームを使用し、デバイスがタグなしフレームを使用する。
 - Cisco IP Phone がタグなしフレームを使用し、デバイスが IEEE 802.1p フレームを使用する。
 - Cisco IP Phone が IEEE 802.1Q フレームを使用し、音声 VLAN がアクセス VLAN と同じである。
- Cisco IP Phone と IP Phone に接続されたデバイスは、同一 VLAN、同一サブネット上にあっても、 使用するフレーム タイプが異なる場合は通信できません。トラフィックは同一サブネット上で ルーティングされないからです(ルーティングによってフレーム タイプの相違が排除されます)。
- 音声 VLAN では、スタティック セキュア MAC(メディア アクセス制御)アドレスを設定できま せん。
- 音声 VLAN ポートには次のポート タイプがあります。
 - ダイナミックアクセスポート。詳細については、「VMPS クライアント上のダイナミックアクセスポートの設定」(P.13-28)を参照してください。
 - IEEE 802.1x 認証ポート。詳細については、「802.1x 準備状態チェックの設定」(P.9-38)を参照してください。



Cisco7960 IP Phone に接続するポートの設定

Cisco7960 IP Phone は、PC または他のデバイスとの接続もサポートしているので、スイッチを Cisco IP Phone に接続するポートは、さまざまな種類のトラフィックを伝送できます。ポートを設定することによって、Cisco IP Phone による音声トラフィックおよびデータ トラフィックの伝送方法を決定できます。

ここでは、次の設定情報について説明します。

- 「Cisco IP Phone の音声トラフィックの設定」(P.15-6)
- 「着信データフレームのプライオリティ設定」(P.15-7)

Cisco IP Phone の音声トラフィックの設定

Cisco IP Phone に CDP パケットを送信して IP Phone による音声トラフィックの送信方法を設定するように、IP Phone に接続するポートを設定できます。IP Phone は指定された音声 VLAN に、レイヤ 2 CoS 値を使用して、IEEE 802.1Q フレームの音声トラフィックを伝送できます。IEEE 802.1p のプライオリティ タグを使用すると、音声トラフィックにさらに高いプライオリティを与え、すべての音声トラフィックをネイティブ(アクセス)VLAN 経由で転送できます。Cisco IP Phone はタグなしの音声トラフィックを送信する、または独自の設定を使用してアクセス VLAN で音声トラフィックを送信することもできます。いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値(デフォルトは5)を伝送します。

ポート上で音声トラフィックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	IP Phoneに接続するインターフェイスを指定し、インターフェイス コ ンフィギュレーション モードを開始します。	
ステップ 3	mls qos trust cos	パケットの CoS 値を使用して着信するトラフィック パケットを分類す るように、インターフェイスを設定します。タグなしパケットの場合、 ポートのデフォルト CoS 値が使用されます。	
		(注) ポートの信頼状態を設定する前に、mls qos グローバル コン フィギュレーション コマンドを使用することによって、QoS を グローバルでイネーブルに設定しておく必要があります。	
ステップ 4	switchport voice vlan {vlan-id	Cisco IP Phone による音声トラフィックの伝送方法を設定します。	
	dot1p none untagged}}	 vlan-id: すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。有効な VLAN ID は 1 ~ 4094 です。 	
		 dot1p:音声トラフィックに IEEE 802.1p プライオリティ タギング を使用し、デフォルトのネイティブ VLAN (VLAN 0)を使用して すべてのトラフィックが伝送されるように、IP Phone を設定しま す。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリ ティ 5 を使用して音声トラフィックを転送します。 	
		 none: IP Phone が独自の設定を使用してタグなしの音声トラフィックを送信するようにします。 	
		 untagged:タグなしの音声トラフィックを送信するように IP Phone を設定します。 	
ステップ 5	end	特権 EXEC モードに戻ります。	
ステップ 6	show interfaces interface-id switchport または	音声 VLAN の設定を確認します。	
	show running-config interface interface-id	QoS および音声 VLAN の設定を確認します。	
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。	

次に、Cisco IP Phone に接続しているポートを設定する例を示します。ポートは、CoS 値を使用して着 信トラフィックを分類し、音声トラフィック用に IEEE 802.1p プライオリティ タギングを使用し、デ フォルトのネイティブ VLAN (VLAN 0)を使用してすべてのトラフィックを伝送するように設定しま す。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet0/1 Switch(config-if)# mls qos trust cos Switch(config-if)# switchport voice vlan dot1p Switch(config-if)# end

着信データ フレームのプライオリティ設定

(注)

着信データ フレームのプライオリティを設定するには、スイッチが LAN Base イメージを実行してい る必要があります。

PC またはその他のデータ デバイスを Cisco IP Phone ポートに接続できます。タグ付きデータ トラ フィック(IEEE 802.1Q または IEEE 802.1p フレーム)を処理するために、スイッチが CDP パケット を送信するように設定できます。CDP は、Cisco IP Phone に、IP Phone 上のアクセス ポートに接続さ れたデバイスからのデータ パケットをどのように送信するかを指定します。PC は、CoS 値が割り当て られたパケットを生成できます。接続デバイスから IP Phone のポートに届いたフレームのプライオリ ティを変更しない(信頼する)または変更する(信頼しない)ように、IP Phone を設定できます。

Cisco IP Phone の非音声ポートから受信したデータ トラフィックのプライオリティを設定するには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的							
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。							
ステップ 2	interface interface-id	Cisco IP Phone に接続するインターフェイスを指定し、インターフェイ ス コンフィギュレーション モードを開始します。							
ステップ 3	<pre>switchport priority extend {cos value trust}</pre>	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプ ライオリティを設定します。							
		 cos value : PC または接続しているデバイスから受信したプライオリティを指定の CoS 値に変更するように、IP Phone を設定します。値は0~7です。7が最高のプライオリティです。デフォルトのプライオリティは cos 0 です。 							
		 trust: PC または接続しているデバイスから受信したプライオリ ティを信頼するように IP Phone のアクセス ポートを設定します。 							
ステップ 4	end	特権 EXEC モードに戻ります。							
ステップ 5	show interfaces interface-id switchport	設定を確認します。							
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。							

ポートをデフォルト設定に戻すには、no switchport voice vlan インターフェイス コンフィギュレー ション コマンドを使用します。

次に、Cisco IP Phone に接続しているポートを設定して、PC または接続しているデバイスから受信するフレームのプライオリティを変更しないようにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

```
ポートをデフォルト設定に戻すには、no switchport priority extend インターフェイス コンフィギュ
レーション コマンドを使用します。
```

音声 VLAN の表示

インターフェイスの音声 VLAN 設定を表示するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを使用します。



снарте 16

STP の設定

この章では、Catalyst 2960 スイッチのポートベース VLAN 上で Spanning Tree Protocol (STP; スパニ ング ツリー プロトコル)を設定する方法について説明します。このスイッチは、IEEE 802.1D 標準に 準拠した Per-VLAN Spanning-Tree plus (PVST+) とシスコ独自の拡張機能の組み合わせか、もしく は IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) プロトコルの いずれかを使用できます。

Multiple Spanning-Tree Protocol (MSTP) および複数の VLAN を同一のスパニング ツリー インスタ ンスにマッピングする方法については、第 17 章「MSTP の設定」を参照してください。PortFast、 UplinkFast、ルート ガードなどのその他のスパニング ツリーの機能については、第 18 章「オプション のスパニング ツリー機能の設定」を参照してください。



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

この章で説明する内容は、次のとおりです。

- 「スパニング ツリー機能の概要」(P.16-2)
- 「スパニング ツリー機能の設定」(P.16-13)
- 「スパニング ツリー ステータスの表示」(P.16-25)

スパニング ツリー機能の概要

ここでは、次の概要について説明します。

- 「STP の概要」(P.16-2)
- 「スパニング ツリー トポロジと BPDU」(P.16-3)
- 「ブリッジ ID、スイッチ プライオリティ、および拡張システム ID」(P.16-4)
- 「スパニング ツリー インターフェイス ステート」(P.16-5)
- 「スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み」(P.16-8)
- 「スパニング ツリーおよび冗長接続」(P.16-9)
- 「スパニング ツリー アドレスの管理」(P.16-10)
- 「接続を維持するためのエージングタイムの短縮」(P.16-10)
- 「スパニング ツリー モードおよびプロトコル」(P.16-10)
- 「サポートされるスパニング ツリー インスタンス」(P.16-11)
- 「スパニング ツリーの相互運用性と下位互換性」(P.16-12)
- 「STP および IEEE 802.1Q トランク」(P.16-12)

設定情報については、「スパニング ツリー機能の設定」(P.16-13)を参照してください。

オプションのスパニング ツリー機能については、第18章「オプションのスパニング ツリー機能の設 定」を参照してください。

STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ2リンク管理プロ トコルです。レイヤ2イーサネットネットワークを正しく動作させるには、2つのステーション間に存 在するアクティブパスは1つでなければなりません。エンドステーション間に複数のアクティブパス があると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドス テーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ2イン ターフェイスのエンドステーション MAC(メディアアクセス制御)アドレスを学習する可能性がで てきます。このような条件が発生すると、不安定なネットワークになります。スパニング ツリーの動 作は透過的であり、エンドステーション側で、単一 LAN セグメントに接続されているのか、複数セグ メントからなるスイッチド LAN に接続されているのかを検出することはできません。

STP は、スパニング ツリー アルゴリズムを使用し、スパニング ツリーのルートとして冗長接続ネット ワーク内のスイッチを1つ選択します。スパニング ツリー アルゴリズムは、アクティブ トポロジでの ポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ2ネットワーク 上で最良のループフリー パスを算出します。

- ルート:スパニング ツリー トポロジに対して選定される転送ポート
- 指定:各スイッチド LAN セグメントに対して選定される転送ポート
- 代替:スパニング ツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ:ループバック コンフィギュレーションのブロック ポート

*すべての*ポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッ チはルート スイッチです。少なくとも *1 つの*ポートに役割が指定されているスイッチは、指定スイッ チを意味します。 冗長データパスはスパニングツリーによって、強制的にスタンバイ(ブロックされた)ステートにされます。スパニングツリーのネットワークセグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリートポロジを再計算し、スタンバイパスをアクティブにします。スイッチは、定期的に Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット)と呼ばれるスパニングツリーフレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリーパスを構築します。BPDUには、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチプライオリティ、ポートプライオリティ、パスコストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチドネットワーク用のルートスイッチおよびルートポートを選定し、さらに、各スイッチドセグメントのルートポートおよび指定ポートを選定します。

スイッチの2つのポートがループの一部になっている場合、スパニング ツリー ポート プライオリティ とパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブ ロッキング ステートにするかが制御されます。スパニング ツリー ポート プライオリティ値は、ネット ワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ 適切であるかを表します。パス コストの値は、メディアの速度を表します。



デフォルトでは、Small Form-factor Pluggable (SFP) を搭載していないインターフェイスにだけ、ス イッチがキープアライブ メッセージを (接続が有効か確認するために) 送信します。[no] keepalive イ ンターフェイス コンフィギュレーション コマンドを使用してインターフェイスのデフォルトを変更す ることができます。

スパニング ツリー トポロジと BPDU

スイッチド ネットワーク内の安定したアクティブ スパニング ツリー トポロジは、次の要素によって制 御されます。

- 各スイッチのそれぞれの VLAN に対応付けられた一意のブリッジ ID (スイッチ プライオリティお よび MAC アドレス)
- ルートスイッチに対するスパニング ツリー パス コスト
- 各レイヤ2インターフェイスに対応付けられたポート ID (ポート プライオリティおよび MAC アドレス)

ネットワーク内のスイッチに電源が投入されると、それぞれがルート スイッチとして機能します。各 スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって 通信が行われ、スパニング ツリー トポロジが計算されます。各コンフィギュレーション BPDU には、 次の情報が含まれます。

- 送信側スイッチがルートスイッチと見なしたスイッチの固有ブリッジ ID
- ルートに対するスパニング ツリー パス コスト
- 送信側スイッチのブリッジ ID
- メッセージの有効期間
- 送信側インターフェイス ID
- Hello タイマー、転送遅延タイマー、および最大エージング プロトコル タイマーの値

スイッチは、*優位の*情報(より小さいブリッジ ID、より低いパス コストなど)を格納したコンフィ ギュレーション BPDU を受信すると、そのポートのためにこの情報を保存します。スイッチは、この BPDU をルート ポートで受信した場合は、更新されたメッセージ付きで、自身が指定スイッチである すべての接続 LAN に対して BPDU を転送します。 そのポートに対して現在保存されているものより *下位*の情報を格納したコンフィギュレーション BPDU を受信した場合は、BPDU は廃棄されます。スイッチが、下位 BPDU の送信元の LAN の指定 スイッチである場合は、そのポート用に保存された最新情報を格納した BPDU をその LAN に送信しま す。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

 ネットワーク内の1台のスイッチがルートスイッチ(スイッチドネットワークのスパニングツ リートポロジの論理的な中心)として選択されます。

各 VLAN で、スイッチのプライオリティが最も高い(プライオリティ値が数値的に最も小さい) スイッチがルート スイッチとして選定されます。すべてのスイッチがデフォルトのプライオリ ティ(32768)で設定されている場合は、VLAN 内で最小の MAC アドレスを持つスイッチがルー トスイッチになります。スイッチのプライオリティ値は、ブリッジ ID の最上位ビットを占めます (表 16-1 (P.16-4)を参照)。

- 各スイッチ(ルートスイッチを除く)に対して1つのルートポートが選択されます。このポートは、スイッチによってパケットがルートスイッチに転送されるときに、最適なパス(最小コスト)を提供します。
- スイッチごとに、パス コストに基づいてルート スイッチまでの最短距離が計算されます。
- 各LAN セグメントの指定スイッチが選定されます。指定スイッチでは、LAN からルート スイッ チへのパケット転送の場合、パスコストが最小となります。指定スイッチが LAN に接続するポー トのことを指定ポートと呼びます。

スイッチド ネットワーク上のすべての地点からルート スイッチに到達する場合に必要のないパスはす べて、スパニング ツリー ブロッキング モードになります。

ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチに一意のブリッジ識別子(ブリッジ ID)を設定する必要がありま す。この ID によってルート スイッチの選択が制御されます。各 VLAN は PVST+ と Rapid PVST+ に よって異なる *論理ブリッジ*と見なされるので、同一のスイッチは設定された各 VLAN とは異なるブ リッジ ID を保有している必要があります。スイッチ上の各 VLAN には一意の 8 バイト ブリッジ ID が 設定されます。上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトがスイッチの MAC アドレスから取得されます。

スイッチでは IEEE 802.1t スパニング ツリー拡張機能がサポートされ、従来はスイッチ プライオリ ティに使用されていたビットの一部が VLAN ID として使用されるようになりました。その結果、ス イッチに割り当てられる MAC アドレスが少なくなり、より広い範囲の VLAN ID をサポートできるよ うになり、しかもブリッジ ID の一意性を損なうこともありません。表 16-1 に示すように、従来はス イッチ プライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張 システム ID 値(VLAN ID と同じ)に割り当てられています。

表 16-1 スイッチ プライオリティ値および拡張システム ID

スイッチ プライオリティ値			拡張システム ID(VLAN ID と同じに設定)												
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニング ツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、スイッチ プ ライオリティ、および割り当てられたスパニング ツリー MAC アドレスを使用します。 拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN の スイッチ プライオリティを手動で設定する方法に影響が生じます。たとえば、スイッチのプライオリ ティ値を変更すると、ルート スイッチとして選定される可能性も変更されることになります。大きい 値を設定すると可能性が低下し、値が小さいと可能性が増大します。詳細については、「ルート スイッ チの設定」(P.16-16)、「セカンダリ ルート スイッチの設定」(P.16-18)、および「VLAN のスイッチ プライオリティの設定」(P.16-21)を参照してください。

スパニング ツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するときに、伝播遅延が生じる可能性があります。その結果、スイッチド ネットワークのさまざまな場所で、さまざまな時期に、トポロジの変更が起こる可能 性があります。インターフェイスがスパニング ツリー トポロジに含まれていない状態からフォワー ディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インター フェイスは新しいトポロジ情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始す る必要があります。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレー ム存続時間を満了させることも必要です。

スパニング ツリーを使用しているスイッチの各レイヤ2インターフェイスは、次のいずれかのステートになります。

- ブロッキング:インターフェイスはフレーム転送に関与しません。
- リスニング:インターフェイスをフレーム転送に関与させることをスパニングツリーが決定した 場合、ブロッキングステートから最初に移行するステートです。
- ラーニング:インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング:インターフェイスはフレームを転送します。
- ディセーブル:インターフェイスはスパニング ツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニング ツリー インスタンスが稼動していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 16-1 に、インターフェイスがステートをどのように移行するかを示します。

図 16-1 スパニング ツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニング ツリーがイネーブルになります。その後、ス イッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよび ラーニングという移行ステートを通過します。スパニング ツリーは、フォワーディング ステートまた はブロッキング ステートで各インターフェイスを安定させます。

スパニング ツリー アルゴリズムがレイヤ2インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

- スパニング ツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待 つ間、インターフェイスはリスニング ステートになります。
- スパニング ツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに 移行させ、転送遅延タイマーをリセットします。
- **3.** ラーニングステートで、スイッチがデータベース転送のためにエンドステーションの位置情報を 学習している間、インターフェイスはフレーム転送を引き続きブロックします。
- **4.** 転送遅延タイマーが満了すると、スパニング ツリーはインターフェイスをフォワーディング ス テートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキングステートのレイヤ2インターフェイスはフレームの転送に関与しません。初期化後、ス イッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交 換するまで、ルートとして動作します。この BPDU 交換によって、ネットワーク上のどのスイッチが ルート、すなわちルート スイッチであるかが確立されます。ネットワークにスイッチが1台しかない 場合は、交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニングステートにな ります。インターフェイスはスイッチの初期化後、必ずブロッキングステートになります。

ブロッキングステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- **BPDU** を受信します。

リスニング ステート

リスニングステートは、ブロッキングステートを経て、レイヤ2インターフェイスが最初に移行する ステートです。インターフェイスがリスニングステートになるのは、スパニング ツリーによってその インターフェイスのフレーム転送への関与が決定された場合です。

リスニングステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ2インターフェイスは、フレームの転送に関与できるように準備します。 インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- **BPDU** を受信します。

フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスは、フレームを転送します。インターフェイ スはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- **BPDU** を受信します。

ディセーブル ステート

ブロッキング ステートのレイヤ2インターフェイスは、フレームの転送やスパニング ツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- **BPDU** を受信しません。

スイッチまたはポートがルート スイッチ またはルート ポートになる仕組み

ネットワーク上のすべてのスイッチがデフォルトのスパニング ツリー設定でイネーブルになっている 場合、最小の MAC アドレスを持つスイッチがルート スイッチになります。図 16-2 では、スイッチ A がルート スイッチとして選定されます(すべてのスイッチのスイッチ プライオリティがデフォルト (32768)に設定されており、スイッチ A の MAC アドレスが最小であるため)。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上 げる(数値を引き下げる)と、スパニング ツリーの再計算が強制的に行われ、最適なスイッチをルー トとした新しいトポロジが形成されます。





RP = ルート ポート DP = 指定ポート

スパニング ツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネット ワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合が あります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続 すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが 理想です。

たとえば、スイッチ B のあるポートがギガビット イーサネット リンクで、別のポート(10/100 リン ク)がルート ポートであると仮定します。ネットワーク トラフィックはギガビット イーサネット リン クに流す方が効率的です。ギガビット イーサネット ポートのスパニング ツリー ポート プライオリ ティをルート ポートより高くする(数値を小さくする)と、ギガビット イーサネット ポートが新しい ルート ポートになります。

スパニング ツリーおよび冗長接続

2 つのスイッチ インターフェイスを別の1 台のデバイス、または2 台の異なるデバイスに接続すること により、スパニング ツリーを使用して冗長バックボーンを作成できます(図 16-3 を参照)。スパニン グ ツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合には そのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必 ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート プライオリティとポート ID が加算され、値の小さいリンクがスパニング ツリーによってディセーブルにされます。



図 16-3 スパニング ツリーおよび冗長接続

EtherChannel グループを使用して、スイッチ間に冗長リンクを設定することもできます。詳細は、第 36章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。

スパニング ツリー アドレスの管理

IEEE 802.1D では、各種ブリッジ プロトコルに使用させるために、0x00180C2000000 ~ 0x0180C2000010 の範囲で 17 のマルチキャスト アドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリー ステートに関係なく、各スイッチは 0x0180C2000000 ~ 0x0180C200000F のアドレ ス宛のパケットを受信しますが、転送は行いません。

スパニングツリーがイネーブルな場合、スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛てのパケットを受信します。スパニングツリーがディセーブルな場合は、スイッチは、それらのパケットを不明のマルチキャスト アドレスとして転送します。

接続を維持するためのエージング タイムの短縮

ダイナミック アドレスのエージング タイムはデフォルトで 5 分です。これは、mac address-table aging-time グローバル コンフィギュレーション コマンドのデフォルト値です。ただし、スパニング ツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5 分以上にわたって到達できないことがあるので、アドレス テーブルからステーション アドレスを削除し、改めて学習できるように、アドレス エージング タイムが短縮されます。スパニング ツリー再構成時に短縮されるエージング タイムは、転送遅延パラメータ値(spanning-tree vlan vlan-id forward-time seconds グローバル コンフィギュレーション コマンド)と同じです。

各 VLAN はそれぞれ独立したスパニング ツリー インスタンスなので、スイッチは VLAN 単位でエー ジング タイムを短縮します。ある VLAN でスパニング ツリーの再構成が行われると、その VLAN で 学習されたダイナミック アドレスがエージング タイム短縮の対象になります。他の VLAN のダイナ ミック アドレスは影響を受けず、スイッチで設定されたエージング タイムがそのまま適用されます。

スパニング ツリー モードおよびプロトコル

このスイッチでサポートされるモードおよびプロトコルは、次のとおりです。

 PVST+: このスパニング ツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠 します。すべてのイーサネット ポートベースの VLAN で使用されるスパニング ツリーのデフォル トモードです。PVST+ はスイッチ上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリー パスを提供します。

PVST+は、対象となる VLAN にレイヤ 2 ロードバランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリ ンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルート スイッチがあります。このルート スイッチは、その VLAN に対応するスパニング ツリー情報を、 ネットワーク上の他のすべてのスイッチに伝送します。このプロセスにより、各スイッチがネット ワークに関する共通の情報を持つようになるので、ネットワーク トポロジが確実に維持されます。
Rapid PVST+: このスパニング ツリー モードは、IEEE 802.1w 標準に準拠した高速コンバージェ ンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はト ポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただち に削除します。このような場合、PVST+では、ダイナミックに学習した MAC アドレス エントリ には短いエージング タイムが使用されます。

Rapid PVST+ は PVST+ と同じ設定を使用しているので(特に明記する場合を除く)、必要なこと は最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベース を Rapid PVST+ に移行するのに、複雑な MSTP 設定の学習やネットワーク再設定の必要がないこ とです。Rapid PVST+ モードでは、各 VLAN は独自のスパニング ツリー インスタンスを最大数 実行します。

 MSTP:このスパニング ツリー モードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同 ーのスパニング ツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要と なるスパニング ツリー インスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol (RSTP) (IEEE 802.1w 準拠)上で実行され、転送遅延を解消し、ルート ポートおよび 指定ポートをフォワーディング ステートにすばやく移行することにより、スパニング ツリーの高 速コンバージェンスを可能にします。RSTP を使用せずに MSTP を稼動することはできません。

MSTP を導入する場合、最も一般的なのは、レイヤ2スイッチドネットワークのバックボーンおよびディストリビューション レイヤへの配備です。詳細は、第17章「MSTPの設定」を参照してください。

サポートされるスパニング ツリー インスタンス数については、次の項を参照してください。

サポートされるスパニング ツリー インスタンス

PVST+ または Rapid PVST+ モードでは、スイッチは最大 128 のスパニングツリー インスタンスをサポートします。

MSTP モードでは、スイッチは最大 65 MST インスタンスをサポートします。特定の MST インスタン スにマッピングできる VLAN の数に制限はありません。

スパニング ツリーと VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル)の相互作用に ついては、「スパニング ツリー設定時の注意事項」(P.16-14)を参照してください。

スパニング ツリーの相互運用性と下位互換性

表 16-2 に、ネットワークでサポートされるスパニング ツリー モード間の相互運用性と下位互換性を示します。

表 16-2 PVST+、MSTP、および Rapid PVST+ の相互運用性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり(制限あり)	あり(PVST+ に戻る)
MSTP	あり(制限あり)	あり	あり(PVST+ に戻る)
Rapid PVST+	あり(PVST+に戻る)	あり(PVST+に戻る)	あり

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree (CST) のルートは MST バックボーンの内側に配置する必要があり、PVST+ スイッチを複数の MST リージョンに接続す ることはできません。

ネットワーク内に Rapid PVST+ が稼動しているスイッチと PVST+ が稼動しているスイッチが存在す る場合、Rapid PVST+ スイッチと PVST+ スイッチを別のスパニング ツリー インスタンスにすること を推奨します。Rapid PVST+ スパニング ツリー インスタンスでは、ルート スイッチは Rapid PVST+ スイッチでなければなりません。PVST+ インスタンスでは、ルート スイッチは PVST+ スイッチでな ければなりません。PVST+ スイッチはネットワークのエッジに配置する必要があります。

STP および IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニング ツリー ストラテジに一定の 制限を設けています。この規格では、トランク上で使用できる*すべて*の VLAN に対して、1 つのスパ ニング ツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクによって接続された シスコ製スイッチのネットワークでは、スイッチはトランク上で使用できる*各*VLAN に 1 つずつ、ス パニング ツリー インスタンスを維持します。

IEEE 802.1Q トランクを使用してシスコ製スイッチを他社製のデバイスに接続する場合、シスコ製ス イッチは PVST+ を使用してスパニング ツリーの相互運用性を実現します。Rapid PVST+ がイネーブ ルの場合、スイッチは PVST+ ではなく Rapid PVST+ を使用します。スイッチは、トランクの IEEE 802.1Q VLAN のスパニング ツリー インスタンスと他社の IEEE 802.1Q スイッチのスパニング ツリー インスタンスを結合します。

ただし、PVST+または Rapid PVST+の情報はすべて、他社製の IEEE 802.1Q スイッチからなるクラ ウドにより分離されたシスコ製スイッチによって維持されます。シスコ製スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

PVST+は IEEE 802.1Q トランクで自動的にイネーブルになるので、ユーザ側で設定する必要はありま せん。アクセス ポートおよび ISL(スイッチ間リンク)トランク ポートでの外部スパニング ツリーの 動作は、PVST+の影響を受けません。

IEEE 802.1Q トランクの詳細については、第13章「VLAN の設定」を参照してください。

スパニング ツリー機能の設定

ここでは、次の設定情報について説明します。

- 「スパニング ツリー機能のデフォルト設定」(P.16-13)
- 「スパニング ツリー設定時の注意事項」(P.16-14)
- 「スパニング ツリー モードの変更」(P.16-15)(必須)
- 「スパニング ツリーのディセーブル化」(P.16-16)(任意)
- 「ルートスイッチの設定」(P.16-16)(任意)
- 「セカンダリルートスイッチの設定」(P.16-18)(任意)
- 「ポート プライオリティの設定」(P.16-19)(任意)
- 「パス コストの設定」(P.16-20)(任意)
- 「VLAN のスイッチ プライオリティの設定」(P.16-21)(任意)
- 「スパニング ツリー タイマーの設定」(P.16-22)(任意)

スパニング ツリー機能のデフォルト設定

表 16-3 に、スパニング ツリー機能のデフォルト設定を示します。

表 16-3 スパニング ツリー機能のデフォルト設定

	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
	詳細については、「サポートされるスパニ ング ツリー インスタンス」(P.16-11)を参 照してください。
スパニング ツリー モード	PVST+ (Rapid PVST+ と MSTP はディ セーブル)
スイッチ プライオリティ	32768
スパニング ツリー ポート プライオリティ(インターフェイス単位で設定可能)	128
スパニング ツリー ポート コスト(インターフェイス単位で設定可能)	1000 Mbps : 4
	100 Mbps : 19
	10 Mbps : 100
スパニング ツリー VLAN ポート プライオリティ(VLAN 単位で設定可能)	128
スパニング ツリー VLAN ポート コスト(VLAN 単位で設定可能)	1000 Mbps : 4
	100 Mbps : 19
	10 Mbps : 100
スパニング ツリー タイマー	Hello タイム:2秒
	転送遅延時間:15秒
	最大エージング タイム:20 秒
	転送保留カウント:6 BPDU

スパニング ツリー設定時の注意事項

VTP にスパニングツリー インスタンスよりも多くの VLAN が定義されている場合、PVST+ または Rapid PVST+ をイネーブルにできるのは、スイッチ上の 128 の VLAN に限られます。残りの VLAN は、スパニング ツリーがディセーブルの状態で動作します。ただし、MSTP を使用して複数の VLAN を同一のスパニング ツリー インスタンスにマッピングすることが可能です。詳細は、第 17 章「MSTP の設定」を参照してください。

128 のスパニング ツリー インスタンスがすでに使用されている場合、VLAN の1 つでスパニング ツ リーをディセーブルにして、STP を稼動させたい別の VLAN でイネーブルにできます。no spanning-tree vlan vlan-id グローバル コンフィギレーション コマンドを使用して、特定の VLAN で スパニング ツリーをディセーブルにし、spanning-tree vlan vlan-id グローバル コンフィギュレーショ ン コマンドを使用して、所定の VLAN でスパニング ツリーをイネーブルにします。



スパニング ツリーが稼動していないスイッチは、スパニング ツリー インスタンスが稼動している VLAN 上の他のスイッチがループを切断できるように、受信した BPDU を引き続き転送します。 したがって、スパニング ツリーは、ネットワーク上のすべてのループを切断できるように十分な数 のスイッチ上で稼動している必要があります。たとえば、VLAN の各ループで少なくとも1 台のス イッチがスパニング ツリーを稼動している必要があります。VLAN 内のすべてのスイッチでスパニ ング ツリーを稼動させる必要はありません。ただし、最小限の数のスイッチだけでスパニング ツ リーが稼動している状況では、不注意なネットワーク変更によって VLAN に別のループが発生し、 ブロードキャスト ストームを引き起こす可能性があります。



スイッチ上の使用可能なスパニング ツリー インスタンスをすべて使い切ってしまったあとに、VTP ド メイン内にさらに別の VLAN を追加すると、そのスイッチ上にスパニング ツリーが稼動しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リストが設定されていると、 すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、 新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチで スパニング ツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニング ツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定するこ とにより、このような可能性を防ぐことができます。ただし、ネットワークに VLAN を追加するとき より多くの作業を伴うことになるので、通常、許可リストの設定は必要ありません。

VLAN スパニング ツリー インスタンスの設定はスパニング ツリー コマンドによって制御されます。 スパニング ツリー インスタンスは、VLAN にインターフェイスを割り当てるときに作成します。スパ ニング ツリー インスタンスは最終インターフェイスが別の VLAN に移されたときに削除されます。ス パニング ツリー インスタンスの作成前に、スイッチとポートのパラメータを設定できます。設定され たパラメータは、スパニング ツリー インスタンスを作成するときに適用されます。

スイッチは、PVST+、Rapid PVST+、および MSTP をサポートしますが、アクティブにできるバー ジョンは常に1つだけです(たとえば、すべての VLAN で PVST+を使用するか、すべての VLAN で Rapid PVST+を使用するか、またはすべての VLAN で MSTP を使用することになります)。さまざま なスパニング ツリー モードおよび相互運用性については、「スパニング ツリーの相互運用性と下位互 換性」(P.16-12)を参照してください。

UplinkFast および BackboneFast に関する設定時の注意事項については、「オプションのスパニング ツリー設定時の注意事項」(P.18-11)を参照してください。



ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、 STP を実行するデバイスを直接接続することを推奨します。

スパニング ツリー モードの変更

スイッチは、PVST+、Rapid PVST+、および MSTP の3 つのスパニング ツリー モードをサポートします。デフォルトで、スイッチは PVST+ プロトコルを使用します。

スパニング ツリー モードを変更するには、特権 EXEC モードで次の手順を実行します。デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<pre>spanning-tree mode {pvst mst rapid-pvst}</pre>	スパニング ツリー モードを設定します。
		 pvst を指定して、PVST+ をイネーブルにします(デフォルト 設定)。
		 mst を指定して、MSTP(および RSTP)をイネーブルにします。設定手順の詳細については、第 17 章「MSTP の設定」を 参照してください。
		• rapid-pvst を指定して、Rapid PVST+ をイネーブルにします。
ステップ 3	interface interface-id	(Rapid PVST+ モードの場合のみ推奨) 設定するインターフェイス を指定し、インターフェイス コンフィギュレーション モードを開 始します。有効なインターフェイスには、物理ポート、VLAN、お よびポートチャネルがあります。VLAN ID の範囲は 1 ~ 4094 で す。ポート チャネルの範囲は 1 ~ 6 です。
ステップ 4	spanning-tree link-type point-to-point	(Rapid PVST+ モードの場合のみ推奨) このポートのリンク タイプ をポイントツーポイントに指定します。
		このポート(ローカル ポート)をポイントツーポイント リンクで リモート ポートと接続し、ローカル ポートが指定ポートになると、 スイッチはリモート ポートとネゴシエーションし、ローカル ポー トをフォワーディング ステートに高速変更します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	clear spanning-tree detected-protocols	(Rapid PVST+ モードの場合のみ推奨) スイッチ上の任意のポート が IEEE 802.1D 準拠のレガシー スイッチのポートと接続されてい る場合に、スイッチ全体でプロトコル移行プロセスを再開します。
		このステップは、このスイッチで Rapid PVST+ が稼動しているこ とを指定スイッチが検出する場合のオプションです。
ステップ 7	show spanning-tree summary	設定を確認します。
	および	
	show spanning-tree interface <i>interface-id</i>	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、no spanning-tree mode グローバル コンフィギュレーション コマ ンドを使用します。ポートをデフォルト設定に戻すには、no spanning-tree link-type インターフェイ ス コンフィギュレーション コマンドを使用します。

スパニング ツリーのディセーブル化

スパニング ツリーはデフォルトで、VLAN 1 および「サポートされるスパニング ツリー インスタン ス」(P.16-11)のスパニング ツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブ ルです。スパニング ツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが 確実な場合だけにしてください。

Æ 注意

スパニング ツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

VLAN 単位でスパニング ツリーをディセーブルにするには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no spanning-tree vlan vlan-id	<i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スパニング ツリーを再びイネーブルにする場合は、spanning-tree vlan vlan-id グローバル コンフィ ギュレーション コマンドを使用します。

ルート スイッチの設定

スイッチは、スイッチ上で設定されているアクティブ VLAN ごとに 1 つずつ、個別のスパニング ツ リー インスタンスを維持します。各インスタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるブリッジ ID が対応付けられます。VLAN ごとに、ブリッジ ID が最小のスイッチが その VLAN のルート スイッチになります。

特定の VLAN でスイッチがルートになるように設定するには、spanning-tree vlan vlan-id root グロー バル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値(32768) からかなり小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、 ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、 スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、この スイッチを指定された VLAN のルートに設定できます。

指定された VLAN のルート スイッチに 24576 未満のスイッチ プライオリティが設定されている場合、 スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します (表 16-1 (P.16-4)に示すように、4096 は 4 ビットのスイッチ プライオリ ティ値の最下位ビットの値です)。



ルート スイッチとして設定する必要のある値が1未満の場合、spanning-tree vlan vlan-id root グロー バル コンフィギュレーション コマンドは失敗します。 <u>》</u> (注)

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合 は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張シ ステム ID によって、旧ソフトウェアが稼動する接続スイッチのプライオリティより VLAN 番号が大 きくなるたびに、スイッチ プライオリティ値が増大します。

(注)

各スパニング ツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリ ビューション スイッチにする必要があります。アクセス スイッチをスパニング ツリーのプライマリ ルートとして設定しないでください。

レイヤ2ネットワークの直径(すなわち、レイヤ2ネットワーク上の任意の2つのエンドステーション間の最大スイッチホップ数)を指定するには、diameterキーワードを指定します。ネットワークの 直径を指定すると、その直径のネットワークに最適なハロータイム、転送遅延時間、および最大エー ジングタイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できま す。自動的に算出された Hello タイムを変更する場合は、hello キーワードを使用します。

(注)

ルート スイッチとして設定したあとで、**spanning-tree vlan** *vlan-id* **hello-time**、**spanning-tree vlan** *vlan-id* **forward-time**、および **spanning-tree vlan** *vlan-id* **max-age** グローバル コンフィギュレーショ ン コマンドを使用して、Hello タイム、転送遅延時間、および最大エージング タイムを手動で設定す ることは推奨できません。

スイッチが特定の VLAN のルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<pre>spanning-tree vlan vlan-id root primary [diameter net-diameter [hello-time seconds]]</pre>	指定された VLAN のルートになるように、スイッチを設定 します。
		 vlan-id には、VLAN ID で識別された単一の VLAN、 ハイフンで区切られた範囲の VLAN、またはカンマで 区切られた一連の VLAN を指定できます。指定できる 範囲は 1 ~ 4094 です。
		 (任意) diameter net-diameter には、任意の2つのエンドステーション間の最大スイッチ数を指定します。 指定できる範囲は2~7です。
		 (任意) hello-time seconds には、ルート スイッチに よってコンフィギュレーション メッセージが生成され る間隔を秒数で指定します。指定できる範囲は 1 ~ 10 です。デフォルトは 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree detail	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、no spanning-tree vlan vlan-id root グローバル コンフィギュレー ション コマンドを使用します。

セカンダリ ルート スイッチの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値 (32768) から 28672 に変更されます。したがって、プライマリ ルート スイッチで障害が発生した場合に、この スイッチが指定された VLAN のルート スイッチになる可能性が高くなります。これは、他のネット ワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能 性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。 spanning-tree vlan vlan-id root primary グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク直径および Hello タイム値を使用してください。

スイッチが特定の VLAN のセカンダリ ルートになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id root secondary [diameter net-diameter [hello-time seconds]]	 指定された VLAN のセカンダリ ルートになるように、スイッチを設定します。 <i>vlan-id</i> には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLANを指定できます。指定できる範囲は 1 ~ 4094 です。 (任意) diameter <i>net-diameter</i> には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。
		 (任意) hello-time seconds には、ルート スイッチによって コンフィギュレーション メッセージが生成される間隔を秒数 で指定します。指定できる範囲は 1 ~ 10 です。デフォルト は 2 です。
		プライマリ ルート スイッチを設定したときと同じネットワーク 直径および Hello タイム値を使用してください。「ルート スイッ チの設定」(P.16-16)を参照してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree detail	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、no spanning-tree vlan vlan-id root グローバル コンフィギュレー ション コマンドを使用します。

ポート プライオリティの設定

ループが発生した場合、スパニング ツリーはポート プライオリティを使用して、フォワーディングス テートにするインターフェイスを選択します。最初に選択させたいインターフェイスには高いプライオ リティ(小さい数値)を与え、最後に選択させたいインターフェイスには低いプライオリティ(大きい 数値)を与えます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパニ ング ツリーはインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他 のインターフェイスをブロックします。

インターフェイスのポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイ ス コンフィギュレーション モードを開始します。
		有効なインターフェイスは、物理ポートおよびポート チャネル論理インターフェイス(port-channel <i>port-channel-number</i>)です。
ステップ 3	spanning-tree port-priority priority	インターフェイスにポート プライオリティを設定しま す。
		<i>priority</i> に指定できる範囲は0~240で、16 ずつ増加 します。デフォルトは128です。有効な値は、0、16、 32、48、64、80、96、112、128、144、160、176、 192、208、224、240です。その他の値はすべて拒否さ れます。値が小さいほど、プライオリティは高くなり ます。
ステップ 4	spanning-tree vlan vlan-id port-priority priority	VLAN にポート プライオリティを設定します。
		 vlan-id には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、ま たはカンマで区切られた一連の VLAN を指定でき ます。指定できる範囲は 1 ~ 4094 です。
		 priority に指定できる範囲は 0 ~ 240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティは高くなります。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show spanning-tree interface interface-id	設定を確認します。
	または	
	show spanning-tree vlan vlan-id	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存 します。



show spanning-tree interface *interface-id* 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能の状態にある場合に限られます。それ以外の情報については、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

デフォルトの設定値に戻す場合は、no spanning-tree [vlan vlan-id] port-priority インターフェイス コ ンフィギュレーション コマンドを使用します。スパニング ツリー ポート プライオリティを使用してト ランク ポートに負荷分散を設定する手順については、「トランク ポートの負荷分散の設定」(P.13-21) を参照してください。

パス コストの設定

スパニング ツリー パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。 ループが発生した場合、スパニング ツリーはコストを使用して、フォワーディング ステートにするイ ンターフェイスを選択します。最初に選択させたいインターフェイスには小さいコスト値を与え、最後 に選択させたいインターフェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコ スト値が与えられている場合、スパニング ツリーはインターフェイス番号が最小のインターフェイス をフォワーディング ステートにし、他のインターフェイスをブロックします。

インターフェイスのコストを設定するには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。有効なインター フェイスは、物理ポートおよびポート チャネル論理インター フェイス(port-channel <i>port-channel-number</i>)です。
ステップ 3	spanning-tree cost cost	インターフェイスにコストを設定します。
		ループが発生した場合、スパニング ツリーはパス コストを使 用して、フォワーディング ステートにするインターフェイス を選択します。パス コストが小さいほど、高速で伝送されま す。
		<i>cost</i> に指定できる範囲は1~200000000です。デフォルト値はインターフェイスのメディア速度に基づきます。
ステップ 4	spanning-tree vlan vlan-id cost cost	VLAN にコストを設定します。
		ループが発生した場合、スパニング ツリーはパス コストを使 用して、フォワーディング ステートにするインターフェイス を選択します。パス コストが小さいほど、高速で伝送されま す。
		 vlan-id には、VLAN ID で識別された単一の VLAN、ハ イフンで区切られた範囲の VLAN、またはカンマで区切 られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。
		 cost に指定できる範囲は1~200000000です。デフォル ト値はインターフェイスのメディア速度に基づきます。
ステップ 5	end	特権 EXEC モードに戻ります。

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

<u>》</u> (注)

show spanning-tree interface *interface-id* 特権 EXEC コマンドで情報が表示されるのは、リンクアップ動作可能の状態にあるポートに限られます。それ以外の情報については、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

デフォルトの設定値に戻す場合は、no spanning-tree [vlan vlan-id] cost インターフェイス コンフィ ギュレーション コマンドを使用します。スパニング ツリー パス コストを使用してトランク ポートに 負荷分散を設定する手順については、「トランク ポートの負荷分散の設定」(P.13-21) を参照してくだ さい。

VLAN のスイッチ プライオリティの設定

スイッチ プライオリティを設定して、スイッチがルート スイッチとして選択される可能性を高めることができます。

(注)

このコマンドは、十分に注意して使用してください。スイッチ プライオリティの変更には、通常は、 spanning-tree vlan *vlan-id* root primary および spanning-tree vlan *vlan-id* root secondary グローバ ル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のスイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この 手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id priority priority	VLAN のスイッチ プライオリティを設定します。
		 vlan-id には、VLAN ID で識別された単一の VLAN、 ハイフンで区切られた範囲の VLAN、またはカンマ で区切られた一連の VLAN を指定できます。指定で きる範囲は 1 ~ 4094 です。
		 priority を指定する場合、指定できる範囲は0~ 61440で、4096ずつ増加します。デフォルトは32768です。数値が小さいほど、スイッチがルートスイッチとして選択される可能性が高くなります。
		有効なプライオリティ値は、4096、8192、12288、 16384、20480、24576、28672、32768、36864、 40960、45056、49152、53248、57344、61440で す。その他の値はすべて拒否されます。
ステップ 3	end	特権 EXEC モードに戻ります。

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

デフォルトの設定値に戻す場合は、no spanning-tree vlan vlan-id priority グローバル コンフィギュ レーション コマンドを使用します。

スパニング ツリー タイマーの設定

表 16-4 で、スパニング ツリーのパフォーマンス全体を左右するタイマーについて説明します。

表 16-4 スパニング ツリー タイマー

変数	説明
Hello タイマー	スイッチから他のスイッチへ Hello メッセージをブロードキャストする頻度を制御します。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継 続する時間を制御します。
最大エージング タイ	インターフェイスが受信したプロトコル情報をスイッチに保存させておく時間を制御します。
マー	
転送保留カウント	1 秒間停止する前に送信できる BPDU 数を制御します。

以下に設定手順を示します。

Hello タイムの設定

Hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージ が生成される間隔を設定できます。

(注)

このコマンドは、十分に注意して使用してください。Hello タイムの変更には、通常、spanning-tree vlan *vlan-id* root primary および spanning-tree vlan *vlan-id* root secondary グローバル コンフィギュ レーション コマンドを使用することを推奨します。

VLANの Hello タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id hello-time seconds	VLAN の Hello タイムを設定します。ハロー タイムはルート スイッチが コンフィギュレーション メッセージを生成する間隔です。これらのメッ セージは、スイッチがアクティブであることを意味します。
		 vlan-id には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。
		 seconds に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。

	コマンド	目的
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定値に戻す場合は、no spanning-tree vlan *vlan-id* hello-time グローバル コンフィギュ レーション コマンドを使用します。

VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	spanning-tree vlan vlan-id forward-time seconds	VLAN の転送時間を設定します。転送遅延時間は、スパニング ツリー ラーニング ステートおよびリスニング ステートからフォワーディング ス テートに移行するまでに、インターフェイスが待機する秒数です。	
		 vlan-id には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 	
		• seconds に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。	
ステップ 3	end	特権 EXEC モードに戻ります。	
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

デフォルトの設定値に戻す場合は、no spanning-tree vlan vlan-id forward-time グローバル コンフィ ギュレーション コマンドを使用します。

VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree vlan vlan-id max-age seconds	VLAN の最大エージング タイムを設定します。最大エージング タイムは、 再構成を試行するまでにスイッチがスパニング ツリー コンフィギュレー ション メッセージを受信せずに待機する秒数です。
		 <i>vlan-id</i>には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。
		• seconds に指定できる範囲は 6 ~ 40 です。デフォルト値は 20 です。

	コマンド	目的	
ステップ 3	end	特権 EXEC モードに戻ります。	
ステップ 4	show spanning-tree vlan vlan-id	設定を確認します。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	
ステップ 4 ステップ 5	show spanning-tree vlan <i>vlan-id</i> copy running-config startup-config	 特権 EAEC モニトに失ります。 設定を確認します。 (任意) コンフィギュレーション ファイルに設定を保存します。 	

デフォルトの設定値に戻す場合は、no spanning-tree vlan vlan-id max-age グローバル コンフィギュ レーション コマンドを使用します。

転送保留カウントの設定

転送保留カウント値を変更することで、BPDU のバースト サイズを設定できます。

(注)

このパラメータをより高い値に変更すると、CPUの使用率が非常に大きくなります(Rapid PVST モード時に特に顕著に変化します)。逆に、この値を低く設定すると、セッションによってはコンバー ジェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

転送保留カウントを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
テップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
テップ 2	spanning-tree transmit hold-count value	1 秒間停止する前に送信できる BPDU 数を設定します。
		<i>value</i> に指定できる範囲は 1 ~ 20 です。デフォルト値は 6 です。
・ップ 3	end	特権 EXEC モードに戻ります。
ーップ 4	show spanning-tree detail	設定を確認します。
・ップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

デフォルトの設定値に戻す場合は、no spanning-tree transmit hold-count value グローバル コンフィ ギュレーション コマンドを使用します。

スパニング ツリー ステータスの表示

スパニングツリー ステータスを表示するには、表 16-5 の特権 EXEC コマンドを1つまたは複数使用します。

表 16-5 スパニング ツリー ステータス表示用のコマンド

コマンド	目的	
show spanning-tree active	アクティブ インターフェイスに関するスパニング ツリー情報だけを表示	
	します。	
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。	
show spanning-tree interface interface-id	特定のインターフェイスのスパニング ツリー情報を表示します。	
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。または STP ステー ト セクションのすべての行を表示します。	

clear spanning-tree [interface *interface-id*] 特権 EXEC コマンドを使用して、スパニングツリー カウ ンタをクリアできます。

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。

■ スパニング ツリー ステータスの表示



снартев 17

MSTP の設定

この章では、Catalyst 2960 スイッチに IEEE 802.1s Multiple STP (MSTP) のシスコ実装を設定する 方法について説明します。

(注)

Multiple Spanning-Tree (MST; 多重スパニング ツリー) 実装は IEEE 802.1s 標準に準拠しています。 Cisco IOS Release 12.2(25)SED よりも古い Cisco IOS リリースの MST 実装は、先行標準のものに準 拠しています。

MSTP は複数の VLAN を同一のスパニング ツリー インスタンスにマッピングできるようにして、多数 の VLAN をサポートする場合に必要となるスパニング ツリー インスタンスの数を減らします。MSTP は、データ トラフィック用に複数の転送パスを提供し、ロードバランシングを可能にします。MSTP を使用すると、1 つのインスタンス(転送パス)で障害が発生しても他のインスタンス(転送パス)は 影響を受けないので、ネットワークのフォールトトレランスが向上します。MSTP を導入する場合、 最も一般的なのは、レイヤ2スイッチド ネットワークのバックボーンおよびディストリビューション レイヤへの導入です。MSTP の導入により、サービス プロバイダー環境に求められる高可用性ネット ワークを実現できます。

スイッチが MST モードの場合、IEEE 802.1w 準拠の Rapid Spanning-Tree Protocol (RSTP) が自動的 にイネーブルになります。RSTP は、IEEE 802.1D の転送遅延を軽減し、ルート ポートおよび指定 ポートをフォワーディング ステートにすばやく移行する明示的なハンドシェイクによって、スパニン グ ツリーの高速コンバージェンスを実現します。

RSTP と MSTP は、(オリジナル) IEEE 802.1D スパニング ツリー準拠デバイス、既存のシスコ独自の Multiple Instance STP (MISTP)、および既存のシスコ Per-VLAN Spanning-Tree plus (PVST+) との 下位互換性を保ちながら、スパニング ツリーの動作を向上させます。PVST+ および Rapid PVST+ に ついては、第 16 章「STP の設定」を参照してください。PortFast、UplinkFast、ルート ガードなどの その他のスパニング ツリーの機能については、第 18 章「オプションのスパニング ツリー機能の設定」 を参照してください。

(注)

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

この章で説明する内容は、次のとおりです。

- 「MSTP の概要」(P.17-2)
- 「RSTP の概要」(P.17-9)
- 「MSTP 機能の設定」(P.17-15)
- 「MST コンフィギュレーションおよびステータスの表示」(P.17-28)

MSTP の概要

MSTP は、高速コンバージェンスが可能な RSTP を使用し、複数の VLAN を1 つのスパニング ツリー インスタンスにまとめます。各インスタンスのスパニング ツリー トポロジは、他のスパニング ツリー インスタンスの影響を受けません。このアーキテクチャによって、データ トラフィックに複数の転送 パスが提供され、ロードバランシングが可能になり、また多数の VLAN をサポートするのに必要なス パニング ツリー インスタンスの数を減らすことができます。

ここでは、MSTP の機能について説明します。

- 「MST リージョン」 (P.17-2)
- 「IST、CIST、および CST」(P.17-2)
- 「ホップ カウント」(P.17-6)
- 「境界ポート」(P.17-6)
- 「IEEE 802.1s の実装」(P.17-7)
- 「IEEE 802.1D STP との相互運用性」(P.17-9)

設定情報については、「MSTP機能の設定」(P.17-15)を参照してください。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して 矛盾のないようにスイッチを設定しなければなりません。同じ MST コンフィギュレーションを持ち、 相互接続されたスイッチの集合を MST リージョンといいます(図 17-1 (P.17-4)を参照)。

各スイッチがどの MST リージョンに属しているかは、MST コンフィギュレーションによって制御さ れます。MST コンフィギュレーションには、リージョン名、リビジョン番号、MST の VLAN とイン スタンスの割り当てマップが保存されています。スイッチにリージョンを設定するには、そのスイッチ で spanning-tree mst configuration グローバル コンフィギュレーション コマンドを使用して、MST コンフィギュレーション モードを開始します。このモードでは、instance MST コンフィギュレーショ ン コマンドを使用して VLAN を MST インスタンスにマッピングし、name MST コンフィギュレー ション コマンドを使用してリージョン名を指定し、revision MST コンフィギュレーション コマンドを 使用してリビジョン番号を設定できます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバーが必要で す。さらに、各メンバーは、RSTP Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユ ニット)を処理できる必要があります。ネットワーク内の MST リージョンの数には制限はありません が、各リージョンがサポートできるスパニング ツリー インスタンスの数は 65 までです。インスタンス は 0 ~ 4094 の数字で識別されます。VLAN には、一度に 1 つのスパニング ツリー インスタンスのみ 割り当てることができます。

IST、CIST、および CST

すべてのスパニング ツリー インスタンスが独立している PVST+ および Rapid PVST+ とは異なり、 MSTP は次の2種類のスパニング ツリーを確立して維持します。

- Internal Spanning-Tree (IST) は、1 つの MST リージョン内で稼動するスパニング ツリーです。
 - 各 MST リージョン内の MSTP は複数のスパニング ツリー インスタンスを維持しています。イン スタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他の MST イン スタンスはすべて 1 ~ 4094 まで番号が付けられます。

IST は、BPDU を送受信する唯一のスパニング ツリー インスタンスです。他のスパニング ツリー の情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。 MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニング ツリー インスタ ンスをサポートする処理が必要な BPDU の数を大幅に減少できます。

同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジ パラメータ (ルート スイッチ ID、ルート パス コストなど) を持っています。デフォルトでは、すべての VLAN が IST に割り当てられています。

MST インスタンスはリージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されていても、リージョン A の MST インスタンス 1 は、リージョン B の MST インス タンス 1 から独立しています。

Common and Internal Spanning-Tree (CIST) は、各 MST リージョン内の IST と、MST リージョンおよびシングル スパニング ツリーを相互接続する Common Spanning-Tree (CST) の集合です。

1 つのリージョン内で計算されたスパニング ツリーは、スイッチド ドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準 をサポートするスイッチ間で実行されるスパニング ツリー アルゴリズムによって形成されます。 MST リージョン内の CIST は、リージョン外の CST と同じです。

詳細については、「MST リージョン内の動作」(P.17-3) および「MST リージョン間の動作」(P.17-4) を参照してください。

(注)

IEEE 802.1s 標準を実装すると、一部の MST 実装関連の用語が変更されます。これらの変更の要約に ついては、表 16-1 (P.16-4) を参照してください。

MST リージョン内の動作

IST は 1 つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルート は、図 17-1 (P.17-4) のように、CIST リージョナル ルート (IEEE 802.1s 標準が実装される以前は *IST マスター*) になります。CIST ルートに対してリージョン内で最も低いスイッチ ID とパス コスト を持つスイッチがルートになります。また、リージョンがネットワーク内に 1 つしかなければ、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リー ジョンの境界に位置する MSTP スイッチの 1 つが CIST リージョナル ルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナル ルートであることを主 張するため、CIST ルートと CIST リージョナル ルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべての インスタンスのルートであると主張します。スイッチは、ポートに現在保存されているルート情報より も優位の MST ルート情報 (小さいスイッチ ID、パス コストなど)を受信すると、CIST リージョナル ルートとしての主張を撤回します。

初期化中、リージョン内にそれぞれが CIST リージョナル ルートである多数のサブリージョンが存在す る場合があります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真 の CIST リージョナル ルートが含まれている新しいサブリージョンに加入します。このようにして、真 の CIST リージョナル ルートが含まれているサブリージョン以外のサブリージョンはすべて縮小させま す。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナル ルートを承認する必要があります。共通の CIST リージョナル ルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

MST リージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシー スイッチが混在している場合、 MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築して維持します。MST インスタンスは、リージョンの境界で IST と結合して CST になり ます。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチド ドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナル ルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

図 17-1 は、3 つの MST リージョンと IEEE 802.1D 準拠のレガシー スイッチ(D) からなるネット ワークを示しています。リージョン1(A)の CIST リージョナル ルートは、CIST のルートでもあり ます。リージョン2の CIST リージョナル ルート(B)およびリージョン3の CIST リージョナル ルー ト(C)は、CIST 内にあるそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼動 しています。



BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニング ツリー 情報を BPDU に追加して、近接スイッチと通信し、最終的なスパニング ツリー トポロジを計算しま す。したがって、BPDU 伝送に関連するスパニング ツリー パラメータ (ハロー タイム、転送時間、最 大エージング タイム、最大ホップ数など) は、CST インスタンスだけで設定されますが、その影響は すべての MST インスタンスにおよびます。スパニング ツリー トポロジに関連するパラメータ (ス イッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど) は、CST インス タンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、IEEE 802.1D 準拠のレガシー スイッチと通信します。MSTP スイッチ同士の通信には、MSTP BPDU が使用 されます。

IEEE 802.1sの用語

シスコ'の先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたは リージョ ンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連し ている外部パラメータと違い、MST リージョン内でのみ影響があります。CIST はネットワーク全体 を網羅するスパニング ツリー インスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル 修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルート スイッチです。
- CIST 外部ルート パス コストは、CIST ルートへのコストです。このコストは MST リージョン内でも変更されずに残ります。CIST では、MST リージョンが単一のスイッチのように見えるので注意してください。CIST 外部ルート パス コストは、これらの仮想スイッチとリージョンに属していないスイッチ間を計算して出したルート パス コストです。
- CIST リージョナル ルートは先行標準の実装では IST マスターと呼ばれていました。CIST ルート がリージョン内にある場合、CIST リージョナル ルートが CIST ルートになります。または、CIST リージョナル ルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リー ジョナル ルートは IST のルート スイッチとして動作します。
- CIST 内部ルート パス コストは、リージョン内の CIST リージョナル ルートへのコストです。この コストは IST (インスタンス 0)のみに関係します。
- 表 17-1 (P.17-5) に、IEEE 標準とシスコの先行標準の用語の比較を示します。

表 17-1 先行標準の用語および標準の用語

IEEE 標準	シスコ先行標準	シスコ標準
CIST リージョナル ルート	IST マスター	CIST リージョナル ルート
CIST 内部ルート パス コスト	IST マスター パス コスト	CIST 内部パス コスト
CIST 外部ルート パス コスト	ルート パス コスト	ルート パス コスト
MSTI リージョナル ルート	インスタンス ルート	インスタンス ルート
MSTI 内部ルート パス コスト	ルート パス コスト	ルート パス コスト

ホップ カウント

IST および MST インスタンスは、スパニング ツリー トポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わり、ルートへ のパス コスト、および IP Time to Live (TTL) メカニズムに似たホップ カウント メカニズムを使用し ます。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用することにより、 リージョン内の最大ホップを設定し、その値をリージョン内の IST インスタンスとすべての MST イン スタンスに適用できます。ホップ カウントを設定すると、メッセージ エージ情報を設定するのと同様 の結果が得られます(再構成の開始時期を決定します)。インスタンスのルート スイッチは、常にコス トを 0、ホップ カウントを最大値に設定して BPDU(または M レコード)を送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウ ントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDUのRSTP部分に格納されているメッセージ有効期間と最大エージングタイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼動する単一のスパニング ツリー リージョン、 PVST+ または Rapid PVST+ が稼動する単一のスパニング ツリー リージョン、または異なる MST コ ンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。また、境界ポー トは、指定スイッチが単一のスパニング ツリー スイッチ、または異なる MST コンフィギュレーショ ンを持つスイッチである LAN に接続されます。

IEEE 8021.s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートで 受信可能な内部(同ーリージョンからの)および外部の2種類のメッセージを識別します。メッセージ が外部のものであれば、CIST によってのみ受信されます。CIST の役割がルートや代替ルートの場合、 または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。 メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは 個々の M レコードのみを受信します。シスコ先行標準の実装では、ポートが境界ポートとして外部 メッセージを受信します。つまり、ポートは内部メッセージと外部メッセージを混在させたものは受信 できません。

MST リージョンには、スイッチと LAN の両方が含まれています。セグメントは、指定されたポート のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポート は境界ポートになります。この定義を利用すると、リージョン内部にある 2 つのポートのうち一方を、 異なるリージョンに属するポートとしてセグメントを共有させることができます。この方法を採用する と、内部および外部の両方からポートでメッセージを受信できる場合があります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。



レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナル ルート スイッチ ID フィールドが加えられたことです。一貫した送信スイッチ ID を近接スイッチに送信することで、リージョン全体で1 つの仮想スイッチのように動作します。この例では、スイッチ A または B がそのセグメントで指定されているかどうかに関わらず、スイッチ C が、ルートの一貫した送信スイッチ ID を持つ BPDU を受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標 準には含まれていない一部の(要望されている)先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでしたが、境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステートに必ずしも従うわけではありません。現状、次の2通りの事例が考えられます。

- 境界ポートが CIST リージョナル ルートのルート ポートである場合: CIST インスタンス ポートを 提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わったあとであれば(そ の後フォワーディングします)、その場合のみ合意を返信してフォワーディング ステートに移行で きます。現在 MSTI ポートは、マスターという特別な役割を担っています。
- 境界ポートが CIST リージョナル ルートのルート ポートでない場合: MSTI ポートは、CIST ポートのステートと役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU (M レコード)を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかり にくいかもしれません。この場合、境界の役割自体は存在していませんが、show コマンドで見る と、出力される type カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシー スイッチと標準スイッチの相互運用

先行標準のスイッチでは先行標準のポートを自動検出ができないため、インターフェイス コンフィ ギュレーション コマンドを使用して認識させます。標準と先行標準の間にあるリージョンは形成でき ませんが、CIST を使用することで相互運用できます。このような特別な方法を採用しても、失われる 機能は、異なるインスタンス上のロード バランシングのみです。ポートが先行標準の BPDU を受信す ると、CLI (コマンドライン インターフェイス) にはポートの設定に応じて異なるフラッグが表示され ます。また、スイッチが、先行標準の BPDU 転送の設定がされてないポートで先行標準の BPDU をは じめて受信すると、Syslog メッセージにも表示されます。 図 17-2 に、このシナリオを示します。A を標準スイッチ、B を先行標準のスイッチと仮定してください。両方とも同じリージョンに設定されています。A が CIST のルート スイッチのため、B にセグメント X のルート ポート(BX) とセグメント Y の代替ポート(BY) があります。セグメント Y がフラッ プして、先行標準の BPDU を送信する前に BY のポートが代替ポートになった場合、AY は Y に接続 している先行標準のスイッチを検出できないため、標準の BPDU を送信し続けます。また、BY ポートは境界で固定されるため、AB 間でのロード バランシングができなくなります。同一の問題はセグメント X でも発生しますが、B がトポロジの変更を転送する場合があります。



図 17-2 標準スイッチおよび先行標準のスイッチでの相互運用

単一方向リンクの失敗の検出

(注)

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフ トウェアを使用することで、受信した BPDU からポートの役割とステートの一貫性を確認し、単一方 向リンクが失敗してブリッジ処理のループを引き起こしていないかどうかを検証できます。

指定ポートで矛盾が検出された場合、役割には従いますが、ブリッジ処理のループを引き起こすより は、矛盾による接続中断のほうが望ましい状態のため、廃棄ステートへ戻ります。

図 17-3 に、ブリッジ処理のループを引き起こす一般的な単一方向リンクの失敗例を示します。スイッ チA はルート スイッチです。スイッチB へ向かうリンク上で、BPDU が紛失しています。RSTP と MST BPDU には、送信ポートの役割とステートが含まれています。この情報があれば、スイッチA は、送信した優位 BPDU にスイッチB が反応しないこと、さらにスイッチB はルート スイッチではな く指定スイッチであることを検出できます。結果として、スイッチA は自身のポートをブロックし (またはブロックを維持して)、ブリッジ処理のループを回避します。



IEEE 802.1D STP との相互運用性

MSTP が稼動しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする 組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU (プロトコルバージョンが 0 に設定されている BPDU) を受信すると、 そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU (バージョン 3)、または RSTP BPDU (バージョン 2) を受信することによって、ポートがリージョンの境界に位置していることを検出でき ます。

ただし、レガシー スイッチが指定スイッチでない場合、レガシー スイッチがリンクから削除されてい るかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動 的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合 であっても、引き続きポートに境界の役割を指定する可能性があります。プロトコル移行プロセスを再 起動する(近接スイッチとの再ネゴシエーションを強制する)には、clear spanning-tree detected-protocols 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシー スイッチが RSTP スイッチであれば、これらのスイッチは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP スイッチは、バージョン 0 コンフィギュ レーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポートで送信します。境 界ポートは、指定スイッチがシングル スパニング ツリー スイッチまたは異なる MST コンフィギュ レーションを持つスイッチのいずれかである LAN に接続されます。

RSTP の概要

RSTP は、ポイントツーポイントの配線を利用して、スパニング ツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパニング ツリーを再構成できます(IEEE 802.1D スパニング ツリーのデフォルトに設定されている 50 秒とは異なります)。

ここでは、RSTP の機能について説明します。

- 「ポートの役割およびアクティブ トポロジ」(P.17-9)
- 「高速コンバージェンス」(P.17-10)
- 「ポートの役割の同期化」(P.17-12)
- 「BPDUのフォーマットおよびプロセス」(P.17-13)

設定については、「MSTP 機能の設定」(P.17-15)を参照してください。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブトポロジを学習することによって高速コンバー ジェンスを実現します。「スパニング ツリートポロジと BPDU」(P.16-3) で説明したように、RSTP は、IEEE 802.1D STP に基づき、スイッチ プライオリティが最も高い(プライオリティの値が最も小 さい) スイッチをルート スイッチに選択します。RSTP はさらに、各ポートに次のいずれか1つの役割 を割り当てます。

- ルートポート:スイッチからルートスイッチへパケットを転送する場合の最適パス(最も低コストなパス)を提供します。
- 指定ポート:指定スイッチに接続します。これにより、LAN からルート スイッチへパケットを転送するときのパス コストが最小になります。指定スイッチが LAN に接続するポートのことを指定ポートと呼びます。

- 代替ポート:現在のルートポートが提供したパスに代わるルートスイッチへの代替パスを提供します。
- バックアップポート:指定ポートが提供した、スパニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップポートが存在できるのは、2つのポートがポイントツーポイントリンクよってループバックで接続されている場合、または1つのスイッチに共有LANセグメントへの接続が2つ以上ある場合です。
- ディセーブル ポート:スパニング ツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートの役割を割り当てられたポートは、アクティブ トポロジの一部となり ます。代替ポートまたはバックアップ ポートの役割を割り当てられたポートは、アクティブ トポロジ から除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTP は、すべてのルート ポートおよび指定ポートがただちにフォワーディングステートに移行し、代替ポートとバックアップ ポートが必ず廃棄ステート(IEEE 802.1Dのブロッキングステートと同じ)になるように保証します。 フォワーディングプロセスおよびラーニングプロセスの動作はポートステートによって制御されま す。表 17-2 に、IEEE 802.1D と RSTP のポートステートの比較を示します。

表 17-2	ポート ステートの比較
--------	-------------

動作ステータス	STP ポート ステー ト(IEEE 802.1D)	RSTP ポート ス テート	ポートが アクティブ トポロジに含まれて いるか
イネーブル	ブロッキング	廃棄	なし
イネーブル	リスニング	廃棄	なし
イネーブル	ラーニング	ラーニング	あり
イネーブル	フォワーディング	フォワーディング	あり
ディセーブル	ディセーブル	廃棄	なし

シスコの STP 実装製品内で整合性を図るため、このマニュアルでは、ポートの*廃棄*ステートをブロッ キングと定義しています。指定ポートは、リスニング ステートから開始します。

高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチ ポート、または LAN に障害が発生しても、ただちに接続を 回復できます。RSTP は、エッジ ポート、新しいルート ポート、およびポイントツーポイント リンク で接続されているポートに次のような高速コンバージェンスを提供します。

- エッジポート: spanning-tree portfast インターフェイス コンフィギュレーション コマンドを使用して、RSTP スイッチ上の1つのポートをエッジポートに設定すると、そのエッジポートはただちにフォワーディング ステートになります。エッジポートは PortFast 対応ポートと同じで、これをイネーブルにできるのは、単一のエンド ステーションに接続されているポート上だけです。
- ルートポート: RSTPは、新しいルートポートを選択すると、古いルートポートをブロックして、 新しいルートポートをただちにフォワーディングステートにします。

 ポイントツーポイントリンク:2つのポートをポイントツーポイントリンクで接続し、ローカル ポートが指定ポートになると、その指定ポートは、提案/合意ハンドシェイクを使用して、相手側 ポートと高速移行をネゴシエーションし、ループのないトポロジを保証します。

図 17-4 では、スイッチ A とスイッチ B はポイントツーポイント リンクを通じて接続され、すべて のポートがブロッキング ステートになっています。スイッチ A のプライオリティ値がスイッチ B のプライオリティ値より小さい数値である場合、スイッチ A はスイッチ B に提案メッセージ(提 案フラグが設定されたコンフィギュレーション BPDU)を送信し、スイッチ A 自身が指定スイッ チになることを提案します。

スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルート ポートとして選択し、すべての非エッジ ポートをブロッキング ステートにします。さらに、新し いルート ポート経由で合意メッセージ(合意フラグが設定された BPDU)を送信します。

スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォ ワーディング ステートにします。スイッチ B はその非エッジ ポートをすべてブロックし、またス イッチ A とスイッチ B はポイントツーポイント リンクで接続されているので、ネットワークに ループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイク メッセージが交換されます。 スイッチ C はスイッチ B に接続されたポートをルート ポートとして選択し、両端のポートはただ ちにフォワーディング ステートに移行します。アクティブ トポロジにスイッチが追加されるたび に、このハンドシェイク プロセスが実行されます。ネットワークが収束すると、この提案/合意ハ ンドシェイクがルートからスパニング ツリーのリーフへと進みます。

スイッチはポートのデュプレックス モードによってリンク タイプを学習します。全二重ポートは ポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。spanning-tree link-type インターフェイス コンフィギュレーション コマンドを使用すると、デュプレックス設定 で制御されたデフォルトの設定値を上書きできます。



図 17-4 高速コンバージェンスの提案/合意ハンドシェイク

ポートの役割の同期化

スイッチのポートの1つで提案メッセージが受信され、そのポートが新しいルート ポートに選択されると、RSTP は他のすべてのポートを新しいルートの情報に同期させます。

他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期 化されます。スイッチ上の個々のポートは次の場合に同期化された状態となります。

- ブロッキング ステートである場合
- エッジ ポートである場合(ネットワークのエッジとして設定されているポート)

指定ポートがフォワーディングステートであり、なおかつエッジポートとして設定されていない場合、 RSTPによって新しいルート情報で強制的に同期化されると、その指定ポートはブロッキングステートになります。一般的に、RSTPがポートを新しいルート情報で強制的に同期化する場合に、そのポートが上記のいずれの条件も満たしていない場合、ポートのステートはブロッキングに設定されます。

スイッチは、すべてのポートが同期化されたことを確認すると、そのルート ポートに対応する指定ス イッチに合意メッセージを送信します。ポイントツーポイント リンクで接続されたスイッチがポート の役割について互いに合意すると、RSTP はポート ステートをただちにフォワーディング ステートに 移行させます。図 17-5 は、この一連のイベントを示します。

図 17-5 高速コンパージェンス中の一連のイベント



BPDU のフォーマットおよびプロセス

RSTP BPDU のフォーマットは、プロトコル バージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい1 バイトのバージョン1の Length フィールドは0 に設定さ れます。これはバージョン1のプロトコルの情報がないことを示しています。表 17-3 に、RSTP のフ ラグ フィールドを示します。

ビット	機能
0	トポロジの変更 (TC)
1	提案
$2\sim3$:	ポートの役割:
00	不明
01	代替ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジの変更の確認 (TCA)

表 17-3 RSTP BPDU フラグ

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定しま す。提案メッセージでは、ポートの役割は常に指定ポートに設定されます。

送信スイッチは、提案を受け入れる場合、RSTP BPDU に合意フラグを設定します。合意メッセージでは、ポートの役割は常にルート ポートに設定されます。

RSTP には個別の Topology Change Notification (TCN; トポロジ変更通知) BPDU はありません。ト ポロジの変更を示すには、トポロジ変更(TC) フラグが使用されます。ただし、IEEE 802.1D スイッ チとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニングとフォワーディングのフラグは、送信ポートのステートに応じて設定されます。

優位 BPDU 情報の処理

現在保存されているルート情報よりも優位のルート情報(小さいスイッチ ID、低パス コストなど)を ポートが受信すると、RSTP は再構成を開始します。そのポートが新しいルート ポートとして提案さ れ、選択されると、RSTP は他のすべてのポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポート を同期化したあと、合意メッセージを送信します。BPDU が IEEE 802.1D BPDU である場合、スイッ チは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルート ポートは フォワーディング ステートに移行するために 2 倍の転送遅延時間を必要とします。

ポートで優位の情報が受信されたために、そのポートがバックアップ ポートまたは代替ポートになる 場合、RSTP はそのポートをブロッキング ステートに設定し、合意メッセージは送信しません。指定 ポートは、転送遅延タイマーが満了するまで提案フラグの設定された BPDU の送信を続けます。タイ マーが満了すると、ポートはフォワーディング ステートに移行します。

下位 BPDU 情報の処理

指定ポートの役割フラグが設定された下位 BPDU(そのポートに現在保存されている値より大きいス イッチ ID、高いパス コストなど)を指定ポートが受信した場合、その指定ポートは、ただちに現在の 自身の情報を応答します。

トポロジの変更

ここでは、スパニング ツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出:IEEE 802.1D ではブロッキングとフォワーディングステート間でのすべての移行によって トポロジの変更が生じますが、RSTP ではトポロジの変更が生じるのは、ブロッキングからフォ ワーディングにステートが移行する場合のみです(トポロジの変更と見なされるのは、相互接続性 が向上する場合だけです)。エッジポートでステートが変更されても、トポロジの変更は生じませ ん。RSTP スイッチは、トポロジの変更を検出すると、そのスイッチのすべての非エッジポート (TC 通知を受信したポートを除く)で学習した情報を削除します。
- 通知: IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行い ます。
- 確認: RSTP スイッチは、指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルート ポートで TC 時間タイマー(IEEE 802.1D のトポロジ変更タイマーと同じ)がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

この処理は、IEEE 802.1D スイッチをサポートする目的でのみ必要とされます。RSTP BPDU では、TCA ビットは設定されません。

- 伝播:RSTP スイッチは、指定ポートまたはルート ポートを介して別のスイッチからTCメッセージを受信すると、自身のすべての非エッジ ポート、指定ポート、およびルート ポート(このTCメッセージを受信したポートを除く)に変更を伝播します。スイッチは、これらのすべてのポートのTC時間タイマーを起動し、これらのポート上で学習した情報を削除します。
- プロトコルの移行: IEEE 802.1D スイッチとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

ポートが初期化されると、移行遅延タイマーが起動され(RSTP BPDU を送信する最小時間を指定)、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコル タイプを無視します。

スイッチはポートの移行遅延タイマーが満了したあとに IEEE 802.1D BPDU を受信した場合、 IEEE 802.1D スイッチに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。 ただし、RSTP スイッチが 1 つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了 したあとに RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使 用が開始されます。

MSTP 機能の設定

ここでは、次の設定情報について説明します。

- 「MSTP のデフォルト設定」(P.17-15)
- 「MSTP 設定時の注意事項」(P.17-16)
- 「MST リージョンの設定および MSTP のイネーブル化」(P.17-16)(必須)
- 「ルートスイッチの設定」(P.17-18)(任意)
- 「セカンダリルートスイッチの設定」(P.17-20)(任意)
- 「ポート プライオリティの設定」(P.17-21)(任意)
- 「パスコストの設定」(P.17-22)(任意)
- 「スイッチ プライオリティの設定」(P.17-23)(任意)
- 「Hello タイムの設定」(P.17-24)(任意)
- 「転送遅延時間の設定」(P.17-24)(任意)
- 「最大エージングタイムの設定」(P.17-25)(任意)
- 「最大ホップカウントの設定」(P.17-25)(任意)
- 「リンクタイプの指定による高速移行の保証」(P.17-26)(任意)
- 「ネイバタイプの指定」(P.17-27)(任意)
- •「プロトコル移行プロセスの再起動」(P.17-27)(任意)

MSTP のデフォルト設定

表 17-4 に、MSTP のデフォルト設定を示します。

表 17-4 MSTP のデフォルト設定

機能	デフォルト設定
スパニング ツリー モード	PVST+(Rapid PVST+ と MSTP はディセーブ ル)
スイッチ プライオリティ(CIST ポート単位で設定可能)	32768
スパニング ツリー ポート プライオリティ (CIST ポート単位で設定可能)	128
スパニング ツリー ポート コスト(CIST ポート単位で設定可能)	1000 Mbps : 4
	100 Mbps : 19
	10 Mbps : 100
ハロータイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

サポートされるスパニング ツリー インスタンス数については、「サポートされるスパニング ツリー インスタンス」(P.16-11)を参照してください。

MSTP 設定時の注意事項

ここでは、MSTP の設定時の注意事項を説明します。

- spanning-tree mode mst グローバル コンフィギュレーション コマンドを使用して、MST をイ ネーブルにすると、RSTP が自動的にイネーブルになります。
- 2つ以上のスイッチを同じ MST リージョンに設定するには、その2つのスイッチに同じ VLAN/インスタンスマッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- スイッチは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピン グできる VLAN の数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは1つの バージョンだけです(たとえば、すべてのVLANでPVST+を使用するか、すべてのVLANで Rapid PVST+を使用するか、またはすべてのVLANでMSTPを使用することになります)。詳細 については、「スパニングツリーの相互運用性と下位互換性」(P.16-12)を参照してください。推 奨するトランクポート設定の詳細については、「他の機能との相互作用」(P.13-16)を参照してく ださい。
- MST コンフィギュレーションの VLAN Trunking Protocol (VTP; VLAN トランキング プロトコ ル) 伝播機能はサポートされません。ただし、CLI または SNMP(簡易ネットワーク管理プロト コル) サポートを通じて、MST リージョン内の各スイッチで MST コンフィギュレーション (リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング)を手動で設定する ことは可能です。
- ネットワーク内の冗長パスでロードバランシングを機能させるには、すべての VLAN/インスタン スマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラ フィックが1つのリンク上で伝送されます。
- PVST+クラウドとMSTクラウドの間、またはRapid PVST+クラウドとMSTクラウドの間で ロードバランシングを実現するには、すべてのMST境界ポートがフォワーディングステートでな ければなりません。そのためには、MSTクラウドのISTマスターがCSTのルートを兼ねている必 要があります。MSTクラウドが複数のMSTリージョンで構成されている場合は、MSTリージョ ンの1つにCSTルートが含まれており、他のすべてのMSTリージョンにおいて、MSTクラウド に含まれているルートへのパスの方がPVST+またはRapid PVST+クラウド経由のパスよりも優 れている必要があります。クラウド内のスイッチを手動で設定しなければならない場合もありま す。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ2デバイスで相互接続された小規模なLAN に分割することを推奨します。
- UplinkFast および BackboneFast に関する設定時の注意事項については、「オプションのスパニン グ ツリー設定時の注意事項」(P.18-11)を参照してください。

MST リージョンの設定および MSTP のイネーブル化

2 つ以上のスイッチを同じ MST リージョンに設定するには、その 2 つのスイッチに同じ VLAN/イン スタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなり ません。 リージョンは、同じ MST コンフィギュレーションを持つ1 つまたは複数のメンバーで構成されます。 リージョンの各メンバーは RSTP BPDU を処理する機能を備えている必要があります。ネットワーク 内の MST リージョンの数には制限はありませんが、各リージョンがサポートできるスパニング ツリー インスタンスの数は 65 までです。VLAN には、一度に1 つのスパニング ツリー インスタンスのみ割 り当てることができます。

MST リージョンの設定を行い、MSTP をイネーブルにするには、特権 EXEC モードで次の手順を実行 します。この手順は必須です。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	spanning-tree mst configuration	MST コンフィギュレーション モードを開始します。	
ステップ 3	instance instance-id vlan vlan-range	VLAN を MST インスタンスに対応付けます。	
		 instance-id に指定できる範囲は、0~4094です。 	
		 vlan vlan-range に指定できる範囲は、1~4094です。 	
		MST インスタンスに VLAN をマッピングする場合、マッピング はインクリメンタルに行われ、コマンドで指定された VLAN が すでにマッピング済みの VLAN に対して追加または削除されま す。	
		VLAN の範囲を指定する場合は、ハイフンを使用します。たとえば、 instance 1 vlan 1-63 と入力すると、VLAN 1 ~ 63 が MST インスタ ンス 1 にマッピングされます。	
		一連の VLAN を指定する場合は、カンマを使用します。たとえば、 instance 1 vlan 10, 20, 30 と入力すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。	
ステップ 4	name name	コンフィギュレーション名を指定します。name ストリングの最大長は 32 文字で、大文字と小文字が区別されます。	
ステップ 5	revision version	コンフィギュレーション リビジョン番号を指定します。指定できる 範囲は 0 ~ 65535 です。	
ステップ 6	show pending	入力した設定を表示して、確認します。	
ステップ 7	exit	変更を適用し、グローバル コンフィギュレーション モードに戻りま す。	
ステップ 8	spanning-tree mode mst	MSTP をイネーブルにします。RSTP もイネーブルになります。	
		 ▲ 注意 スパニング ツリー モードを変更すると、すべてのスパニング ツリー インスタンスが前のモードで停止して新しいモードで再起動されるので、トラフィックが中断する可能性があります。 	
		MISIF と FVSI+ または MISIF と Kapid FVSI+ を回時に美行することはできません。	
ステップ 9	end	特権 EXEC モードに戻ります。	
ステップ 10	show running-config	設定を確認します。	
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

デフォルトの MST リージョン コンフィギュレーションに戻すには、no spanning-tree mst configuration グローバル コンフィギュレーション コマンドを使用します。VLAN インスタンス マッ ピングをデフォルトの設定に戻すには、no instance *instance-id* [vlan vlan-range] MST コンフィギュレーション コマンドを使用します。デフォルトの名前に戻すには、no name MST コンフィギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、no revision MST コンフィ ギュレーション コマンドを使用します。デフォルトのリビジョン番号に戻すには、no revision MST コンフィ ジョンロマンドを使用します。デフォルトのリビジョン番号に戻すには、no spanning-tree mode または spanning-tree mode pyst グローバル コンフィギュレーション コマンドを使用します。

次に、MST コンフィギュレーション モード4の例を示します。まず MST コンフィギュレーション モードを開始して VLAN 10 ~ 20 を MST インスタンス 1 にマッピングし、そのリージョンの名前を region1 に設定します。次にコンフィギュレーション リビジョン番号として 1 を設定し、入力した設定 を表示させて変更を適用します。そして最後にグローバル コンフィギュレーション モードに戻ります。

```
Switch(config) # spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst) # revision 1
Switch(config-mst) # show pending
Pending MST configuration
Name
        [region1]
Revision 1
Instance Vlans Mapped
_____
         _____
0
        1-9,21-4094
        10-20
1
```

Switch(config-mst)# exit
Switch(config)#

ルート スイッチの設定

スイッチは、スパニング ツリー インスタンスを VLAN グループとマッピングして維持します。各イン スタンスには、スイッチ プライオリティとスイッチの MAC アドレスからなるスイッチ ID が対応付け られます。最小のスイッチ ID を持つスイッチがその VLAN グループのルート スイッチになります。

特定のスイッチがルートになるように設定するには、spanning-tree mst instance-id root グローバル コンフィギュレーション コマンドを使用して、スイッチ プライオリティをデフォルト値(32768)か らきわめて小さい値に変更します。これにより、そのスイッチが指定されたスパニング ツリー インス タンスのルート スイッチになることができます。このコマンドを入力すると、スイッチは、ルート ス イッチのスイッチ プライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定 されたインスタンスについて、自身のプライオリティを 24576 に設定します(この値によって、この スイッチが指定されたスパニング ツリー インスタンスのルートになる場合)。

指定されたインスタンスのルート スイッチに 24576 より小さいスイッチ プライオリティが設定されて いる場合、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値 に設定します (表 16-1 (P.16-4)に示すように、4096 は 4 ビットのスイッチ プライオリティ値の最下 位ビットの値です)。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合 は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張シ ステム ID によって、旧ソフトウェアが稼動する接続スイッチのプライオリティより VLAN 番号が大 きくなるたびに、スイッチ プライオリティ値が増大します。

各スパニング ツリー インスタンスのルート スイッチは、バックボーン スイッチまたはディストリ ビューション スイッチにする必要があります。アクセス スイッチをスパニング ツリーのプライマリ ルートとして設定しないでください。 レイヤ2ネットワークの直径(つまり、レイヤ2ネットワーク上の任意の2つのエンドステーション 間の最大スイッチホップ数)を指定するには、diameterキーワードを指定します(MST インスタン ス0の場合のみ使用可)。ネットワークの直径を指定すると、その直径のネットワークに最適な ハロー タイム、転送遅延時間、および最大エージング タイムをスイッチが自動的に設定するので、コンバー ジェンスの所要時間を大幅に短縮できます。自動的に算出された Hello タイムを変更する場合は、 hello キーワードを使用します。

(注)

スイッチをルート スイッチとして設定したあとに、spanning-tree mst hello-time、spanning-tree mst forward-time、および spanning-tree mst max-age グローバル コンフィギュレーション コマンドを使用して、ハロー タイム、転送遅延時間、最大エージング タイムを手動で設定することは推奨できません。

スイッチをルートスイッチに設定するには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst <i>instance-id</i> root primary [diameter <i>net-diameter</i> [hello-time <i>seconds</i>]]	 スイッチをルートスイッチに設定します。 <i>instance-id</i>には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 (任意) diameter net-diameter には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。
		 指定でざる範囲は2~7です。このキーリードを使用できるのは MST インスタンス 0 の場合だけです。 (任意) hello-time seconds には、ルート スイッチによってコンフィギュレーション メッセージが生成される間隔を秒数で指定します。指定できる範囲は1~10秒です。デフォルトは2秒です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst instance-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst *instance-id* root グローバル コンフィ ギュレーション コマンドを使用します。

セカンダリ ルート スイッチの設定

拡張システム ID をサポートするスイッチをセカンダリルートとして設定すると、スイッチ プライオリ ティはデフォルト値(32768)から 28672 に変更されます。その結果、プライマリ ルート スイッチに 障害が発生した場合に、このスイッチが、指定されたインスタンスのルート スイッチになる可能性が 高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を 使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。 spanning-tree mst *instance-id* root primary グローバル コンフィギュレーション コマンドでプライマ リ ルート スイッチを設定したときと同じネットワーク直径および ハロー タイム値を使用してくださ い。

スイッチをセンカンダリ ルート スイッチに設定するには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst instance-id root secondary [diameter net-diameter [hello-time seconds]]	 スイッチをセカンダリ ルート スイッチに設定します。 <i>instance-id</i>には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 (任意) diameter net-diameter には、任意の 2 つのエンドステーション間の最大スイッチ数を指定します。指定できる範囲は 2 ~ 7 です。このキーワードを使用できるのは MST インスタンス 0 の場合だけです。
		 (任意) hello-time seconds には、ルート スイッチによって コンフィギュレーション メッセージが生成される間隔を秒数 で指定します。指定できる範囲は 1 ~ 10 秒です。デフォル トは 2 秒です。
		プライマリ ルート スイッチを設定したときと同じネットワーク 直径および Hello タイム値を使用してください。「ルート スイッ チの設定」(P.17-18)を参照してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst instance-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst *instance-id* root グローバル コンフィ ギュレーション コマンドを使用します。
ポート プライオリティの設定

ループが発生した場合、MSTP はポート プライオリティを使用して、フォワーディング ステートにす るインターフェイスを選択します。最初に選択させたいインターフェイスには高いプライオリティ(小 さい数値)を与え、最後に選択させたいインターフェイスには低いプライオリティ(大きい数値)を与 えます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTP はイン ターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイ スをブロックします。

インターフェイスの MSTP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイ ス コンフィギュレーション モードを開始します。
		有効なインターフェイスには、物理ポートとポート チャネル論理インターフェイスがあります。ポート チャネルの範囲は 1 ~ 6 です。
ステップ 3	spanning-tree mst instance-id port-priority	ポート プライオリティを設定します。
	priority	 instance-id には、単一のインスタンス、ハイフン で区切られた範囲のインスタンス、またはカンマで 区切られた一連のインスタンスを指定できます。指 定できる範囲は 0 ~ 4094 です。
		 priorityに指定できる範囲は0~240で、16ずつ増加します。デフォルト値は128です。値が小さいほど、プライオリティは高くなります。
		プライオリティ値は、0、16、32、48、64、80、 96、112、128、144、160、176、192、208、224、 および 240 です。その他の値はすべて拒否されま す。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show spanning-tree mst interface interface-id	設定を確認します。
	または	
	show spanning-tree mst instance-id	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存 します。

<u>》</u> (注)

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンク アップ動作可能状態のポートの情報だけです。それ以外の情報については、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、no spanning-tree mst *instance-id* port-priority イン ターフェイス コンフィギュレーション コマンドを使用します。

パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生 した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択し ます。最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインター フェイスには大きいコスト値を与えます。すべてのインターフェイスに同じコスト値が与えられている 場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、 他のインターフェイスをブロックします。

インターフェイスの MSTP コストを設定するには、特権 EXEC モードで次の手順を実行します。この 手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。有効なインター フェイスには、物理ポートとポート チャネル論理インター フェイスがあります。ポート チャネルの範囲は 1 ~ 6 です。
ステップ 3	spanning-tree mst instance-id cost cost	コストを設定します。
		ループが発生した場合、MSTP はパス コストを使用して、 フォワーディング ステートにするインターフェイスを選択し ます。パス コストが小さいほど、高速で伝送されます。
		 instance-id には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた 一連のインスタンスを指定できます。指定できる範囲は0 ~ 4094 です。
		 cost に指定できる範囲は1~20000000です。デフォル ト値はインターフェイスのメディア速度に基づきます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show spanning-tree mst interface <i>interface-id</i>	設定を確認します。
	または	
	show spanning-tree mst instance-id	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

(注)

show spanning-tree mst interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンク アップ動作可能状態のポートの情報だけです。それ以外の情報については、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

インターフェイスをデフォルト設定に戻すには、no spanning-tree mst *instance-id* cost インターフェ イス コンフィギュレーション コマンドを使用します。

スイッチ プライオリティの設定

スイッチ プライオリティを設定して、スイッチがルート スイッチとして選択される可能性を高めるこ とができます。

(注)

このコマンドは、十分に注意して使用してください。スイッチ プライオリティの変更には、通常は、 spanning-tree vlan *vlan-id* root primary および spanning-tree vlan *vlan-id* root secondary グローバ ル コンフィギュレーション コマンドを使用することを推奨します。

スイッチ プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst instance-id priority priority	スイッチ プライオリティを設定します。
		 instance-id には、単一のインスタンス、ハイフンで 区切られた範囲のインスタンス、またはカンマで区切 られた一連のインスタンスを指定できます。指定でき る範囲は 0 ~ 4094 です。
		 priority を指定する場合、指定できる範囲は0~ 61440で、4096ずつ増加します。デフォルトは32768です。数値が小さいほど、スイッチがルートスイッチとして選択される可能性が高くなります。
		プライオリティ値は、0、4096、8192、12288、 16384、20480、24576、28672、32768、36864、 40960、45056、49152、53248、57344、61440で す。その他の値はすべて拒否されます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst instance-id	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst *instance-id* priority グローバル コン フィギュレーション コマンドを使用します。

Hello タイムの設定

Hello タイムを変更することによって、ルート スイッチによってコンフィギュレーション メッセージ が生成される間隔を設定できます。

すべての MST インスタンスの ハロー タイムを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst hello-time seconds	すべての MST インスタンスの ハロー タイムを設定しま す。ハロー タイムはルート スイッチがコンフィギュレー ション メッセージを生成する間隔です。これらのメッセー ジは、スイッチがアクティブであることを意味します。 seconds に指定できる範囲は 1 ~ 10 です。デフォルト値は 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst hello-time グローバル コンフィギュ レーション コマンドを使用します。

転送遅延時間の設定

すべての MST インスタンスの転送遅延時間を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst forward-time seconds	すべての MST インスタンスの転送遅延時間を設定します。転 送遅延時間は、スパニング ツリー ラーニング ステートおよび リスニング ステートからフォワーディング ステートに移行す るまでに、ポートが待機する秒数です。
		<i>seconds</i> に指定できる範囲は 4 ~ 30 です。デフォルト値は 15 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst forward-time グローバル コンフィギュ レーション コマンドを使用します。

最大エージング タイムの設定

すべての MST インスタンスの最大エージング タイムを設定するには、特権 EXEC モードで次の手順 を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst max-age seconds	すべての MST インスタンスの最大エージング タイムを設定 します。最大エージング タイムは、再構成を試行するまで にスイッチがスパニング ツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。 seconds に指定できる範囲は 6 ~ 40 です。デフォルト値は 20 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

スイッチをデフォルト設定に戻すには、no spanning-tree mst max-age グローバル コンフィギュレー ション コマンドを使用します。

最大ホップ カウントの設定

すべての MST インスタンスの最大ホップ カウントを設定するには、特権 EXEC モードで次の手順を 実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree mst max-hops hop-count	BPDU が廃棄され、ポートに維持されていた情報が期限切れになるまでの、リージョン内でのホップ数を指定します。
		<i>hop-count</i> に指定できる範囲は 1 ~ 255 です。デフォルト値は 20 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree mst	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻すには、no spanning-tree mst max-hops グローバル コンフィギュレー ション コマンドを使用します。

リンク タイプの指定による高速移行の保証

2 つのポートをポイントツーポイント リンクで接続し、ローカル ポートが指定ポートになると、RSTP は提案/合意ハンドシェイクを使用して、相手側ポートと高速移行をネゴシエーションし、ループのな いトポロジを保証します(「高速コンバージェンス」(P.17-10)を参照)。

デフォルトでは、リンク タイプは、インターフェイスのデュプレックス モードによって制御されます。 全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。MSTP が稼動しているリモート スイッチ上の1 つのポートと物理的にポイントツーポイントで接続されてい る半二重リンクが存在する場合は、リンク タイプのデフォルト設定値を変更して、フォワーディング ステートへの高速移行をイネーブルにできます。

リンクタイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
プ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
プ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コ ンフィギュレーション モードを開始します。有効なイン
		ターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範 囲は $1 \sim 4094$ です。ポート チャネルの範囲は $1 \sim 6$ です。
プ 3	spanning-tree link-type point-to-point	ポートのリンク タイプをポイントツーポイントに指定しま す。
プ4	end	特権 EXEC モードに戻ります。
プ 5	show spanning-tree mst interface interface-id	設定を確認します。
プ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

ポートをデフォルト設定に戻すには、no spanning-tree link-type インターフェイス コンフィギュレー ション コマンドを使用します。

ネイバ タイプの指定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることが できます。デフォルトでは、ポートは自動的に先行標準のデバイスを検出します。ただし、ポート自体 は、標準と先行標準の BPDU を両方受信できます。デバイスとネイバの間に不一致があれば、CIST の みがインターフェイス上で動作します。

ポートを選択して、先行標準の BPDU のみ送信するように設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての show コマンドで表示されます。

リンクタイプのデフォルト設定を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コ ンフィギュレーション モードを開始します。指定できるイ ンターフェイスとして、物理ポートも含まれます。
ステップ 3	spanning-tree mst pre-standard	先行標準の BPDU のみ送信するようにポートを指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show spanning-tree mst interface interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

ポートをデフォルト設定に戻すには、no spanning-tree mst prestandard インターフェイス コンフィ ギュレーション コマンドを使用します。

プロトコル移行プロセスの再起動

MSTP が稼動しているスイッチは、IEEE 802.1D 準拠のレガシー スイッチとの相互運用を可能にする 組み込み型のプロトコル移行メカニズムをサポートします。このスイッチは、レガシー IEEE 802.1D コンフィギュレーション BPDU(プロトコルバージョンが 0 に設定されている BPDU)を受信すると、 そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP スイッチは、レガシー BPDU、別のリージョンに関連付けられている MST BPDU(バージョン 3)、または RST BPDU (バージョン 2)を受信することによって、ポートがリージョンの境界に位置していることを検出でき ます。

ただし、レガシー スイッチが指定スイッチでない場合、レガシー スイッチがリンクから削除されてい るかどうか検出できないので、スイッチは IEEE 802.1D BPDU を受け取らなくなった場合でも、自動 的に MSTP モードには戻りません。さらにスイッチは、接続先スイッチがリージョンに加入した場合 であっても、ポートに対して引き続き、境界の役割を割り当てる可能性もあります。

スイッチでプロトコル移行プロセスを再起動する(近接スイッチとの再ネゴシエーションを強制する) には、clear spanning-tree detected-protocols 特権 EXEC コマンドを使用します。

特定のインターフェイスでプロトコル移行プロセスを再開するには、clear spanning-tree detected-protocols interface *interface-id* 特権 EXEC コマンドを使用します。

MST コンフィギュレーションおよびステータスの表示

スパニングツリー ステータスを表示するには、表 17-5 の特権 EXEC コマンドを1つまたは複数使用します。

表 17-5 MST ステータスを表示するコマンド

コマンド	目的
show spanning-tree mst configuration	MST リージョン コンフィギュレーションを表示します。
show spanning-tree mst configuration digest	現在の MSTCI に含まれている Message Digest 5 (MD5) ダイジェストを 表示します。
show spanning-tree mst instance-id	特定のインスタンスの MST 情報を表示します。
show spanning-tree mst interface interface-id	特定のインターフェイスの MST 情報を表示します。

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。





オプションのスパニング ツリー機能の設定

この章では、Catalyst 2960 スイッチにオプションのスパニング ツリー機能を設定する方法について説 明します。スイッチが Per-VLAN Spanning-Tree Plus (PVST+) を実行している場合、これらのすべ ての機能を設定できます。スイッチが Multiple Spanning-Tree Protocol (MSTP) または Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルを稼動している場合は、明記した機能のみ を設定できます。

PVST+および Rapid PVST+の詳細については、第16章「STP の設定」を参照してください。MSTP の詳細および複数の VLAN を同一スパニング ツリー インスタンスにマッピングする方法については、 第17章「MSTP の設定」を参照してください。

(注)

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

この章で説明する内容は、次のとおりです。

- 「オプションのスパニング ツリー機能の概要」(P.18-1)
- 「オプションのスパニング ツリー機能の設定」(P.18-10)
- 「スパニング ツリー ステータスの表示」(P.18-19)

オプションのスパニング ツリー機能の概要

ここでは、次の概要について説明します。

- 「PortFast の概要」(P.18-2)
- 「BPDU ガードの概要」(P.18-3)
- 「BPDU フィルタリングの概要」(P.18-3)
- 「UplinkFast の概要」(P.18-4)
- 「BackboneFast の概要」(P.18-6)
- 「EtherChannel ガードの概要」(P.18-8)
- 「ルート ガードの概要」(P.18-8)
- 「ループガードの概要」(P.18-10)

PortFast の概要

PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインター フェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートか ら直接フォワーディング ステートに移行します。単一のワークステーションまたはサーバに接続され たインターフェイス上で PortFast を使用すると、スパニング ツリーが収束するのを待たずにデバイス をただちにネットワークに接続できます(図 18-1を参照)。

1 台のワークステーションまたはサーバに接続されたインターフェイスが Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)を受信しないようにする必要があります。スイッチを 再起動すると、PortFast がイネーブルに設定されているインターフェイスは通常のスパニング ツリー ステータスの遷移をたどります。



PortFast の目的は、インターフェイスがスパニング ツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はエンドステーションに接続されたインターフェイス上で使用する場合にのみ有効になります。他のスイッチに接続するインターフェイスで PortFast をイネーブルにすると、スパニング ツリーのループが生じる可能性があります。

この機能をイネーブルにするには、spanning-tree portfast インターフェイス コンフィギュレーション コマンド、または spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用 します。



図 18-1 PortFast 対応インターフェイス

BPDU ガードの概要

BPDU ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルに することもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、spanning-tree portfast bpduguard default グローバル コンフィギュ レーション コマンドを使用して、PortFast 対応ポート上で BPDU ガードをイネーブルにできます。こ れらのポート上で BPDU が受信されると、スパニング ツリーは、PortFast で動作しているポートを シャットダウンします。設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、認可されていないデバイスの接続などの無効な設定が存在す ることを示しており、BPDU ガード機能によってポートは errdisable ステートになります。この状態に なると、スイッチは違反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、errdisable detect cause bpduguard shutdown vlan グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となってい る VLAN だけをシャットダウンします。

インターフェイス レベルの場合は、**PortFast 機能をイネーブルにしなくても**、spanning-tree bpduguard enable インターフェイス コンフィギュレーション コマンドを使用して、任意のポート上で BPDU ガードをイネーブルにできます。BPDU を受信したポートは、errdisable ステートになります。

手動でインターフェイスを再び動作させなければならないので、BPDU ガード機能は無効な設定に対 する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツ リーに参加しないようにするには、BPDU ガード機能を使用します。

BPDU フィルタリングの概要

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス 単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

グローバル レベルの場合は、spanning-tree portfast bpdufilter default グローバル コンフィギュレー ション コマンドを使用して、PortFast 対応インターフェイス上で BPDU フィルタリングをイネーブル にできます。このコマンドを使用すると、PortFast 動作ステートのインターフェイスは BPDU を送受 信できなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始 するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェ イスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリング をグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイス では PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

インターフェイス レベルの場合は、**PortFast 機能をイネーブルにしなくても**、spanning-tree bpdufilter enable インターフェイス コンフィギュレーション コマンドを使用して、任意のインター フェイス上で BPDU フィルタリングをイネーブルにできます。このコマンドを実行すると、インター フェイスは BPDU を送受信できなくなります。

注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェ イス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが 発生することがあります。

スイッチ全体または1つのインターフェイスで BPDU フィルタリング機能をイネーブルにできます。

UplinkFastの概要

階層型ネットワークに配置されたスイッチは、バックボーン スイッチ、ディストリビューション ス イッチ、およびアクセス スイッチに分類できます。図 18-2 に、ディストリビューション スイッチおよ びアクセス スイッチに少なくとも1つの冗長リンクが確保されている複雑なネットワークの例を示し ます。冗長リンクは、ループを防止するために、スパニング ツリーによってブロックされています。



[—] アクティブリンク

スイッチの接続が切断されると、スイッチはスパニング ツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニング ツリーが再設定された場合は、spanning-tree uplinkfast グローバル コンフィギュレーション コマンドを使用して UplinkFast をイネーブルにすることにより、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニング ツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

アクセス スイッチ

スパニング ツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマル チキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送 信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィッ クのバーストを制限できます (このパラメータはデフォルトで毎秒 150 パケットです)。ただし、0 を 入力すると、ステーション学習フレームが生成されないので、接続切断後スパニング ツリー トポロジ がコンバージェンスする速度が遅くなります。

(注)

UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのス イッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの 機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用 して、冗長レイヤ2リンク間でロードバランシングを実行します。アップリンク グループは、(VLAN ごとの)レイヤ2インターフェイスの集合であり、いかなるときも、その中の1つのインターフェイス 図 18-3

だけが転送を行います。具体的には、アップリンク グループは(転送を行う)ルート ポートと1組の ブロック ポートからなります (セルフ ループ ポートは除く)。アップリンク グループは、転送中のリ ンクで障害が発生した場合に、代替パスを提供します。

図 18-3 に、リンク障害が発生していないトポロジの例を示します。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。ス イッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。



直接リンク障害発生前の UplinkFast の例

C が、ルート ポートの現在アクティブ リンクである L2 でリンク障害(*直接*リンク障害)を検出する と、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニン グ ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます (図 18-4 を参照)。この切り替えに必要な時間は、約1~5秒です。



図 18-4 直接リンク障害発生後の UplinkFast の例

BackboneFast の概要

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害 に対応します。BackboneFast は、最大エージング タイマーを最適化します。最大エージング タイマー によって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御さ れます。スイッチが別のスイッチの指定ポートから下位 BPDU を受信した場合、BPDU は他のスイッ チでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFast はルートまでの別のパ スを見つけようとします。

BackboneFast をイネーブルにするには、spanning-tree backbonefast グローバル コンフィギュレー ション コマンドを使用します。スイッチ上のルート ポートまたはブロック インターフェイスが指定ス イッチから下位 BPDU を受信すると、BackboneFast が開始します。下位 BPDU は、ルート ブリッジ と指定スイッチの両方として宣言したスイッチを識別します。スイッチが下位 BPDU を受信した場合、 そのスイッチが直接接続されていないリンク (*間接*リンク)で障害が発生したことを意味します(指定 スイッチとルート スイッチ間の接続が切断されています)。スパニング ツリーのルールとして、 spanning-tree vlan vlan-id max-age グローバル コンフィギュレーション コマンドによって設定された

最大エージング タイムの間、スイッチは下位 BPDU を無視します。

スイッチは、ルート スイッチへの代替パスの有無を判別します。下位 BPDU がブロック インターフェ イスに到達した場合、スイッチ上のルート ポートおよび他のブロック インターフェイスがルート ス イッチへの代替パスになります (セルフループ ポートは、ルート スイッチへの代替パスとは見なされ ません)。下位 BPDU がルート ポートに到達した場合、すべてのブロック インターフェイスがルート スイッチへの代替パスになります。下位 BPDU がルート ポートに到達し、しかもブロック インター フェイスがない場合、スイッチはルート スイッチへの接続が切断されたものと見なし、ルート ポート の最大エージング タイムが経過するまで待ち、通常のスパニング ツリー ルールに従ってルート スイッ チになります。

スイッチが代替パスでルート スイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query (RLQ)要求を送信します。スイッチは、すべての代替パスに RLQ 要求を送信し、ネット ワーク内の他のスイッチからの RLQ 応答を待機します

ルートへの代替パスがまだ存在していると判断したスイッチは、下位 BPDU を受信したインターフェ イスの最大エージング タイムが経過するまで待ちます。ルート スイッチへのすべての代替パスが、ス イッチとルート スイッチ間の接続が切断されていることを示している場合、スイッチは RLQ 応答を受 信したインターフェイスの最大エージング タイムを満了させます。1 つまたは複数の代替パスからルー ト スイッチへ引き続き接続できる場合、スイッチは下位 BPDU を受信したすべてのインターフェイス を指定ポートにして、(ブロッキング ステートになっていた場合) ブロッキング ステートを解除し、リ スニング ステート、ラーニング ステートを経てフォワーディング ステートに移行させます。

図 18-5 に、リンク障害が発生していないトポロジの例を示します。ルート スイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。



図 18-6 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、その障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイス を、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。BackboneFast は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを設定します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。図 18-6 では、リンク L1 で障害が発生した場合 BackboneFast がどのようにトポロジを再構成する かを示します。



図 18-6 間接リンク障害発生後の BackboneFast の例

図 18-7 のように、新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定ス イッチ (スイッチ B) から下位 BPDU が届いていないので、BackboneFast はアクティブになりませ ん。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。 ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッ チであるスイッチ A への指定スイッチであることを学習します。



図 18-7 メディア共有型トポロジにおけるスイッチの追加

EtherChannel ガードの概要

EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を 検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方の デバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、 EtherChannel の両端でチャネルのパラメータが異なる場合にも、設定の矛盾が発生します。 EtherChannel 設定時の注意事項については、「EtherChannel 設定時の注意事項」(P.36-10) を参照して ください。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのイン ターフェイスを errdisable ステートにし、エラー メッセージを表示します。

spanning-tree etherchannel guard misconfig グローバル コンフィギュレーション コマンドを使用してこの機能をイネーブルにできます。

ルート ガードの概要

SP (サービス プロバイダー) のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多 く含まれている場合があります。このようなトポロジでは、に示すように、スパニング ツリーが再構 成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。図 18-8 この状況を 防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルー トガード機能をイネーブルに設定します。スパニング ツリーの計算によってカスタマー ネットワーク 内のインターフェイスがルート ポートとして選択されると、ルート ガードがそのインターフェイスを root-inconsistent (ブロッキング) ステートにして、カスタマーのスイッチがルート スイッチにならな いように、またはルートへのパスに組み込まれないようにします。

SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ (root-inconsistent ステートになり)、スパニング ツリーが新しいルート スイッチを選択します。カス タマーのスイッチがルート スイッチになることはなく、ルートへのパスに組み込まれることもありま せん。 スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定 ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree (IST) インスタ ンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロッ クされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定 を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するす べての VLAN にルート ガードが適用されます。VLAN は、MST インスタンスに対してグループ化さ れたあと、マッピングされます。

spanning-tree guard root インターフェイス コンフィギュレーション コマンドを使用してこの機能を イネーブルにできます。



図 18-8 サービス プロバイダー ネットワークのルート ガード



ループ ガードの概要

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害に よって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体でイネーブルに した場合に最も効果があります。ループ ガードによって、代替ポートおよびルート ポートが指定ポー トになることが防止され、スパニング ツリーがルート ポートまたは代替ポートで BPDU を送信するこ とはありません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドを使用してこの機能を イネーブルにできます。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループ ガードによって、代替 ポートおよびルート ポートが指定ポートになることが防止され、スパニング ツリーがルート ポートま たは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループ ガードによってすべての MST インスタンスでイ ンターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポー トでは、ループ ガードがすべての MST インスタンスでインターフェイスをブロックします。

オプションのスパニング ツリー機能の設定

ここでは、次の設定情報について説明します。

- 「オプションのスパニング ツリー機能のデフォルト設定」(P.18-11)
- 「オプションのスパニング ツリー設定時の注意事項」(P.18-11)
- 「PortFast のイネーブル化」(P.18-11)(任意)
- 「BPDU ガードのイネーブル化」(P.18-12)(任意)
- 「BPDU フィルタリングのイネーブル化」(P.18-14)(任意)
- 「冗長リンク用 UplinkFast のイネーブル化」(P.18-15)(任意)
- 「BackboneFast のイネーブル化」(P.18-16)(任意)
- 「EtherChannel ガードのイネーブル化」(P.18-16)(任意)
- 「ルートガードのイネーブル化」(P.18-17)(任意)
- 「ループガードのイネーブル化」(P.18-18)(任意)

オプションのスパニング ツリー機能のデフォルト設定

表 18-1 に、オプションのスパニング ツリー機能のデフォルト設定を示します。

表 18-1 オプションのスパニング ツリー機能のデフォルト設定

	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル(インターフェイス単位で個別に
	設正する場合を除く)
UplinkFast	グローバルにディセーブル
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル
ルート ガード	すべてのインターフェイスでディセーブル
ループ ガード	すべてのインターフェイスでディセーブル

オプションのスパニング ツリー設定時の注意事項

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、PortFast、BPDU ガード、 BPDU フィルタリング、EtherChannel ガード、ルート ガード、またはループ ガードを設定できます。

Rapid PVST+ または MSTP 用に、UplinkFast または BackboneFast 機能を設定できます。ただし、ス パニングツリー モードを PVST+ に変更するまで、この機能はディセーブル(非アクティブ)のままで す。

PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たず に、ただちにスパニング ツリー フォワーディング ステートに移行されます。

注意

PortFast を使用するのは、単一エンドステーションをアクセスポートまたはトランクポートに接続する場合に*限定*してください。スイッチまたはハブに接続するインターフェイス上でこの機能を イネーブルにすると、スパニング ツリーがネットワーク ループを検出または阻止できなくなり、その結果、ブロードキャストストームおよびアドレス学習の障害が起きる可能性があります。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。詳細は、第15章「音 声 VLAN の設定」を参照してください。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、この機能をイネーブルにできます。

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

	コマンド	目的
7 = 1		
ステッノイ	configure terminal	クローバルコンワイキュレーションモードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイスコン
		フィギュレーション モードを開始します。

	コマンド	目的			
ステップ 3	spanning-tree portfast [trunk]	単一ワークステーションまたはサーバに接続されたアクセス ポート上で PortFast をイネーブルにします。trunk キーワー ドを指定すると、トランク ポート上で PortFast をイネーブル にできます。			
		 (注) トランク ポート上で PortFast 機能をイネーブルにす る場合は、spanning-tree portfast trunk インター フェイス コンフィギュレーション コマンドを使用し なければなりません。spanning-tree portfast コマン ドは、トランク ポート上では機能しないためです。 			
		 ▲ 注意 トランク ポート上で PortFast をイネーブルにする 場合は、事前に、トランク ポートとワークステー ションまたはサーバの間にループがないことを確 認してください。 			
		デフォルトでは、PortFast はすべてのインターフェイスで ディセーブルです。			
ステップ 4	end	特権 EXEC モードに戻ります。			
ステップ 5	show spanning-tree interface interface-id portfast	設定を確認します。			
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。			

(注)

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての 非トランク ポート上で PortFast 機能をグローバルにイネーブルにできます。

PortFast 機能をディセーブルにする場合は、spanning-tree portfast disable インターフェイス コン フィギュレーション コマンドを使用します。

BPDU ガードのイネーブル化

PortFast 対応ポート (PortFast 動作ステートのポート) で BPDU ガードをグローバルにイネーブルに すると、スパニング ツリーは、そのポートでの動作を継続します。そのポートは、BPDU を受信しな ければ起動したままになります。

設定が有効であれば、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を 受信した場合は、認可されていないデバイスの接続などの無効な設定が存在することを示しており、 BPDU ガード機能によってポートは errdisable ステートになります。この状態になると、スイッチは違 反が発生したポート全体をシャットダウンします。

ポートをシャットダウンしないようにするには、errdisable detect cause bpduguard shutdown vlan グローバル コンフィギュレーション コマンドを使用して、違反が発生したポート上の原因となってい る VLAN だけをシャットダウンします。

手動でポートを再び動作させなければならないので、BPDU ガード機能は無効な設定に対する安全対策になります。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。



PortFast は、エンド ステーションに接続するポートに限って設定します。そうしないと、偶発的な トポロジループが原因でデータ パケット ループが発生し、スイッチおよびネットワークの動作が 妨げられることがあります。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コン フィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもで きます。BPDU を受信したポートは、errdisable ステートになります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、BPDU ガード機能をイネーブルにできます。

BPDU ガード機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree portfast bpduguard default	BPDU ガードをグローバルにイネーブルにします。
		BPDU ガードは、デフォルトではディセーブルに設定されてい ます。
ステップ 3	interface interface-id	エンド ステーションに接続するインターフェイスを指定し、 インターフェイス コンフィギュレーション モードを開始しま す。
ステップ 4	spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

BPDU ガードをディセーブルにするには、no spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を 上書きするには、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマン ドを使用します。

BPDU フィルタリングのイネーブル化

PortFast 対応インターフェイスで BPDU フィルタリングをグローバルにイネーブルにすると、PortFast 動作ステートのインターフェイスは BPDU を送受信できなくなります。ただし、リンクが確立してか らスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないよう にするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。 BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。



PortFast は、エンドステーションに接続するインターフェイスに限って設定します。そうしない と、偶発的なトポロジループが原因でデータパケットループが発生し、スイッチおよびネット ワークの動作が妨げられることがあります。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpdufilter enable** インターフェイス コン フィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネー ブルにすることもできます。このコマンドを実行すると、インターフェイスは BPDU を送受信できな くなります。

Æ 注意

BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェ イス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが 発生することがあります。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、BPDU フィルタリング機能 をイネーブルにできます。

BPDU フィルタリング機能をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree portfast bpdufilter default	BPDU フィルタリングをグローバルにイネーブルにします。
		BPDU フィルタリングは、デフォルトではディセーブルに設 定されています。
ステップ 3	interface interface-id	エンド ステーションに接続するインターフェイスを指定し、 インターフェイス コンフィギュレーション モードを開始しま す。
ステップ 4	spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

BPDU フィルタリングをディセーブルにする場合は、no spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドを使用します。

no spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdufilter enable** インターフェイス コンフィギュレーション コマンドを使用します。

冗長リンク用 UplinkFast のイネーブル化

スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチ プライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に no spanning-tree vlan vlan-id priority グローバル コンフィギュレーション コマンドを使用する ことによって、VLAN のスイッチ プライオリティをデフォルト値に戻す必要があります。

(注)

UplinkFast をイネーブルにすると、スイッチのすべての VLAN に影響します。個々の VLAN に UplinkFast を設定することはできません。

Rapid PVST+または MSTP 用に、UplinkFast 機能を設定できます。ただし、スパニングツリーモード を PVST+ に変更するまで、この機能はディセーブル(非アクティブ)のままです。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	spanning-tree uplinkfast [max-update-rate <i>pkts-per-second</i>]	 UplinkFast をイネーブルにします。 (任意) <i>pkts-per-second</i> に指定できる範囲は毎秒 0 ~ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないの
		で、接続切断後スパニング ツリー トポロジがコンバージェンス する速度が遅くなります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されま す。UplinkFast をイネーブルにする、または UplinkFast がすでにイネーブルに設定されている場合に、 パス コストを 3000 未満に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コス トが 3000 だけ増加します (パス コストを 3000 以上に変更した場合、パス コストは変更されません)。 スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が 低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

アップデート パケット レートをデフォルトの設定値に戻す場合は、no spanning-tree uplinkfast max-update-rate グローバル コンフィギュレーション コマンドを使用します。UplinkFast をディセー ブルにする場合は、no spanning-tree uplinkfast コマンドを使用します。

BackboneFast のイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニング ツリーの再構成をより早 く開始できます。

(注)

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルにしなければなり ません。BackboneFast は、トークンリング VLAN 上ではサポートされません。この機能は他社製ス イッチでの使用にサポートされています。

Rapid PVST+ または MSTP 用に、BackboneFast 機能を設定できます。ただし、スパニング ツリー モードを PVST+ に変更するまで、この機能はディセーブル(非アクティブ)のままです。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	spanning-tree backbonefast	BackboneFast をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存
		します。

BackboneFast 機能をディセーブルにする場合は、no spanning-tree backbonefast グローバル コン フィギュレーション コマンドを使用します。

EtherChannel ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、EtherChannel の設定の矛盾 を検出する EtherChannel ガード機能をイネーブルにできます。

EtherChannel ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順 は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	spanning-tree etherchannel guard	EtherChannel ガードをイネーブルにします。
	misconfig	
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show spanning-tree summary	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存
		します。

EtherChannel ガード機能をディセーブルにするには、no spanning-tree etherchannel guard misconfig グローバル コンフィギュレーション コマンドを使用します。

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾 が原因でディセーブルになっているスイッチ ポートを表示できます。リモート デバイス上では、**show etherchannel summary** 特権 EXEC コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正したあと、誤って設定していたポート チャネル インターフェイス上で、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力してください。

ルート ガードのイネーブル化

1 つのインターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが所属するす べての VLAN にルート ガードが適用されます。UplinkFast 機能が使用するインターフェイスで、ルー ト ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に(ブロッキング ステートの)バックアップ インターフェイスがルート ポートになります。ただし、同時にルート ガー ドもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェ イスが root-inconsistent(ブロック)ステートになり、フォワーディング ステートに移行できなくなり ます。



ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、この機能をイネーブルにできます。

インターフェイス上でルート ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ステップ 3	spanning-tree guard root	インターフェイスでルート ガードをイネーブルに設定します。 デフォルトでは、ルート ガードはすべてのインターフェイスでディセー ブルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ルート ガードをディセーブルにする場合は、no spanning-tree guard インターフェイス コンフィギュレーション コマンドを使用します。

ループ ガードのイネーブル化

ループ ガードを使用すると、代替ポートまたはルート ポートが、単一方向リンクの原因となる障害に よって指定ポートになることを防ぎます。この機能は、スイッチド ネットワーク全体に設定した場合 に最も効果があります。ループ ガードは、スパニング ツリーがポイントツーポイントと見なすイン ターフェイス上でのみ動作します。

(注)

ループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼動している場合、この機能をイネーブルにできます。

ループ ガードをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	show spanning-tree active	どのインターフェイスが代替ポートまたはルート ポートで
	または	あるかを確認します。
	show spanning-tree mst	
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree loopguard default	ループ ガードをイネーブルにします。
		ループ ガードは、デフォルトではディセーブルに設定され ています。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し ます。

ループ ガードをグローバルにディセーブルにする場合は、no spanning-tree loopguard default グロー バル コンフィギュレーション コマンドを使用します。no spanning-tree loopguard default グローバ ル コンフィギュレーション コマンドの設定を上書きするには、spanning-tree guard loop インター フェイス コンフィギュレーション コマンドを使用します。

スパニング ツリー ステータスの表示

スパニングツリー ステータスを表示するには、表 18-2 の特権 EXEC コマンドを1つまたは複数使用します。

表 18-2 スパニング ツリー ステータスを表示するためのコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニング ツリー情報だけを表
	示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface interface-id	特定のインターフェイスのスパニング ツリー情報を表示します。
show spanning-tree mst interface interface-id	特定のインターフェイスの MST 情報を表示します。
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。またはスパニング
	ツリー ステート セクションのすべての行を表示します。

clear spanning-tree [interface *interface-id*] 特権 EXEC コマンドを使用して、スパニングツリー カウ ンタをクリアできます。

show spanning-tree 特権 EXEC コマンドの他のキーワードについては、このリリースに対応するコマンド リファレンスを参照してください。

■ スパニング ツリー ステータスの表示



снартек 19

Flex Link および MAC アドレス テーブル移 動更新機能の設定

(注)

Flex Link および MAC アドレス テーブル移動更新機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

この章では、Flex Link を設定する方法について説明します。Flex Link は、Catalyst 2960 スイッチ上 のインターフェイスのペアで、相互バックアップを提供します。また、MAC Address-Table Move Update Feature (MAC アドレス テーブル移動更新機能、Flex Links の双方向高速コンバージェンス機 能とも呼ばれます)の設定方法も説明します。

(注)

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

この章で説明する内容は、次のとおりです。

- 「Flex Link および MAC アドレス テーブル移動更新機能の概要」(P.19-1)
- 「Flex Link および MAC アドレス テーブル移動更新機能の設定」(P.19-8)
- 「Flex Link および MAC アドレス テーブル移動更新のモニタ」(P.19-16)

Flex Link および MAC アドレス テーブル移動更新機能の概 要

ここでは、次の情報について説明します。

- 「Flex Link」 (P.19-2)
- 「VLAN Flex Link ロード バランシングおよびサポート」(P.19-3)
- 「Flex Link マルチキャスト高速コンバージェンス」(P.19-3)
- 「MAC アドレス テーブル移動更新」(P.19-7)

Flex Link

Flex Link は、レイヤ2 インターフェイス(スイッチ ポートまたはポート チャネル)のペアで、1 つの インターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、 Spanning Tree Protocol (STP; スパニングツリー プロトコル)の代替ソリューションを提供します。 ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。Flex Link は、 通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに 設定されます。スイッチが STP を実行中の場合は、STP がすでにリンクレベルの冗長性またはバック アップを提供しているため、Flex Link は不要です。

別のレイヤ2インターフェイスを Flex Link またはバックアップリンクとして割り当てることで、1 つ のレイヤ2インターフェイス (アクティブリンク) に Flex Link を設定します。リンクの1 つがアップ でトラフィックを転送しているときは、もう一方のリンクがスタンバイ モードで、このリンクが シャット ダウンした場合にトラフィックの転送を開始できるように準備しています。どの時点でも、1 つのインターフェイスのみがリンクアップ ステートでトラフィックを転送しています。プライマリ リ ンクがシャットダウンした場合は、スタンバイ リンクがトラフィックの転送を開始します。アクティ ブリンクがアップに戻った場合はスタンバイ モードになり、トラフィックが転送されません。STP は Flex Link インターフェイスでディセーブルです。

図 19-1 では、スイッチ A のポート 1 およびポート 2 がアップリンク スイッチ B およびアップリンク スイッチ C に接続されています。これらのスイッチは Flex Link として設定されているので、どちらか のインターフェイスがトラフィックを転送し、もう一方のインターフェイスはスタンバイ モードにな ります。ポート 1 がアクティブ リンクになる場合、ポート 1 とスイッチ B との間でトラフィックの転 送を開始し、ポート 2 (バックアップ リンク) とスイッチ C との間のリンクでは、トラフィックの転 送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送 し始めます。ポート 1 は、再び動作を開始するとスタンバイ モードになり、トラフィックを転送しま せん。ポート 2 がトラフィック転送を続けます。

また、優先してトラフィックの転送に使用するポートを指定して、プリエンプト メカニズムを設定す ることもできます。たとえば、図 19-1 では、Flex Link ペアをプリエンプト モードで設定することに より、ポート 2 より帯域幅の大きいポート 1 が再び動作を開始したあと、ポート 1 が 60 秒後にトラ フィックの転送を開始し、ポート 2 がスタンバイとなります。これを行うには、switchport backup interface preemption mode bandwidth および switchport backup interface preemption delay イン ターフェイス コンフィギュレーション コマンドを入力します。



プライマリ(転送)リンクがダウンした場合、トラップがネットワーク管理ステーションに通知しま す。スタンバイリンクがダウンした場合、トラップがユーザに通知します。

Flex Link はレイヤ 2 ポートおよびポート チャネルでのみサポートされ、VLAN(仮想 LAN)ではサ ポートされません。

VLAN Flex Link ロード バランシングおよびサポート

VLAN Flex Link ロード バランシングにより、ユーザは相互に排他的な VLAN のトラフィックを両方 のポートで同時に転送するように Flex Link ペアを設定できます。たとえば、Flex Link ポートが 1 ~ 100 の VLAN に対して設定されている場合、最初の 50 の VLAN のトラフィックを 1 つのポートで転 送し、残りの VLAN のトラフィックをもう一方のポートで転送できます。どちらかのポートで障害が 発生した場合には、もう一方のアクティブ ポートがすべてのトラフィックを転送します。障害ポート が回復すると、優先する VLAN のトラフィックの転送を再開します。このように、Flex Link のペアは 冗長性を提供するだけでなく、ロード バランシングの用途に使用できます。また、Flex Link VLAN ロード バランシングによってアップリンク スイッチが制約を受けることはありません。



Flex Link マルチキャスト高速コンバージェンス

(注)

Flex Link マルチキャスト高速コンバージェンスを使用するには、スイッチが LAN Base イメージを実行している必要があります。

Flex Link マルチキャスト高速コンバージェンスにより、Flex Link の障害発生後のマルチキャスト トラフィック コンバージェンス時間が短縮されます。Flex Link マルチキャスト高速コンバージェンス は、次の各ソリューションを組み合わせることにより実装されます。

- 「その他の Flex Link ポートを mrouter ポートとして学習」(P.19-4)
- 「IGMP レポートの生成」(P.19-4)
- 「IGMP レポートのリーク」 (P.19-4)
- 「設定例」(P.19-5)

その他の Flex Link ポートを mrouter ポートとして学習

通常のマルチキャスト ネットワークでは、個々の VLAN について 1 つのクエリアが選定されます。 ネットワーク エッジに展開されたスイッチには、クエリーを受信するいずれかの Flex Link ポートが存 在します。Flex Link ポートは常に、転送状態になります。

クエリーを受信するポートが、スイッチの *mrouter* ポートとして追加されます。mrouter ポートは、ス イッチが学習したすべてのマルチキャスト グループの1 つとして認識されます。切り替えの後、クエ リーは別の Flex Link ポートによって受信されます。この別の Flex Link ポートは mrouter ポートとし て認識されるようになります。切り替えの後、マルチキャスト トラフィックは別の Flex Link ポートを 介して流れます。トラフィック コンバージェンスを高速化するために、いずれか一方の Flex Link ポー トが mrouter ポートとして学習されると、両方の Flex Link ポートが mrouter ポートとして認識されま す。いずれの Flex Link ポートも常に、マルチキャスト グループの一部として扱われます。

通常の動作モードではいずれの Flex Link ポートもグループの一部として認識されますが、バックアッ プポートを通過するトラフィックはすべてブロックされます。したがって、mrouter ポートとしてバッ クアップポートを追加しても、通常のマルチキャスト データ フローが影響を受けることはありませ ん。切り替えが生じると、バックアップポートのブロックが解除され、トラフィックが流れるように なります。この場合、バックアップポートのブロックが解除されるとただちに、アップストリーム データが流れ始めます。

IGMP レポートの生成

切り替えの後、バックアップリンクがアップ状態になると、アップストリームでの新しいディストリ ビューション スイッチでのマルチキャスト データの転送は開始されません。これは、ブロックされた Flex Link ポートに接続されているアップストリーム ルータのポートが、いずれのマルチキャスト グ ループの一部としても認識されないからです。マルチキャスト グループのレポートは、バックアップ リンクがブロックされているため、ダウンストリーム スイッチでは転送されません。このポートの データは、マルチキャスト グループが学習されるまで流れません。マルチキャスト グループの学習は、 レポートを受信した後にだけ行われます。

レポートは、一般クエリーが受信されると、ホストより送信されます。一般クエリーは、通常のシナリ オであれば 60 秒以内に送信されます。バックアップ リンクが転送を開始し、マルチキャスト データを 高速で収束できるようになると、ダウンストリーム スイッチが一般クエリーを待つことなく、ただち にこのポート上のすべての学習済みグループに対し、プロキシ レポートを送信します。

IGMP レポートのリーク

マルチキャストトラフィックを最小限の損失で収束させるために、Flex Linkのアクティブリンクがダ ウンする前に冗長データパスを設定しておく必要があります。マルチキャストトラフィックのコン バージェンスは、Flex Link バックアップリンクに IGMP レポートパケットだけをリークさせれば行 えます。こうしてリークさせた IGMP レポートメッセージがアップストリームのディストリビュー ションルータで処理されるため、マルチキャストデータのトラフィックはバックアップインターフェ イスに転送されます。バックアップインターフェイスの着信トラフィックはすべてアクセス スイッチ の入り口部分でドロップされるため、ホストが重複したマルチキャストトラフィックを受信すること はありません。Flex Linkのアクティブリンクに障害が発生した場合、ただちにアクセス スイッチが バックアップリンクからのトラフィックを受け入れ始めます。このスキームの唯一の欠点は、ディス トリビューション スイッチ間のリンク、およびディストリビューション スイッチをアクセス スイッチ の間のバックアップリンクで帯域幅が大幅に消費される点です。この機能はデフォルトでディセーブ ルになっています。switchport backup interface *interface-id* multicast fast-convergence コマンドを 使用して、設定を変更できます。

切り替え時にこの機能がイネーブルになっている場合、スイッチでは転送ポートに設定されたバック アップ ポート上でプロキシ レポートは生成されません。

設定例

次に、Gigabit Ethernet0/11 と Gigabit Ethernet0/12 に Flex Link を設定した状態で、show interfaces switchport backup コマンドの実行結果を出力させる場合、mrouter ポートとして別の Flex Link 学習 させる設定例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitehernet0/11
Switch(config-if) # switchport trunk encapsulation dotlq
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport backup interface gigabitehernet0/12
Switch(config-if)# exit
Switch(config)# interface gigabitehernet1/0/12
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

この出力は、Gigabit Ethernet0/11: を介してスイッチに到達するクエリーを伴う VLAN 1 と 401 のク エリアを示しています。

Switch#	show ip igmp	snooping querier	
Vlan	IP Address	IGMP Version	Port
1 401	1.1.1.1 41.41.41.1	v2 v2	Gi0/11 Gi0/11

次に VLAN 1 と 401 に対する show ip igmp snooping mrouter コマンドの出力を示します。

Switch# show ip igmp snooping mrouter
Vlan ports
---- ---1 Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401 Gi1/0/11(dynamic), Gi1/0/12(dynamic)

同様に、いずれの Flex Link ポートも学習済みグループの一部になっています。この例では、Gigabit Ethernet0/11 が VLAN 1 のレシーバ/ホストとして使用され、次の 2 つのマルチキャスト グループに関 与します。

Switch#	show ip ig	mp snoop	ing groups				
Vlan	Group	Туре	Version	Port List			
1 1	228.1.5.1 228.1.5.2	igmp igmp	v2 v2	Gi1/0/11, Gi1/0/11,	Gi1/0/12, Gi1/0/12,	Gi2/0/11 Gi2/0/11	-

ー般クエリーに対してあるホストが応答すると、スイッチがすべての mrouter ポートに関するこのレ ポートを転送します。この例の場合、あるホストが 228.1.5.1 グループに関するレポートを送信する と、バックアップ ポート バックアップ ポート Gigabit Ethernet0/12 がブロックされているため、 Gigabit Ethernet0/11 だけに転送されます。アクティブ リンク、Gigabit Ethernet0/11 がダウンすると、 バックアップ ポート、Gigabit Ethernet0/12 が転送を開始します。 このポートが転送を開始すると、ただちにホストに代わり、228.1.5.1 と 228.1.5.2 のグループにプロキ シレポートを送信します。アップストリーム ルータはグループを学習し、マルチキャスト データの転 送を開始します。これは、Flex Link のデフォルトの動作です。この動作は、ユーザが switchport backup interface gigabitEthernet 0/12 multicast fast-convergence コマンドを使用して高速コンバー ジェンスを設定すると、変更されます。次に、この機能をオンにする例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config) # interface gigabitethernet 0/11 Switch(config-if)# switchport backup interface gigabitethernet 0/12 multicast fast-convergence Switch(config-if) # exit Switch# show interfaces switchport backup detail Switch Backup Interface Pairs: Active Interface Backup Interface State _____ GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby Preemption Mode : off Multicast Fast Convergence : On Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12) Mac Address Move Update Vlan : auto

この出力は、Gigabit Ethernet0/11 を介してスイッチに到達するクエリーを伴う VLAN 1 と 401 のクエ リアを示しています。

Switch# show ip igmp snooping querierVlanIP AddressIGMP VersionPort11.1.1.1v2Gi0/1140141.41.41.1v2Gi0/11

次に VLAN 1 と 401 に対する show ip igmp snooping mrouter コマンドの出力を示します。

Switch#	show ip igmp snooping mrouter
Vlan	ports
1	Gi0/11(dynamic), Gi0/12(dynamic)
401	Gi10/11(dynamic), Gi0/12(dynamic)

同様に、いずれの Flex Link ポートも学習済みグループの一部になっています。この例では、Gigabit Ethernet0/11 が VLAN 1 のレシーバ/ホストとして使用され、次の 2 つのマルチキャスト グループに関 与します。

Switch#	show ip ig	mp snoop	ing groups			
Vlan	Group	Туре	Version	Port List		
1	228.1.5.1	igmp	v2	Gi1/0/11,	Gi1/0/12,	Gi2/0/11
1	228.1.5.2	igmp	v2	Gi1/0/11,	Gi1/0/12,	Gi2/0/11

ー般クエリーに対してあるホストが応答すると必ず、スイッチがすべての mrouter ポートに関するこの レポートを転送します。コマンドライン ポートによりこの機能をオンにすると、GigabitEthernet0/11 のスイッチによりレポートが転送されたときに、バックアップ ポートの GigabitEthernet0/12 バック アップ ポートのギガビット イーサネットにもリークされます。アップストリーム ルータはグループを 学習し、マルチキャスト データの転送を開始します。このデータは、GigabitEthernet0/12 がブロック されているため、入り口部分でドロップされます。アクティブ リンク、GigabitEthernet0/11 がダウン すると、バックアップ ポートの GigabitEthernet0/12 が転送を開始します。マルチキャスト データはす でにアップストリーム ルータにより転送されているため、いずれのプロキシ レポートも送信する必要 はありません。バックアップ ポートにレポートをリークさせることにより、冗長マルチキャスト パス が設定されるため、マルチキャスト トラフィック コンバージェンスに要する時間が最小限に抑えられ ます。

MAC アドレス テーブル移動更新

MAC アドレス テーブル移動更新機能により、プライマリ(転送)リンクがダウンしてスタンバイ リ ンクがトラフィックの転送を開始したときに、スイッチで高速双方向コンバージェンスが提供されま す。

図 19-3 では、スイッチ A がアクセス スイッチで、スイッチ A のポート1 および 2 が Flex Link ペア 経由でアップリンク スイッチの B と D に接続されます。ポート1 はトラフィックの転送中で、ポート 2 はバックアップ ステートです。PC からサーバへのトラフィックはポート1 からポート 3 に転送され ます。PC の MAC アドレスが、スイッチ C のポート 3 で学習されています。サーバから PC へのトラ フィックはポート 3 からポート1 に転送されます。

MAC アドレス テーブル移動更新機能が設定されておらず、ポート1 がダウンした場合は、ポート2 が トラフィックの転送を開始します。しかし、少しの間、スイッチ C がポート3 経由でサーバから PC に トラフィックを転送し続けるため、ポート1 がダウンしていることにより、PC へのトラフィックが途 切れます。スイッチ C がポート3 で PC の MAC アドレスを削除し、ポート4 で再度学習した場合は、 トラフィックはポート2 経由でサーバから PC へ転送される可能性があります。

図 19-3 で MAC アドレス テーブル移動更新機能が設定され、各スイッチでイネーブルになっていて、 ポート1 がダウンした場合は、ポート2 が PC からサーバへのトラフィックの転送を開始します。ス イッチは、ポート2 から MAC アドレス テーブル移動更新パケットを送出します。スイッチ C はこの パケットをポート4 で受信し、ただちに PC の MAC アドレスをポート4 で学習します。これにより、 再収束時間が短縮されます。

アクセススイッチであるスイッチ A を設定し、MAC アドレス テーブル移動更新メッセージを送信 (send) することができます。また、アップリンク スイッチ B、C、および D を設定して、MAC アド レス テーブル移動更新メッセージの取得(get) および処理を行うこともできます。スイッチ C がス イッチ A から MAC アドレス テーブル移動更新メッセージを受信すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブル エントリを含め、MAC アドレス テーブルをアップデートします。

スイッチ A が、MAC アドレス テーブル移動更新を待機する必要はありません。スイッチはポート 1 上の障害を検出すると、ただちに、新しい転送ポートであるポート 2 からのサーバ トラフィックの転 送を開始します。この変更は、100 ミリ秒 (ms) 以内に行われます。PC はスイッチ A に直接接続さ れ、その接続状態に変更はありません。スイッチ A による、MAC アドレス テーブルでの PC エントリ の更新は必要ありません。



Flex Link および MAC アドレス テーブル移動更新機能の設 定

ここでは、次の情報について説明します。

- 「デフォルト設定」(P.19-9)
- 「設定時の注意事項」(P.19-9)
- 「Flex Link の設定」(P.19-10)
- 「Flex Link の VLAN ロード バランシングの設定」(P.19-12)
- 「MAC アドレス テーブル移動更新機能の設定」(P.19-14)
デフォルト設定

Flex Link は設定されておらず、バックアップインターフェイスは定義されていません。

プリエンプト モードはオフです。

プリエンプト遅延は 35 秒です。

MAC アドレス テーブル移動更新機能は、スイッチで設定されていません。

設定時の注意事項

Flex Link の設定時には、次の注意事項に従ってください。

- 最大16のバックアップリンクを設定できます。
- アクティブリンクに対して設定可能な Flex Link バックアップリンクは1つのみで、アクティブインターフェイスとは別のインターフェイスである必要があります。
- インターフェイスは1つの Flex Link ペアにのみ所属できます。1つのインターフェイスは、1つのアクティブリンクに対してのみバックアップリンクとなることができます。アクティブリンクは別の Flex Link ペアに属することはできません。
- どちらのリンクも EtherChannel に属するポートにはなりません。ただし、2 つのポート チャネル (EtherChannel 論理インターフェイス) を Flex Link として設定でき、1 つのポート チャネルと1 つの物理インターフェイスを Flex Link として設定できます。ポート チャネルまたは物理インター フェイスのいずれかがアクティブリンクとなります。
- バックアップリンクはアクティブリンクと同じタイプ(ファストイーサネット、ギガビットイー サネット、またはポートチャネル)にする必要はありません。ただし、スタンバイリンクがトラ フィックの転送を開始した場合にループが発生することや、動作が変更されることがないように、 同じ特性で両方のFlex Linkを設定する必要があります。
- STP は Flex Link ポートでディセーブルです。ポート上にある VLAN が STP 用に設定されている 場合でも、Flex Link ポートは STP に参加しません。STP がイネーブルでない場合は、設定されて いるトポロジーでループが発生しないようにしてください。Flex Link 設定が削除されると、その ポートの STP は再びイネーブルになります。

Flex Link 機能による VLAN ロード バランシングを設定するときには、次の注意事項に従ってください。

- Flex Link VLAN ロード バランシングでは、バックアップ インターフェイス上で優先される VLAN を選択する必要があります。
- 同じ Flex Link ペアに対して、プリエンプト メカニズムと VLAN ロード バランシングを設定する ことはできません。

MAC アドレス テーブル移動更新機能の設定時には、次の注意事項に従ってください。

- アクセススイッチでこの機能のイネーブル化と設定を行うと、MACアドレステーブル移動更新を 送信(send)することができます。
- アップリンクスイッチでこの機能のイネーブル化と設定を行うと、MACアドレステーブル移動更新を受信(receive)することができます。

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

Flex Link の設定

Flex Link のペアを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し
		ます。
ステップ 2	interface interface-id	インターフェイスを指定して、インターフェイス コ
		ンフィギュレーション モードを開始します。イン
		ターフェイスは物理レイヤ2インターフェイスまたは
		ポート チャネル(論理インターフェイス)に設定で
		きます。指定できるポートチャネルの範囲は1~6で
		す。
ステップ 3	switchport backup interface interface-id	物理レイヤ2インターフェイス (ポート チャネル)
		をインターフェイスがある Flex Link ペアの一部とし
		て設定します。1 つのリンクがトラフィックを転送し
		ている場合、もう一方のインターフェイスはスタンバ
		イモードです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces [interface-id] switchport backup	設定を確認します。
ステップ 6	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレー
		ション ファイルに設定を保存します。

Flex Link バックアップ インターフェイスをディセーブルにするには、**no switchport backup interface** *interface-id* インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイスをバックアップインターフェイスに設定し、設定を確認する例を示します。

Switch# configure terminal Switch(conf)# interface gigabitethernet0/1 Switch(conf-if)# switchport backup interface gigabitethernet0/2 Switch(conf-if)# end

Switch# show interfaces switchport backup Switch Backup Interface Pairs:

Active Interface Backup Interface State

GigabitEthernet0/1 GigabitEthernet0/2 Active Standby/Backup Up Vlans Preferred on Active Interface: 1-3,5-4094 Vlans Preferred on Backup Interface: 4 Flex Link ペアのプリエンプト方式を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し ます。
ステップ 2	interface interface-id	インターフェイスを指定して、インターフェイス コ ンフィギュレーション モードを開始します。イン ターフェイスは物理レイヤ2インターフェイスまたは ポートチャネル(論理インターフェイス)に設定で きます。指定できるポートチャネルの範囲は1~6で す。
ステップ 3	switchport backup interface interface-id	物理レイヤ2インターフェイス(ポートチャネル) をインターフェイスがある Flex Link ペアの一部とし て設定します。1つのリンクがトラフィックを転送し ている場合、もう一方のインターフェイスはスタンバ イモードです。
ステップ 4	switchport backup interface <i>interface-id</i> preemption mode [forced bandwidth off]	Flex Link インターフェイス ペアのプリエンプト メカ ニズムとプリエンプト遅延を設定します。次のプリエ ンプト モードを設定することができます。
		 Forced:アクティブ インターフェイスが常に バックアップ インターフェイスより先に使用され ます。
		 Bandwidth:より大きい帯域幅のインターフェイ スが常にアクティブインターフェイスとして動作 します。
		 Off: アクティブ インターフェイスとバックアップ インターフェイスのどちらも優先されません。
ステップ 5	<pre>switchport backup interface interface-id preemption delay delay-time</pre>	ポートが他のポートより先に使用されるまでの遅延時 間を設定します。
		(注) 遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces [interface-id] switchport backup	設定を確認します。
ステップ 8	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレー ション ファイルに設定を保存します。

プリエンプト方式を削除するには、no switchport backup interface *interface-id* preemption mode イ ンターフェイス コンフィギュレーション コマンドを使用します。遅延時間をデフォルトにリセットす るには、no switchport backup interface *interface-id* preemption delay インターフェイス コンフィ ギュレーション コマンドを使用します。

次に、バックアップ インターフェイスのペアに対してプリエンプト モードを *forced* に設定し、設定を 確認する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)#switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(conf-if)#switchport backup interface gigabitethernet0/2 preemption delay 50
Switch(conf-if)# end
```

Switch# show interfaces switchport backup detail Active Interface Backup Interface State				
GigabitEthernet0/1 GigabitEthernet0/2 Active Up/Backup Standby Interface Pair : Gi0/1, Gi0/2 Preemption Mode : forced				
Preemption Delay : 50 seconds Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2) Mac Address Move Update Vlan : auto				

Flex Link の VLAN ロード バランシングの設定

Flex Linkの VLAN ロード バランシングを設定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始し
	ます。
interface interface-id	インターフェイスを指定して、インターフェイス コ
	ンフィギュレーション モードを開始します。イン
	ターフェイスは物理レイヤ2インターフェイスまたは
	ポート チャネル(論理インターフェイス)に設定で
	きます。指定できるポートチャネルの範囲は1~6で
	す。
switchport backup interface interface-id prefer vlan	物理レイヤ2インターフェイス(またはポートチャ
vlan-range	ネル)をインターフェイスがある Flex Link ペアの一
	部として設定します。VLAN ID の範囲は 1~4094
	です。
end	特権 EXEC モードに戻ります。
show interfaces [interface-id] switchport backup	設定を確認します。
copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレー
	ション ファイルに設定を保存します。
	コマンド configure terminal interface interface-id switchport backup interface interface-id prefer vlan vlan-range end show interfaces [interface-id] switchport backup copy running-config startup config

VLAN ロード バランシング機能をディセーブルにするには、no switchport backup interface *interface-id* prefer vlan *vlan-range* インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチに VLAN 1 ~ 50、60、および 100 ~ 120 を設定する例を示します。

Switch(config)#interface gigabitethernet 0/6 Switch(config-if)#switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120

両方のインターフェイスがアップの場合、Gi0/8 は VLAN 60 および 100 ~ 120 のトラフィックを転送 し、Gi0/6 は VLAN 1 ~ 50 のトラフィックを転送します。

Switch#show interfaces switchport backup Switch Backup Interface Pairs:

Active Interface Backup Interface State GigabitEthernet0/6 GigabitEthernet0/8 Active Up/Backup Up Vlans Preferred on Active Interface: 1-50 Vlans Preferred on Backup Interface: 60, 100-120 Flex Link インターフェイスがダウン(LINK_DOWN)すると、このインターフェイスの優先 VLAN は Flex Link ペアの相手側のインターフェイスに移されます。この例では、インターフェイス Gi0/6 が ダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

Switch#show interfaces switchport backup Switch Backup Interface Pairs:

 Active Interface
 Backup Interface
 State

 GigabitEthernet0/6
 GigabitEthernet0/8
 Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50 Vlans Preferred on Backup Interface: 60, 100-120

Flex Link インターフェイスがアップになると、このインターフェイスの優先 VLAN は、相手側のイン ターフェイス上ではブロックされ、アップしたインターフェイス上でフォワーディング ステートに移 行します。この例では、インターフェイス Gi0/6 が再び稼動し始めると、このインターフェイスで優先 される VLAN がピア インターフェイス Gi0/8 でブロックされ、Gi0/6 に転送されます。

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

 Active Interface
 Backup Interface
 State

 GigabitEthernet0/6
 GigabitEthernet0/8
 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50 Vlans Preferred on Backup Interface: 60, 100-120

Switch#show interfaces switchport backup detail Switch Backup Interface Pairs:

 Active Interface
 Backup Interface
 State

 FastEthernet0/3
 FastEthernet0/4
 Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094 Vlans Preferred on Backup Interface: 3-4 Preemption Mode : off Bandwidth : 10000 Kbit (Fa0/3), 100000 Kbit (Fa0/4) Mac Address Move Update Vlan : auto

MAC アドレス テーブル移動更新機能の設定

ここでは、次の情報について説明します。

- MAC アドレス テーブル移動更新を送信するためのスイッチの設定
- MAC アドレス テーブル移動更新を受信するためのスイッチの設定

MAC アドレス テーブル移動更新を送信するようにアクセス スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し ます。
ステップ 2	interface interface-id	インターフェイスを指定して、インターフェイス コ ンフィギュレーション モードを開始します。イン ターフェイスは物理レイヤ 2 インターフェイスまたは ポート チャネル (論理インターフェイス) に設定で きます。指定できるポートチャネルの範囲は 1 ~ 6 で す。
ステップ 3	switchport backup interface interface-id または switchport backup interface interface-id mmu	物理レイヤ2インターフェイス(ポートチャネル) をインターフェイスがある Flex Link ペアの一部とし て設定します。MAC アドレス テーブル移動更新 VLAN はインターフェイスで最も低い VLAN ID で す。
	primary vlan vlan-id	物理レイヤ 2 インターフェイス(ポート チャネル) を設定し、MAC アドレス テーブル移動更新の送信に 使用されるインターフェイスの VLAN ID を指定しま す。
		1 つのリンクがトラフィックを転送している場合、も う一方のインターフェイスはスタンバイ モードです。
ステップ 4	end	グローバル コンフィギュレーション モードに戻りま す。
ステップ 5	mac address-table move update transmit	プライマリ リンクがダウンし、スイッチがスタンバ イ リンク経由でトラフィックの転送を開始した場合 は、アクセス スイッチをイネーブルにして、MAC ア ドレス テーブル移動更新をネットワーク上の他のス イッチに送信します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mac address-table move update	設定を確認します。
ステップ 8	copy running-config startup config	(任意)スイッチのスタートアップ コンフィギュレー ション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、no mac address-table move update transmit インターフェイス コンフィギュレーション コマンドを使用します。MAC アドレス テーブル 移動更新情報を表示するには、show mac address-table move update 特権 EXEC コマンドを使用しま す。

次に、アクセス スイッチを設定して、MAC アドレス テーブル移動更新メッセージの送信と設定の確認を行う例を示します。

```
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

次に、設定を確認する例を示します。

Switch# show mac-address-table move update Switch-ID : 010b.4630.1780 Dst mac-address : 0180.c200.0010 Vlans/Macs supported : 1023/8320 Default/Current settings: Rcv Off/On, Xmt Off/On Max packets per min : Rcv 40, Xmt 60 Rcv packet count : 5 Rcv conforming packet count : 5Rcv invalid packet count : 0 Rcv packet count this min : 0 Rcv threshold exceed count : 0 Rcv last sequence# this min : 0 Rcv last interface : Po2 Rcv last src-mac-address : 000b.462d.c502 Rcv last switch-ID : 0403.fd6a.8700 Xmt packet count : 0 Xmt packet count this min : 0 Xmt threshold exceed count : 0 Xmt pak buf unavail cnt : 0 Xmt last interface : None

MAC アドレス テーブル移動更新メッセージの受信および処理を行うようにスイッチを設定するには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し
		ます。
ステップ 2	mac address-table move update receive	スイッチをイネーブルにして、MAC アドレス テーブ ル移動更新の受信および処理を行います。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mac address-table move update	設定を確認します。
ステップ 5	copy running-config startup config	(任意) スイッチのスタートアップ コンフィギュレー
		ション ファイルに設定を保存します。

MAC アドレス テーブル移動更新機能をディセーブルにするには、no mac address-table move update receive インターフェイス コンフィギュレーション コマンドを使用します。 MAC アドレス テーブル移動更新情報を表示するには、 show mac address-table move update 特権 EXEC コマンドを使用します。

次に、スイッチを設定して、MAC アドレス テーブル移動更新メッセージの受信と処理を行う例を示します。

Switch# configure terminal Switch(conf)# mac address-table move update receive Switch(conf)# end

Flex Link および MAC アドレス テーブル移動更新のモニタ

表 19-1 は、Flex Link 設定と MAC アドレス テーブル移動更新情報をモニタする特権 EXEC コマンド を示します。

表 19-1 Flex Link および MAC アドレス テーブル移動更新のモニタ コマンド

コマンド	目的
show interfaces [interface-id] switchport	あるインターフェイス用に設定された Flex Link バックアップ インター
backup	フェイス、または設定されたすべての Flex Link と、各アクティブ イン
	ターフェイスおよびバックアップ インターフェイスの状態(アップまたは
	スタンバイ モード)を表示します。VLAN ロード バランシングがイネーブ
	ルであると、出力には、アクティブ インターフェイスおよびバックアップ
	インターフェイスの優先 VLAN が表示されます。
show mac address-table move update	スイッチの MAC アドレス テーブル移動更新情報を表示します。



20 НАРТЕР

DHCP 機能 および IP ソース ガード機能の設 定

(注)

Dynamic Host Configuration Protocol (DHCP) 機能を使用するには、スイッチが LAN Base イメージ を実行している必要があります。

この章では、DHCP スヌーピングと Option 82 データ挿入の設定方法、および Catalyst2960 スイッチ における DHCP サーバ ポートベースのアドレス割り当て機能の設定方法について説明します。また、 IP Source Guard (IPSG; IP ソース ガード)機能の設定方法についても説明します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』の「DHCP Commands」を参照してください。このコマンドリファレンスには、 Cisco.com ホームページ(Documentation > Cisco IOS Software > 12.2 Mainline > Command References)からアクセスできます。

この章で説明する内容は、次のとおりです。

- 「DHCP スヌーピングの概要」(P.20-2)
- 「DHCP スヌーピングの設定」(P.20-8)
- 「DHCP スヌーピング情報の表示」(P.20-15)
- 「IP ソース ガードの概要」(P.20-15)
- 「IP ソース ガードの設定」(P.20-18)
- 「IP ソース ガード情報の表示」(P.20-24)
- 「DHCP サーバ ポートベースのアドレス割り当ての概要」(P.20-24)
- 「DHCP サーバ ポートベースのアドレス割り当ての設定」(P.20-25)
- 「DHCP サーバ ポートベースのアドレス割り当ての表示」(P.20-28)

DHCP スヌーピングの概要

DHCP は、中央のサーバからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用され ており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。DHCP では、ネット ワークに接続されたホストだけが IP アドレスを使用し、IP アドレスを永続的にホストに割り当てる必 要がなくなるため、限られた IP アドレス空間を節約できます。

ここでは、次の情報について説明します。

- 「DHCP サーバ」 (P.20-2)
- 「DHCP リレーエージェント」 (P.20-2)
- 「DHCP スヌーピング」(P.20-3)
- 「Option 82 データ挿入」(P.20-4)
- 「DHCP スヌーピング バインディング データベース」(P.20-7)

DHCP クライアントの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「*IP Addressing and Services*」にある「*Configuring DHCP*」を参照してください。このガイドには、 Cisco.com ホームページ (**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Configuration Guides**) からアクセスできます。

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求さ れた設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理 者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバ イスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求お よび応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過 的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを 受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バイ ンディング データベース (DHCP スヌーピング バインディング テーブルとも呼ばれる)の作成および 管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンド ユーザに接続された信頼できないイン ターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別で きます。

(注)

DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェ イス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、ネットワークまたはファイアウォールの外側から送信された メッセージのことです。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタ マーのスイッチなど、サービス プロバイダー ネットワーク上にないデバイスから送信されたメッセー ジが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック 攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、 バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスのイ ンターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続さ れたホストの情報はありません。

サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたイン ターフェイスが信頼できるインターフェイスとなります。ネットワーク内の信頼できないインターフェ イスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスは、信 頼できないインターフェイスとなります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレス と DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合(デフォル ト)、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットを廃棄しま す。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットを廃棄します。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パ ケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着 信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアン トのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バイン ディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP Option 82 情報を挿入するエッジス イッチに接続されているスイッチは、Option 82 情報を含むパケットが信頼できないインターフェイス に着信した場合、それらのパケットを廃棄します。DHCP スヌーピングがイネーブルに設定されてい る場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを 作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジスイッチに接続できる場合、ip dhcp snooping information option allow-untrusted グローバル コンフィギュレーション コマンドを入力す ると、集約スイッチはエッジスイッチによって挿入された Option 82 情報を含むパケットを受け入れま す。集約スイッチは、信頼できないスイッチ インターフェイスを介して接続されたホストのバイン ディングを認識します。集約スイッチで、Dynamic ARP Inspection (DAI; ダイナミック ARP インス ペクション)や IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできま すが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない 入力インターフェイスで受信します。集約スイッチ上のエッジスイッチとの接続ポートは、信頼でき るインターフェイスとして設定する必要があります。

Option 82 データ挿入

住宅地域にあるメトロポリタンイーサネットアクセス環境では、DHCPにより、多数の加入者の IP アドレス割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。加入者 LAN 上の複数のホストをアクセス スイッチの同一ポートに接続でき、これらは一意に識別されます。

(注)

DHCP Option 82 機能は、DHCP スヌーピングがグローバルにイネーブルであり、この機能を使用する 加入者装置が割り当てられた VLAN でもイネーブルである場合に限りサポートされます。

図 20-1 に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを 割り当てるメトロポリタン イーサネット ネットワークの例を示します。DHCP クライアントとそれら に関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント (Catalyst スイッチ) にヘルパー アドレスを設定することにより、ブロードキャ スト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 20-1 メトロポリタン イーサネット ネットワークにおける DHCP リレー エージェント



スイッチで DHCP スヌーピング情報オプション Option 82 をイネーブルにすると、以下のイベントが この順序で発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、ネットワーク上にブロードキャストしま す。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。リモート ID サブオプションはスイッチの MAC アドレスであり、回線 ID サブオプションはパケットを受信 したポートの識別子 vlan-mod-port です。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバがこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装し たりできます。次に、DHCP サーバは DHCP 応答内に Option 82 フィールドをエコーします。
- 要求がスイッチによってサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。
- この一連のイベントが発生する間、図 20-2 に示す以下のフィールドの値は変更されません。
- 回線 ID サブオプション フィールド
 - サブオプションタイプ
 - サブオプションタイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプションタイプの長さ
 - リモート ID タイプ
 - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号は 3 から始まります。たとえば、24 個の 10/100 ポートと Small Form-factor Pluggable (SFP) モジュール スロットを備えたスイッチでは、 ポート 3 がファスト イーサネット 0/1 ポート、ポート 4 がファスト イーサネット 0/2 ポートなどとなります。さらに、ポート 27 は SFP モジュール スロット 0/1 などとなります。 図 20-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。ス イッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、 ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合で す。

図 20-2 サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット

サブオプ タイご	ション プ II	回線 Dタイ	プ			
	長さ		長さ			
–¥ –	6	0	₩ 4	VLAN	モジュール	ポート
1バイ	ト1バイト	1バイト	1バイト	2バイト	1バイト	1バイト

リモート ID サブオプション フレーム フォーマット

サブ	オプシ タイプ	ミン !	ノモー) タイ	トプ		
		長さ		長さ		
	2	8	0	6	MAC アドレス	
	1バイト	1バイト	1バイト	1バイト	6バイト	1163(

図 20-3 は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式 を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、ip dhcp snooping information option format remote-id グローバル コンフィギュレーション コマンド、およ び ip dhcp snooping vlan information option format-type circuit-id string インターフェイス コン フィギュレーション コマンドを入力した場合に、これらのパケットが使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらの フィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
 - 回線 ID タイプが1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
 - リモート ID タイプが1 である。
 - 設定した文字列の長さに応じて、長さの値が変化する。



回線 ID サブオプション フレーム フォーマット(ユーザ設定のストリング):



リモート ID サブオプション フレーム フォーマット(ユーザ設定のストリング):



DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報 を DHCP スヌーピング バインディング データベースに保存します。このデータベースには最大 8192 のバインディングを保存できます。

各データベース エントリ (バインディング) は、IP アドレス、それに関連付けられた MAC アドレス、 リース期間(16進形式)、バインディングが適用されるインターフェイス、およびインターフェイスが 属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバイン ディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エ ントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトの データがあり、その後に1つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェ ントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクショ ンまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースが ダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントが ディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませ んが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディン グ データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディン グ ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、直ちにデータベース内の エントリを更新します。スイッチはバインディングファイル内のエントリも更新します。バインディ ングファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイ ルが指定された時間内(書き込み遅延および中断タイムアウトの値によって設定される)に更新されな い場合、更新は停止します。

```
バインディングが含まれるファイルの形式は次のとおりです。
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
<entry-n> <checksum-1-2-...n>
END
```

このファイルの谷エントリにはチェックリム値を示すタクが内行られます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1

TYPE DHCP-SNOOPING

VERSION 1

BEGIN

192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb

192.1.168.3 3 0003.44d6.c52f 2BB648EB interface-id 1bdb223f

192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 584a38f0

END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、ス イッチはバインディングファイルのエントリを読み取り、バインディングを DHCP スヌーピング バイ ンディング データベースに追加します。以下のいずれかの状況が発生した場合、スイッチはエントリ を無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している(スイッチはリース期間の終了時にバインディングエントリを削除しないことがある)。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッドインターフェイスまたは DHCP スヌーピングにおける信頼できる インターフェイスである。

DHCP スヌーピングの設定

ここでは、次の設定情報について説明します。

- 「DHCP スヌーピングのデフォルト設定」(P.20-9)
- 「DHCP スヌーピング設定時の注意事項」(P.20-9)
- 「DHCP リレーエージェントの設定」(P.20-11)
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」(P.20-11)
- 「DHCP スヌーピング バインディング データベース エージェントのイネーブル化」(P.20-13)

DHCP スヌーピングのデフォルト設定

表 20-1 に、DHCP スヌーピングのデフォルト設定を示します。

表 20-1 DHCP スヌーピングのデフォルト設定

	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。 ¹
DHCP リレーエージェント	イネーブル。 ²
DHCP パケット転送アドレス	未設定。
リレーエージェント情報の確認	イネーブル (無効なメッセージは廃棄)。 ²
DHCP リレー エージェント転送ポリシー	既存のリレーエージェント情報を置換。2
DHCP スヌーピングをグローバルにイネーブル	ディセーブル。
DHCP スヌーピング情報オプション	イネーブル。
パケットを信頼できない入力インターフェイスで 受け取る DHCP スヌーピング オプション ³	ディセーブル。
DHCP スヌーピング レート制限	未設定。
DHCP スヌーピング信頼状態	untrusted。
DHCP スヌーピング VLAN	ディセーブル。
DHCP スヌーピングの MAC アドレス検証	イネーブル。
DHCP スヌーピング バインディング データベー ス エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先 が設定されている場合に限り有効。

1. スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。

2. スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。

3. この機能は、スイッチがエッジスイッチによって Option 82 が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

ここでは、DHCP の設定時の注意事項を説明します。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、VLAN で DHCP スヌーピングがイネーブルになるまでアクティブになり ません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認し てください。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにすると、スヌーピングをディセー ブルにするまで以下の Cisco IOS コマンドは使用できません。これらのコマンドを入力すると、ス イッチがエラーメッセージを返し、設定は適用されません。
 - ip dhcp relay information check グローバル コンフィギュレーション コマンド
 - ip dhcp relay information policy グローバル コンフィギュレーション コマンド
 - ip dhcp relay information trust-all グローバル コンフィギュレーション コマンド
 - ip dhcp relay information trusted インターフェイス コンフィギュレーション コマンド

- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- スイッチ上で文字数の多いサーキット ID を設定する場合、Nonvolatile Random-Access Memory (NVRAM; 不揮発性 RAM)またはフラッシュメモリに長い文字列が与える影響を考慮してください。サーキット ID 設定がその他のデータと組み合わされた場合、NVRAM またはフラッシュメモリの容量を超えてしまい、エラーメッセージが表示されます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを 設定してください。たとえば、DHCP サーバが割り当てたり除外したりできる IP アドレスを指定 するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントを セットアップする必要があります。
- DHCP リレー エージェントがイネーブルで、DHCP スヌーピングがディセーブルである場合、 DHCP Option 82 データ挿入機能はサポートされません。
- スイッチ ポートが DHCP サーバに接続されている場合は、ip dhcp snooping trust インターフェ イス コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してく ださい。
- スイッチ ポートが DHCP クライアントに接続されている場合は、no ip dhcp snooping trust イン ターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして 設定してください。
- DHCP スヌーピング バインディング データベースを設定するときには、次の注意事項に従ってく ださい。
 - NVRAM とフラッシュメモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することをお勧めします。
 - ネットワーク ベースの URL (TFTP や FTP など) については、スイッチがバインディングを その URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイ ルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについ ては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように 設定できないことがあります。
 - データベースに正しいリース期間が記録されるように、NTP をイネーブルにし、設定することをお勧めします。詳細については、「NTP の設定」(P.6-4)を参照してください。
 - NTP を設定した場合、スイッチは、スイッチのシステム クロックが NTP と同期したときにだ けバインディングの変更をバインディング ファイルに書き込みます。
- 信頼できないデバイスが接続された集約スイッチでは、ip dhcp snooping information option allow-untrusted コマンドを入力しないでください。このコマンドを入力すると、信頼できないデ バイスが偽装した Option 82 情報を提供する可能性があります。
- show ip dhcp snooping statistics ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報 を表示したり、clear ip dhcp snooping statistics 特権 EXEC コマンドを入力してスヌーピング統 計情報をクリアしたりできるようになりました。



⁽注) RSPAN VLAN では、Dynamic Host Configuration Protocol (DHCP) スヌーピングをイネー ブルにしないでください。RSPAN VLAN で DHCP スヌーピングをイネーブルにすると、 DHCP パケットが RSPAN 宛先ポートに届かない可能性があります。

DHCP リレー エージェントの設定

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	service dhcp	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイ ネーブルにします。この機能はデフォルトでイネーブルです。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DHCP サーバおよび DHCP リレー エージェントをディセーブルにするには、no service dhcp グロー バル コンフィギュレーション コマンドを使用します。

以下の手順については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」にある「*Configuring DHCP*」を参照してください。このガイドには、Cisco.com ホームページ(Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides) からアクセスできます。

- リレーエージェント情報のチェック(検証)
- リレーエージェント転送ポリシーの設定

DHCP スヌーピングおよび Option 82 のイネーブル化

スイッチ上で DHCP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ステップ 3	ip dhcp snooping vlan vlan-range	1 つの VLAN または VLAN 範囲で DHCP スヌーピングをイネーブ ルにします。指定できる範囲は 1 ~ 4094 です。
		VLAN ID 番号で示される 1 つの VLAN ID、カンマで区切られた 連の VLAN ID、ハイフンで区切られた VLAN ID の範囲、またはス ペースで区切られた開始 VLAN ID と終了 VLAN ID で示される VLAN ID の範囲を指定できます。
ステップ 4	ip dhcp snooping information option	スイッチが DHCP サーバへの DHCP 要求メッセージにおいて DHCP リレー情報(Option 82 フィールド)を挿入および削除できるように します。これがデフォルトの設定です。

	コマンド	目的				
ステップ 5	ip dhcp snooping information option	 (任意) リモート ID サブオプションを設定します。 (王ート ID は次のように設定できます。 最高 63 文字の ASCII 文字列 (スペースなし) 設定されたスイッチのホスト名 (エスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。 (エフォルトのリモート ID は、スイッチの MAC アドレスです。 (日意) スイッチがエッジ スイッチに接続された集約スイッチである 会、スイッチがエッジ スイッチに接続された集約スイッチである 会、スイッチがエッジ スイッチにはって Option 82 情報が挿入さいた着信 DHCP スヌーピング パケットを受け入れるようにします。 (エフォルト設定はディセーブルです。 (エクリンドは、信頼できるデバイスに接続された集約ス イッチだけで入力してください。 (エクリンターフェイスを指定し、インターフェイスコンフィ ビュレーションモードを開始します。 (エクロの範囲の VI AN ID を使用して、VI AN なたびポート ID 				
	format remote-id [string ASCII-string	リモート ID は次のように設定できます。				
	[nosinume]	 最高 63 文字の ASCII 文字列 (スペースなし) 				
		 設定されたスイッチのホスト名 				
		(注) ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。				
		デフォルトのリモート ID は、スイッチの MAC アドレスです。				
ステップ 6	ip dhcp snooping information option allow-untrusted	(任意) スイッチがエッジ スイッチに接続された集約スイッチである 場合、スイッチがエッジ スイッチによって Option 82 情報が挿入さ れた着信 DHCP スヌーピング パケットを受け入れるようにします。				
		デフォルト設定はディセーブルです。				
		 れた着信 DHCP スヌーピング パケットを受け入れるようにしま デフォルト設定はディセーブルです。 (注) このコマンドは、信頼できるデバイスに接続された集約ス イッチだけで入力してください。 設定するインターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。 (任意) 指定されたインターフェイスの回線 ID サブオプションを 定します。 1 ~ 4094 の範囲の VLAN ID を使用して、VLAN およびポート を指定します。デフォルトの回線 ID は、vlan-mod-port 形式で れたポート ID です。 				
ステップ 7	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。				
ステップ 8	ip dhep snooping vlan vlan information option format-type	(任意) 指定されたインターフェイスの回線 ID サブオプションを設 定します。				
	circuit-id [override] string ASCII-string	1 ~ 4094 の範囲の VLAN ID を使用して、VLAN およびポート ID を指定します。デフォルトの回線 ID は、vlan-mod-port 形式で表さ れたポート ID です。				
		回線 ID は、3 ~ 63 文字の ASCII 文字列(スペースなし)で設定します。				
		(任意)TLV 形式で挿入された回線 ID サブオプションで、加入者情報を定義する必要がない場合は、override キーワードを使用します。				
ステップ 9	ip dhcp snooping trust	(任意) インターフェイスを信頼できるインターフェイスまたは信頼 できないインターフェイスとして設定します。信頼できないクライ アントからのメッセージを受信するようにインターフェイスを設定 するには、no キーワードを使用します。デフォルト設定は untrusted です。				
ステップ 10	ip dhcp snooping limit rate rate	(任意) インターフェイスが受信できる 1 秒あたりの DHCP パケット 数を設定します。指定できる範囲は 1 ~ 2048 です。デフォルトで は、レート制限は設定されません。				
		(注) 信頼できないインターフェイスのレート制限を1秒あたり 100パケット以下に設定することをお勧めします。信頼でき るインターフェイスのレート制限を設定する場合、DHCPス ヌーピングを使った複数のVLANに割り当てられたトランク ポートでは、レート制限の値を大きくすることが必要になる ことがあります。				
ステップ 11	exit	グローバル コンフィギュレーション モードに戻ります。				
ステップ 12	ip dhcp snooping verify mac-address	 (任意) 信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと 一致することを確認するようにスイッチを設定します。デフォルト では、送信元 MAC アドレスがパケットのクライアント ハードウェ ア アドレスと一致することを確認します。 				

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

	コマンド	目的			
ステップ 13	end	特権 EXEC モードに戻ります。			
ステップ 14	show running-config	設定を確認します。			
ステップ 15	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。			

DHCP スヌーピングをディセーブルにするには、no ip dhcp snooping グローバル コンフィギュレー ション コマンドを使用します。1 つの VLAN または VLAN の範囲で DHCP スヌーピングをディセー ブルにするには、no ip dhcp snooping vlan vlan-range グローバル コンフィギュレーション コマンド を使用します。Option 82 フィールドの挿入および削除をディセーブルにするには、no ip dhcp snooping information option グローバル コンフィギュレーション コマンドを使用します。エッジス イッチによって Option 82 情報が挿入された着信 DHCP スヌーピング パケットを廃棄するように集約 スイッチを設定するには、no ip dhcp snooping information option allow-untrusted グローバル コン フィギュレーション コマンドを使用します。

次に、DHCP スヌーピングをグローバルおよび VLAN 10 でイネーブルにし、ポートのレート制限を1 秒あたり 100 パケットに設定する例を示します。

Switch(config)# ip dhcp snooping Switch(config)# ip dhcp snooping vlan 10 Switch(config)# ip dhcp snooping information option Switch(config)# interface gigabitethernet0/1 Switch(config-if)# ip dhcp snooping limit rate 100

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにし、設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring DHCP」にある「DHCP Configuration Task List」 を参照してください。このガイドには、Cisco.com ホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Configuration Guides**)からアクセスできます。

DHCP スヌーピング バインディング データベース エージェントのイネー ブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定 するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 1 ステップ 2	<pre>ip dhcp snooping database {flash:/filename ftp://user:password@host/filename http://[[username:password]@]]{hostn ame host-ip}[/directory] /image-name.tar rcp://user@host/filename} tftp://host/filename</pre>	 次のいずれかの形式を使用して、データベース エージェントまたは バインディング ファイルの URL を指定します。 flash:/filename ftp://user:password@host/filename http://[[username:password]@]{hostname host-ip}[/directory] /image-name.tar rcp://user@host/filename tftp://host/filename

	コマンド	目的
ステップ 3	ip dhcp snooping database timeout seconds	データベース転送プロセスが完了するのを待ち、それまでに完了し ない場合はプロセスを停止する時間(秒数)を指定します。
		デフォルト値は 300 秒です。指定できる範囲は 0 ~ 86400 です。無限の時間を定義し、転送の試行を無期限に続けるには、0 を使用します。
ステップ 4	ip dhcp snooping database write-delay <i>seconds</i>	バインディング データベースが変更されてから転送を開始するまで の遅延時間を指定します。指定できる範囲は 15 ~ 86400 秒です。デ フォルト値は 300 秒 (5 分)です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds	(任意) DHCP スヌーピング バインディング データベースにバイン ディング エントリを追加します。vlan-id の範囲は 1 ~ 4904 です。 seconds の範囲は 1 ~ 4294967295 です。
		このコマンドは、追加するエントリごとに入力します。
		(注) このコマンドは、スイッチをテストまたはデバッグするとき に使用します。
ステップ 7	show ip dhcp snooping database [detail]	DHCP スヌーピング バインディング データベース エージェントのス テータスおよび統計情報を表示します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

データベース エージェントおよびバインディング ファイルの使用を停止するには、no ip dhcp snooping database グローバル コンフィギュレーション コマンドを使用します。タイムアウトまたは 遅延時間の値をリセットするには、ip dhcp snooping database timeout *seconds* または ip dhcp snooping database write-delay *seconds* グローバル コンフィギュレーション コマンドを使用します。

DHCP スヌーピング バインディング データベース エージェントの統計情報をクリアするには、clear ip dhcp snooping database statistics 特権 EXEC コマンドを使用します。データベースを更新するに は、renew ip dhcp snooping database 特権 EXEC コマンドを使用します。

DHCP スヌーピング バインディング データベースからバインディング エントリを削除するには、no ip dhcp snooping binding *mac-address* vlan *vlan-id ip-address* interface *interface-id* 特権 EXEC コマ ンドを使用します。このコマンドは、削除するエントリごとに入力します。

DHCP スヌーピング情報の表示

DHCP スヌーピング情報を表示するには、表 20-2 に示す特権 EXEC コマンドを使用します。

表 20-2 DHCP 情報を表示するためのコマンド

コマンド	目的
show ip dhcp snooping	スイッチの DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディ ングだけを表示します。このようなバインディングは、バインディング テーブルと も呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。

(注)

DHCP スヌーピングがイネーブルであり、インターフェイスがダウン ステートに変わった場合、ス イッチは静的に設定されたバインディングを削除しません。

IP ソース ガードの概要

IPSGは、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バイ ンディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド レイヤ2イン ターフェイスでの IP トラフィックを制限するセキュリティ機能です。IP ソース ガードを使用して、ホ ストが、そのネイバの IP アドレスの使用を試みた場合のトラフィック攻撃を防ぐことができます。

IP ソース ガードは、信頼できないインターフェイス上で DHCP スヌーピングがイネーブルにされてい る場合にイネーブルにできます。インターフェイス上で IPSG をイネーブルにすると、スイッチは、 DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべ ての IP トラフィックをブロックします。ポート Access Control List (ACL; アクセス コントロール リ スト)は、このインターフェイスに適用されます。ポート ACL は、IP ソース バインディング テーブ ルに送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他のトラフィックはすべて拒否しま す。

(注)

ポート ACL は、同じインターフェイスに影響を与えるその他のルータ ACL や VLAN マップよりも優 先されます。

IP ソース バインディング テーブル バインディングは、DHCP スヌーピングにより学習されるか、また は手動で設定されます(スタティック IP ソース バインディング)。このテーブルのエントリはすべて、 MAC アドレスと VLAN 番号が関連付けられた IP アドレスを持ちます。スイッチは、IP ソース ガード がイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。 IPSG がサポートされているのは、アクセス ポートおよびとランク ポートを含むレイヤ2 ポートだけで す。送信元 IP アドレス フィルタリングや、送信元 IP および MAC アドレス フィルタリングを使用し て、IPSG を設定することができます。

- 「送信元 IP アドレスのフィルタリング」(P.20-16)
- 「送信元 IP アドレスおよび MAC アドレスのフィルタリング」(P.20-16)
- 「スタティック ホスト用 IP ソース ガード」(P.20-17)

送信元 IP アドレスのフィルタリング

IPSG でこのオプションがイネーブルにされている場合、IP トラフィックは、送信元 IP アドレスに基 づいてフィルタリングされます。スイッチは、送信元 IP が DHCP スヌーピング バインディング デー タベースのエントリ、または IP ソース バインディング テーブルのバインディングと一致する場合に、 IP トラフィックを転送します。

インターフェイス上で、DHCP スヌーピング バインディング、またはスタティック IP ソース バイン ディングが追加、変更、または削除された場合、スイッチは IP ソース バインディングの変更を使用し て、ポート ACL を変更し、このポート ACL をインターフェイスに再度適用します。

IP ソース バインディング (DHCP スヌーピングにより動的に学習された、または手動で設定されたもの) が設定されていないインターフェイス上で IPSG をイネーブルにした場合、スイッチはこのイン ターフェイス上で IP トラフィックすべてを拒否するポート ACL を作成し、適用します。IP ソース ガードをディセーブルにした場合、スイッチはインターフェイスからポート ACL を削除します。

送信元 IP アドレスおよび MAC アドレスのフィルタリング

IP トラフィックは、送信元 IP アドレスおよび MAC アドレスに基づいてフィルタリングされます。ス イッチは、送信元 IP アドレスと MAC アドレスが IP ソース バインディング テーブルのエントリとー 致する場合だけ、トラフィックを転送します。

アドレス フィルタリングがイネーブルの場合、スイッチは IP トラフィックと非 IP トラフィックを フィルタリングします。IP パケット、または非 IP パケットの送信元 MAC アドレスが有効な IP ソース バインディングと一致する場合、スイッチはこのパケットを転送します。DHCP パケットを除き、そ の他の種類のパケットはすべて、スイッチにより廃棄されます。

スイッチは、送信元 MAC アドレスのフィルタリングにポート セキュリティを使用します。ポート セキュリティ違反が発生した場合、インターフェイスはシャットダウンします。

スタティック ホスト用 IP ソース ガード

(注)

アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード (IPSG) を 使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するもの です。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接 続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持た ないものはすべて廃棄されます。このセキュリティ機能により、非ルーテッド レイヤ 2 インターフェ イス上の IP トラフィックは制限されます。この機能は、DHCP スヌーピング バインディング データ ベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリング します。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エント リに依存していまます。このスイッチは、指定されたポートで有効なホストのリストを維持するため に、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。ま た、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイ ヤ3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、 IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デ バイス トラッキング テーブルは同じエントリを学習します。show ip device tracking all 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であ ると表示されます。



(注) 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェ イスに無効なパケットを注入することができます。この無効なパケットには、ソース アドレス として、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが 含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバイ ンディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法 については、対応するオペレーティングシステムとネットワーク インターフェイスのベンダー にお問い合せください。

最初、スタティックホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バ インディング、または MAC バインディングを学習します。IP バインディング、または MAC バイン ディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これ らはデバイストラッキング データベースに保存されます。指定されたポートで動的に学習、または静 的に設定された IP アドレスの数が最大値に達した場合、新しい IP アドレスを持つパケットはすべて、 ハードウェアにより廃棄されます。何らかの理由で移動された、またはなくなったホストを解決するた めに、スタティック ホスト用 IPSG は IP デバイストラッキングを活用して、動的に学習した IP アド レス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用でき ます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立 されます。たとえば、バインディングは、デバイストラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定

- 「デフォルトの IP ソース ガード設定」(P.20-18)
- 「IP ソース ガード設定時の注意事項」(P.20-18)
- 「IP ソース ガードのイネーブル化」(P.20-19)
- 「スタティック ホスト用 IP ソース ガードの設定」(P.20-20)

デフォルトの IP ソース ガード設定

IP ソース ガードは、デフォルトではディセーブルに設定されています。

IP ソース ガード設定時の注意事項

 スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド イン ターフェイスで ip source binding mac-address vlan vlan-id ip-address interface interface-id グ ローバル コンフィギュレーション コマンドに入力すると、次のエラー メッセージが表示されま す。

Static IP source binding can only be configured on switch port.

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これら すべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。



- (注) IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切 にトラフィックをフィルタリングできない可能性があります。
- 送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、 インターフェイスの DHCP スヌーピングとポート セキュリティをイネーブルにする必要がありま す。また、ip dhcp snooping information option グローバル コンフィギュレーション コマンドを 入力して、DHCP サーバに確実にオプション 82 をサポートさせる必要もあります。MAC アドレ スフィルタリングとともに IP ソース ガードをイネーブルにした場合、DHCP ホストによりリース が認可されるまで、このホストの MAC アドレスは学習されません。サーバからホストにパケット を転送する場合、DHCP スヌーピングはオプション 82 データを使用して、ホスト ポートを識別し ます。
- プライベート VLAN が設定されているインターフェイスに IP ソース ガードを設定した場合、ポート セキュリティはサポートされません。
- EtherChannels では、IP ソース ガードはサポートされません。
- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- Ternary Content Addressable Memory (TCAM) エントリの数が最大値を超えた場合、CPU の使 用率は増加します。

IP ソース ガードのイネーブル化

特権 EXEC モードで開始します。

	コマンド	目的	
ステップ 1	configure terminal	· ローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。	
ステップ 3	ip verify source または	送信元 IP アドレス フィルタリングによる IP ソース ガードをイネー ブルにします。	
	ip verify source port-security	送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。	
		(注) ip verify source port-security インターフェイス コンフィ ギュレーション コマンドを使用して、IP ソース ガードと ポート セキュリティの両方をイネーブルにする場合は次の 2 点に注意してください。	
		 DHCP サーバはオプション 82 をサポートしなければなりません。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 	
		 DHCP パケットの MAC アドレスが、セキュア アドレスとして学習されることはありません。DHCP クライアントのMAC アドレスがセキュア アドレスとして学習されるには、スイッチが非 DHCP データ トラフィックを受信した場合だけです。 	
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。	
ステップ 5	ip source binding mac-address vlan vlan-id ip-address inteface interface-id	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。	
ステップ 6	end	特権 EXEC モードに戻ります。	
ステップ 7	<pre>show ip verify source [interface interface-id]</pre>	IP ソース ガードの設定を確認します。	
ステップ 8	show ip source binding [<i>ip-address</i>] [<i>mac-address</i>] [dhcp-snooping static] [inteface <i>interface-id</i>] [vlan <i>vlan-id</i>]	スイッチ、特定の VLAN、または特定のインターフェイス上に IP ソース バインディングを表示します。	
ステップ 9	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。	

送信元 IP アドレス フィルタリングによる IP ソース ガードをディセーブルにするには、no ip verify source インターフェイス コンフィギュレーション コマンドを使用します。

スタティック IP ソース バインディング エントリを削除するには、no ip source グローバル コンフィ ギュレーション コマンドを使用します。

次の例では、VLAN 10 および 11 で、送信元 IP および MAC フィルタリングによる IP ソース ガード をイネーブルにする方法を示します。

Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# interface gigabitethernet0/1 Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet0/1
Switch(config)# end

スタティック ホスト用 IP ソース ガードの設定

• 「レイヤ2アクセスポートでのスタティックホスト用 IP ソースガードの設定」(P.20-20)

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティック ホスト用 IPSG を動作させるには、ip device tracking maximum limit-number インター フェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。ポートでこのコ マンドを設定しただけで、IP デバイス トラッキングをグローバルにイネーブルにしなかった場合、ま たはこのインターフェイスで IP デバイス トラッキングを最大値に設定した場合、スタティック ホスト を持つ IPSG は、このインターフェイスからの IP トラフィックをすべて拒否します。特権 EXEC モー ドで次の手順を実行します。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始し ます。		
ステップ 2	ip device tracking	IP ホスト テーブルをオンにし、IP デバイス トラッキ ングをグローバルにイネーブルにします。		
ステップ 3	interface interface-id	インターフェイス コンフィギュレーション モードを 開始します。		
ステップ 4	switchport mode access	ポートをアクセスとして設定します。		
ステップ 5	switchport access vlan vlan-id	このポート用の VLAN を設定します。		
ステップ 6	ip verify source tracking port-security	MACアドレスフィルタリングとともにスタティック ホスト用 IPSG をイネーブルにします。		
		(注) ip verify source port-security インターフェ イス コンフィギュレーション コマンドを使用 して、IP ソース ガードとポート セキュリ ティの両方をイネーブルにする場合、		
		 DHCP サーバはオプション 82 をサポートしなければなりません。サポートしていない場合、クライアントには IP アドレスを割り当てることができません。 		
		 DHCP パケットの MAC アドレスが、セキュ ア アドレスとして学習されることはありま せん。DHCP クライアントの MAC アドレス がセキュア アドレスとして学習されるには、 スイッチが非 DHCP データ トラフィックを 受信した場合だけです。 		

	コマンド	目的		
ステップ 7	ip device tracking maximum number	そのポートで、IP デバイス トラッキング テーブルに より許可されるスタティック IP 数の上限を設定しま す。指定できる範囲は 1 ~ 10 です。最大値は 10 で す。		
		(注) ip device tracking maximum limit-number イ ンターフェイス コンフィギュレーション コマ ンドを設定する必要があります。		
ステップ 8	switchport port-security	(任意) このポートのポート セキュリティをアクティ ブにします。		
ステップ 9	switchport port-security maximum value	(任意) このポートに対する MAC アドレスの最大値 を設定します。		
ステップ 10	end	特権 EXEC モードに戻ります。		
ステップ 11	show ip verify source interface interface-id	設定を確認し、スタティックホストに対する IPSG 許可 ACL を表示します。		
ステップ 12	show ip device track all [active inactive] count	スイッチ インターフェイス上の指定されたホストに 対する IP/MAC バインディングを表示して、設定を 確認します。		
		 アクティブであるものすべて:アクティブな IP または MAC バインディング エントリだけを表 示します 		
		 非アクティブであるものすべて:非アクティブな IP または MAC バインディング エントリだけを 表示します 		
		 すべて:アクティブおよび非アクティブな IP または MAC バインディング エントリを表示します 		

次に、インターフェイス上でスタティックホストを使って IPSG を停止する例を示します。

Switch(config-if)# no ip verify source Switch(config-if)# no ip device tracking max

次に、ポート上でスタティックホストを使って IPSG をイネーブルにする例を示します。

Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security

次に、レイヤ2アクセスポートで IP フィルターを使用してスタティックホスト用 IPSG をイネーブル にし、インターフェイス Gi0/3 で有効な IP バインディングを確認する例を示します。

Switch# configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking
Switch(config-if)# end
```

Switch# show ip verify source

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Gi0/3	ip trk	active	40.1.1.24		10
Gi0/3	ip trk	active	40.1.1.20		10
Gi0/3	ip trk	active	40.1.1.21		10

次に、レイヤ2アクセスポートで IP-MAC フィルターを使用してスタティック ホスト用 IPSG をイ ネーブルにし、インターフェイス Gi0/3 で有効な IP-MAC バインディングを確認してから、このイン ターフェイス上で上限に達したバインディングの数を確認する例を示します。

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# ip device tracking Switch(config)# interface gigabitethernet 0/3 Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan 1 Switch(config-if)# ip device tracking maximum 5 Switch(config-if)# switchport port-security Switch(config-if)# switchport port-security maximum 5 Switch(config-if)# ip verify source tracking port-security Switch(config-if)# ip verify source tracking port-security Switch(config-if)# ip verify source tracking port-security

Switch# show ip verify source

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
Gi0/3	ip-mac trk	active	40.1.1.24	00:00:00:00:03:04	1
Gi0/3	ip-mac trk	active	40.1.1.20	00:00:00:00:03:05	1
Gi0/3	ip-mac trk	active	40.1.1.21	00:00:00:00:03:06	1
Gi0/3	ip-mac trk	active	40.1.1.22	00:00:00:00:03:07	1
Gi0/3	ip-mac trk	active	40.1.1.23	00:00:00:00:03:08	1

この例は、すべてのインターフェイスに対する IP または MAC バインディング エントリをすべて表示 します。CLI はアクティブ エントリと非アクティブ エントリの両方を表示します。インターフェイス でホストが学習されると、この新しいエントリは、アクティブとマークされます。このホストをこのイ ンターフェイスから切断し、別のインターフェイスに接続すると、ホストを検出すると同時に、新しい IP または MAC バインディング エントリがアクティブとして表示されます。以前のインターフェイス では、このホストに対する古いエントリが非アクティブとマークされます。

```
Switch# show ip device tracking all
```

```
IP Device Tracking = Enabled
```

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.8	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.9	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.10	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.1	0001.0600.0000	9	GigabitEthernet0/2	ACTIVE

200.1.1.1	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet0/2	ACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet0/2	ACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet0/2	ACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet0/2	ACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE

この例は、すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリをすべて表示します。

```
Switch# show ip device tracking all active

IP Device Tracking = Enabled

IP Device Tracking Probe Count = 3

IP Device Tracking Probe Interval = 30
```

IP Address	MAC Address	Vlan	Interface	STATE
200.1.1.1	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.2	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.3	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.4	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE
200.1.1.5	0001.0600.0000	9	GigabitEthernet0/1	ACTIVE

この例は、すべてのインターフェイスに対する非アクティブな IP または MAC バインディング エント リをすべて表示します。このホストはまず、GigabitEthernet 0/1 で学習され、次に GigabitEthernet 0/2 で移動されます。GigabitEthernet 0/1 で学習された IP または MAC バインディング エントリは非アク ティブとマークされます。

```
Switch# show ip device tracking all inactive

IP Device Tracking = Enabled

IP Device Tracking Probe Count = 3

IP Device Tracking Probe Interval = 30

IP Address MAC Address Vlan Interface STATE

200.1.1.8 0001.0600.0000 8 GigabitEthernet0/1 INACTIVE

200.1.1.9 0001.0600.0000 8 GigabitEthernet0/1 INACTIVE

200.1.1.10 0001.0600.0000 8 GigabitEthernet0/1 INACTIVE

200.1.1.1 0001.0600.0000 8 GigabitEthernet0/1 INACTIVE

200.1.1.1 0001.0600.0000 8 GigabitEthernet0/1 INACTIVE
```

200.1.1.1	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.2	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.3	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.4	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.5	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.6	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE
200.1.1.7	0001.0600.0000	8	GigabitEthernet0/1	INACTIVE

この例は、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの 総数を表示します。

```
Switch# show ip device tracking all count

Total IP Device Tracking Host entries: 5

Interface Maximum Limit Number of Entries

Gi0/3 5
```

IP ソース ガード情報の表示

IP ソース ガード情報を表示するには、表 20-3の特権 EXEC コマンドを1つ以上使用します。

表 20-3 IP ソース ガード情報を表示するためのコマンド

コマンド	目的
show ip device tracking	すべてのインターフェイスに対してアクティブな IP または MAC バインディング エントリを表示します。
show ip source binding	スイッチ上の IP ソース バインディングを表示します。
show ip verify source	スイッチ上の IP ソース ガード設定を表示します。

DHCP サーバ ポートベースのアドレス割り当ての概要

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはク ライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アド レスを維持できるようにする機能です。

ネットワークに導入されたイーサネットスイッチは、直接接続されたデバイスに接続を提供します。 工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、その ネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この 代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタ リングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待 しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り 当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接 続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが 変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。 DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識 別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレ スにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID ま たはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアン ト ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイス に、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

DHCP サーバ ポートベースのアドレス割り当ての設定

ここでは、次の設定情報について説明します。

- 「ポートベースのアドレス テーブルのデフォルト設定」(P.20-25)
- 「ポートベースのアドレス割り当て設定時の注意事項」(P.20-25)
- 「DHCP サーバ ポートベースのアドレス割り当てのイネーブル化」(P.20-25)

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

ここでは、DHCP ポートベースのアドレス割り当て設定時の注意事項を説明します。

- 1 つのポートに付き割り当てることができる IP アドレスは1 つだけです。
- 専用アドレス(事前に設定されたアドレス)は、clear ip dhcp binding グローバル コンフィギュ レーション コマンドではクリアできません。
- 事前に設定されたアドレスは、通常の動的な IP アドレス割り当てからは自動的に除外されます。
 ホスト プールでは、事前に設定されたアドレスは使用できませんが、1 つの DHCP アドレス プールに対して複数のアドレスを事前に設定することはできます。
- DHCP プールから事前に設定された予約への割り当てを制限する(予約されていないアドレスは クライアントに提供されず、その他のクライアントはプールによるサービスを受けない)ために、 reserved-only DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を 自動的に生成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始	
		します。	
ステップ 2	ip dhcp use subscriber-id client-id	すべての着信 DHCP メッセージで、加入者 ID が クライアント ID としてグローバルに使用されるよ うに DHCP サーバを設定します。	
ステップ 3	ip dhcp subscriber-id interface-name	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。	
		特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。	
ステップ 4	interface interface-id	設定するインターフェイスを指定し、インター フェイス コンフィギュレーション モードを開始し ます。	

	コマンド	目的		
ステップ 5	ip dhcp server use subscriber-id client-id	インターフェイス上ですべての着信 DHCP メッ		
		セージで、加入者 ID がクライアント ID として使		
		用されるように DHCP サーバを設定します。		
ステップ 6	end	特権 EXEC モードに戻ります。		
ステップ 7	show running config	設定を確認します。		
ステップ 8	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定		
		を保存します。		

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、ip dhcp pool グ ローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアント への関連付けを行います。DHCP プールから事前に設定された予約への割り当てを制限するために、 reserved-only DHCP プール コンフィギュレーション コマンドを入力することができます。ネット ワークに含まれているアドレスやプール範囲にあるアドレスでも、予約されていないアドレスはクライ アントに提供されず、他のクライアントには DHCP プールのサービスが提供されません。ユーザはこ のコマンドを使用して、DHCP プールを装備した1 組のスイッチが共通の IP サブネットを共有し、他 のスイッチのクライアントからの要求を無視するように設定できます。

IP アドレスを事前に割り当て、これをインターフェイス名で識別されるクライアントに関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始
		します。
ステップ 2	ip dhcp pool poolname	DHCP プール コンフィギュレーション モードを開 始し、DHCP プールの名前を定義します。プール 名は、記号文字列(Engineering など)または整 数(0 など)です。
ステップ 3	network <i>network-number</i> [<i>mask</i> / <i>prefix-length</i>]	DHCP アドレス プールのサブネット ネットワーク 番号とマスクを指定します。
ステップ 4	address ip-address client-id string [ascii]	インターフェイス名で指定された DHCP クライア ントの IP アドレスを予約します。
		<i>string</i> : ASCII 値、または 16 進数値のいずれかで す。
ステップ 5	reserved-only	 (任意) DHCP アドレス プールでは、予約された アドレスだけを使用します。デフォルトでは、 プール アドレスは制限されません。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip dhcp pool	DHCP プール設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定 を保存します。

DHCP ポートベースのアドレス割り当てをディセーブルにするには、no ip dhcp use subscriber-id client-id グローバル コンフィギュレーション コマンドを使用します。加入者 ID の自動生成をディ セーブルにするには、no ip dhcp subscriber-id interface-name グローバル コンフィギュレーション コマンドを使用します。インターフェイス上で加入者 ID をディセーブルにするには、no ip dhcp server use subscriber-id client-id インターフェイス コンフィギュレーション コマンドを使用します。 DHCP プールから IP アドレスの予約を削除するには、no address *ip-address* client-id *string* DHCP プール コンフィギュレーション コマンドを使用します。アドレス プールを非制限に変更するには、no reserved-only DHCP プール コンフィギュレーション コマンドを入力します。

次の例では、加入者 ID が自動的に生成され、DHCP サーバは DHCP メッセージ内のクライアント ID フィールドを一切無視して、その代わりに、加入者の ID を使用しています。加入者 ID はインター フェイスのショート名に基づきます。また、クライアントの事前割り当てされた IP アドレスは 10.1.1.7 です。

```
switch# show running config
Building configuration ...
Current configuration : 4899 bytes
version 12.2
1
hostname switch
1
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
ip dhcp pool dhcppool
network 10.1.1.0 255.255.255.0
address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>
```

次に、事前割り当てされたアドレスが DHCP プールに正常に予約された例を示します。

```
switch# show ip dhcp pool dhcppool
Pool dhcp pool:
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 0
Excluded addresses : 4
Pending event : none
1 subnet is currently in the pool:
                                       Leased/Excluded/Total
Current index IP address range
               10.1.1.1 - 10.1.1.254
10.1.1.1
                                        0 / 4 / 254
1 reserved address is currently in the pool
Address
               Client
10.1.1.7 Et1/0
```

DHCP サーバ ポートベースのアドレス割り当て機能の設定の詳細については、Cisco.com にアクセス し、[Search] フィールドに「*Cisco IOS IP Addressing Services*」と入力して、Cisco IOS ソフトウェア マニュアルを参照してください。また、次の URL でもこのマニュアルにアクセスできます。

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DHCP サーバ ポートベースのアドレス割り当ての表示

DHCP サーバ ポートベースのアドレス割り当て情報を表示するには、表 20-4の特権 EXEC コマンド を1つ以上使用します。

表 20-4 DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface interface id	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバでのアドレス バインディングを表示します。

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド


снартев 21

ダイナミック ARP インスペクションの設定

(注)

ダイナミック ARP インスペクションを使用するには、スイッチが LAN Base イメージを実行している 必要があります。

この章では、Catalyst2960 スイッチにダイナミック アドレス解決プロトコル インスペクション (ダイ ナミック ARP インスペクション)を設定する方法について説明します。この機能では、不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のあ る攻撃を回避することができます。



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

この章で説明する内容は、次のとおりです。

- 「ダイナミック ARP インスペクションの概要」(P.21-2)
- 「ダイナミック ARP インスペクションの設定」(P.21-6)
- 「ダイナミック ARP インスペクション情報の表示」(P.21-17)

ダイナミック ARP インスペクションの概要

ARP は、IP アドレスを MAC アドレスにマッピングすることにより、レイヤ 2 ブロードキャスト ドメ イン内での IP コミュニケーションを提供します。たとえば、ホスト B はホスト A に情報を送信する必 要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャス トドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロード キャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。 しかし、ARP は、ARP 要求が受信されなった場合でも、無償の応答を許可するため、ARP スプーフィ ング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃後、攻撃を受けたデバイ スからのトラフィックはすべて、攻撃者のコンピュータを経由して、ルータ、スイッチ、またはホスト にフローします。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図 21-1 に、 ARP キャッシュ ポイズニングの例を示します。

図 21-1 ARP キャッシュ ポイズニング



ホストA、B、およびCは、インターフェイスA、B、およびC上にあるスイッチに接続されていま す。これらはすべて同一のサブネット上にあります。かっこ内に示されているのは、これらの IP アド レス、および MAC アドレスです。たとえば、ホストA が使用する IP アドレスは IA、MAC アドレス は MA です。ホストA が IP レイヤにあるホストB と通信する必要がある場合、ホストA は IP アドレ ス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレ ス MA にバインドされています。ホストB が応答すると、スイッチ、およびホストA は、IP アドレス が IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA (または IB) で、MAC アドレスが MC のホストに対するバインディン グを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ポイズニングされた ARP キャッシュを持つホス トは、IA または IB を対象としたトラフィックに対する宛先 MAC アドレスとして、MAC アドレス MC を使用します。つまり、このトラフィックは、ホスト C により代行受信されます。ホスト C は IA および IB に関連付けられた正しい MAC アドレスを知っているため、正しい MAC アドレスを宛先と して使用して、代行受信したトラフィックをこれらのホストに転送することができます。ホスト C は 自身をホスト A からホスト B へのトラフィック ストリームに挿入します。おなじみの man-in-the middle 攻撃です。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットの正当性を確認するセキュ リティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに 記録して、廃棄します。この機能により、ネットワークをある種の man-in-the-middle 攻撃から保護す ることができます。 ダイナミック ARP インスペクションにより、有効な ARP 要求と応答だけが確実にリレーされるよう になります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートで ARP 要求および応答をすべて代行受信します
- ローカル ARP キャッシュを更新する前、または適切な宛先にパケットを転送する前に、代行受信 したパケットがそれぞれ、有効な IP/MAC アドレス バインディングを持つかどうかを検証します
- 無効な ARP パケットを廃棄します

ダイナミック ARP インスペクションは、信頼できるデータベースである DHCP スヌーピング バイン ディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パ ケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピング がイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインター フェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送しま す。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケッ トを転送します。

ip arp inspection vlan vlan-range グローバル コンフィギュレーション コマンドを使用して、VLAN ご とにダイナミック ARP インスペクションをイネーブルにすることができます。設定情報については、 「DHCP 環境でのダイナミック ARP インスペクションの設定」(P.21-8) を参照してください。

非 DHCP 環境では、ダイナミック ARP インスペクションは、静的に設定された IP アドレスを持つホ ストに対するユーザ設定の ARP Access Control List (ACL; アクセス コントロール リスト) と照らし 合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、arp access-list acl-name グローバル コンフィギュレーション コマンドを使用します。設定情報について は、「非 DHCP 環境での ARP ACL の設定」(P.21-10) を参照してください。スイッチは廃棄されたパ ケットをログに記録します。ログ バッファの詳細については、「廃棄されたパケットのロギング」 (P.21-5) を参照してください。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イー サネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットを廃棄するようにダイナ ミック ARP インスペクションを設定することができます。このためには、ip arp inspection validate {[src-mac] [dst-mac] [ip]} グローバル コンフィギュレーション コマンドを使用します。詳細について は、「確認検査の実行」(P.21-14) を参照してください。

インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インスペクションは、スイッチの各インターフェイスに信頼状態を関連付けます。 信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インスペクションの確認検査 をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP イ ンスペクションの検証プロセスを受けます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できな いものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。 この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリ ティ チェックをバイパスします。VLAN またはネットワークの他の部分では、その他の検証を行う必 要はありません。信頼設定は、ip arp inspection trust インターフェイス コンフィギュレーション コマ ンドを使用して行います。



信頼状態のコンフィギュレーションは慎重に使用します。インターフェイスを信頼できるものとし て設定すべきときに、信頼できないものとして設定すると、接続が失われます。 図 21-2 では、スイッチ A とスイッチ B の両方が、ホスト1 とホスト 2 を含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト1 とホスト 2 が、スイッチ A に接続している DHCP サーバから IP アドレスを取得している場合、スイッチ A だけが、ホスト1 の IP/MAC アドレ スをバインディングします。したがって、スイッチ A とスイッチ B の間のインターフェイスが信頼で きない場合、ホスト1からの ARP パケットは、スイッチ B により廃棄されます。ホスト1 とホスト 2 の間の接続は失われます。

図 21-2 ダイナミック ARP インスペクションのためにイネーブルにされた VLAN 上の ARP パケット検 証



実際は信頼できないインターフェイスを信頼できるものとして設定すると、ネットワークにセキュリ ティ ホールが残ります。スイッチ A でダイナミック ARP インスペクションが実行されていない場合、 ホスト1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます(および、これらのスイッチ の間のリンクが信頼できるものとして設定されている場合はホスト 2)。この状況は、スイッチ B がダ イナミック ARP インスペクションを実行している場合でも発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッ チに接続された(信頼できないインターフェイス上の)ホストが、そのネットワークにあるその他のホ ストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP イ ンスペクションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インスペクショ ンを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにするこ とはできません。

VLAN のスイッチの一部がダイナミック ARP インスペクションを実行し、残りのスイッチは実行して いない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定しま す。ただし、非ダイナミック ARP インスペクションスイッチからパケットのバインディングを検証す るには、ARP ACL を使用して、ダイナミック ARP インスペクションを実行するスイッチを設定しま す。このようなバインディングが判断できない場合は、レイヤ3で、ダイナミック ARP インスペク ション スイッチを実行していないスイッチから、ダイナミック ARP インスペクションを実行している スイッチを分離します。設定情報については、「非 DHCP 環境での ARP ACL の設定」(P.21-10) を参 照してください。



DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パ ケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチ CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻 撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないイ ンターフェイスの比率は1秒あたり 15 パケット(15 pps)です。信頼できるインターフェイスはレー ト制限されません。この設定は、ip arp inspection limit インターフェイス コンフィギュレーション コ マンドを使用して変更することができます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートに します。ユーザが介入するまで、ポートはそのステートのままです。errordisable 回復をイネーブルに して、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするに は、errdisable recovery グローバル コンフィギュレーション コマンドを使用します。

設定情報については、「着信 ARP パケットのレート制限」(P.21-12)を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的な優先順位

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、 DHCP スヌーピング バインディング データベースが使用されます。

ARP ACL は、DHCP スヌーピング バインディング データベースのエントリよりも優先されます。ス イッチが ACL を使用するのは、ACL が ip arp inspection filter vlan グローバル コンフィギュレー ション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ 設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効 なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパ ケットを拒否します。

廃棄されたパケットのロギング

スイッチがパケットを廃棄すると、ログバッファにエントリが記録され、その割合に応じて、システムメッセージが生成されます。メッセージの生成後、スイッチにより、ログバッファからこのエントリが消去されます。各ログエントリには、受信 VLAN、ポート番号、発信元および宛先 IP アドレス、発信元および宛先 MAC アドレスなどのフロー情報が含まれます。

バッファ内のエントリ数、および指定された期間にシステム メッセージを生成するために必要なエン トリ数を設定するには、ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを 使用します。ログに記録されるパケットのタイプを指定するには、ip arp inspection vlan logging グ ローバル コンフィギュレーション コマンドを使用します。設定情報については、「ログ バッファの設 定」(P.21-15) を参照してください。

ダイナミック ARP インスペクションの設定

ここでは、次の設定情報について説明します。

- 「ダイナミック ARP インスペクションのデフォルト設定」(P.21-6)
- 「ダイナミック ARP インスペクション設定時の注意事項」(P.21-7)
- 「DHCP 環境でのダイナミック ARP インスペクションの設定」(P.21-8)(DHCP 環境では必須)
- 「非 DHCP 環境での ARP ACL の設定」(P.21-10)(非 DHCP 環境では必須)
- 「着信 ARP パケットのレート制限」(P.21-12)(任意)
- 「確認検査の実行」(P.21-14)(任意)
- 「ログバッファの設定」(P.21-15)(任意)

ダイナミック ARP インスペクションのデフォルト設定

表 21-1 に、ダイナミック ARP インスペクションのデフォルト設定を示します。

表 21-1 ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブル
インターフェイス信頼状態	すべてのインターフェイスは信頼できません
着信 ARP パケットのレート制限	このレートは、信頼できないインターフェイス上で15 ppsに設定されています。ただし、1 台のホストが1 秒 間に15 台の新規ホストに接続できるスイッチド ネット ワークであると仮定しています。
	信頼できるすべてのインターフェイスでは、レートは 無制限です。
	バースト インターバルは 1 秒に設定されています。
非 DHCP 環境の ARP ACL	ARP ACL は定義されていません
確認検査	どの検証も実行されません。
ログ バッファ	ダイナミック ARP インスペクションがイネーブル化さ れると、拒否または廃棄された ARP パケットはすべて が記録されます。
	ログのエントリ数は 32 です。
	システム メッセージの数は 1 秒あたり 5 つに制限され ています。
	ロギングレート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄された ARP パケットは、すべて記録さ れます。

ダイナミック ARP インスペクション設定時の注意事項

ダイナミック ARP インスペクション設定時の注意事項は次のとおりです。

- ダイナミック ARP インスペクションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていな いスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては 有効ではありません。man-in-the-middle 攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限 されているため、チェックされないドメインと、ダイナミック ARP インスペクションにより チェックされるドメインは区別します。このアクションは、ダイナミック ARP インスペクション のためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナ ミック ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依 存します。動的に割り当てられた IP アドレスを持つ ARP パケットを許可する DHCP スヌーピン グを必ずイネーブルにしてください。設定情報については、第 20 章「DHCP 機能 および IP ソー スガード機能の設定」を参照してください。

DHCP スヌーピングがディセーブルにされているか、または非 DHCP 環境にある場合は、ARP ACL を使用して、パケットを許可、または拒否してください。

ダイナミック ARP インスペクションは、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポート上でサポートされています。



RSPAN VLAN では、ダイナミック ARP インスペクションをイネーブルにしないでください。 RSPAN VLAN でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに届かない可能性があります。

 物理ポートは、この物理ポートの信頼状態とチャネルポートの信頼状態が一致する場合だけ、 EtherChannel ポートチャネルに加入できます。一致しない場合、物理ポートは、ポートチャネル でサスペンドされたままになります。ポートチャネルは、信頼状態を、チャネルに加入した最初 の物理ポートから継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態 と一致する必要はありません。

逆に、ポート チャネルで信頼状態を変更すると、スイッチは、チャネルを構成するすべての物理 ポートで新しい信頼状態を設定します。

 ポート チャネルの動作レートは、チャネル内の物理ポートすべてにわたって累積されます。たと えば、ARP レート制限が 400 pps のポート チャネルを設定した場合、チャネル上で組み合わされ ているすべてのインターフェイスは、合計 400 pps を受け取ります。EtherChannel ポート上での着 信 ARP パケットのレートは、すべてのチャネル メンバからの着信パケットのレートの合計と同じ になります。EtherChannel ポートのレート制限は、必ずすべてのチャネルポート メンバすべての 着信 ARP パケットのレートを調べてから設定してください。

物理ポートでの着信パケットのレートは、物理ポートの設定ではなく、ポートチャネルの設定に対してチェックされます。ポート チャネルのレート制限の設定は、物理ポートの設定とは関係ありません。

EtherChannel が、設定されたレートよりも多くの ARP パケットを受信している場合、チャネル (すべての物理ポートを含む) は、errdisable ステートに置かれます。

- 着信トランクポートで、ARPパケットのレートを必ず制限してください。トランクポートの集約 を反映し、複数のダイナミックARPインスペクションがイネーブルにされた VLAN にわたってパ ケットを処理するために、トランクポートのレートをより高く設定します。また、ip arp inspection limit none インターフェイス コンフィギュレーション コマンドを使用して、レートを 無制限に設定することもできます。VLAN でレート制限を高くすると、ソフトウェアがこのポー トを errdisable ステートにしたときに、他の VLAN が DoS 攻撃を受ける原因となります。
- スイッチで、ダイナミック ARP インスペクションをイネーブルにすると、ARP トラフィックをポ リシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラ フィックは CPU に送信されます。

DHCP 環境でのダイナミック ARP インスペクションの設定

この手順では、2 つのスイッチがダイナミック ARP インスペクションをサポートしているときに、こ の機能を設定する方法を示します。図 21-2 (P.21-4) に示すとおり、ホスト1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています。スイッチは両方とも、ホストの配置されている VLAN 1 でダイ ナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。 どちらのホストも、同一の DHCP サーバから IP アドレスを取得します。したがって、スイッチ A はホ スト1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを 持ちます。



着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミッ ク ARP インスペクション DHCP スヌーピング バインディング データベースのエントリに依存します。 動的に割り当てられた IP アドレスを持つ ARP パケットを許可する DHCP スヌーピングを必ずイネー ブルにしてください。設定情報については、第 20 章「DHCP 機能 および IP ソース ガード機能の設定」 を参照してください。

スイッチの1つだけがこの機能をサポートしている場合にダイナミック ARP インスペクションを設定 する方法の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.21-10)を参照してください。

ダイナミック ARP インスペクションを設定するには、特権 EXEC モードで次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	show cdp neighbors	スイッチ間の接続を確認します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip arp inspection vlan vlan-range	VLAN 単位で、ダイナミック ARP インスペクションをイ ネーブルにします。デフォルトでは、すべての VLAN 上で ダイナミック ARP インスペクションはディセーブルになっ ています。
		<i>vlan-range</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマ で区切られた一連の VLAN を指定できます。指定できる範 囲は 1 ~ 4094 です。
		両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	interface interface-id	もう1つのスイッチに接続するインターフェイスを指定し、 インターフェイス コンフィギュレーション モードを開始し ます。

	コマンド	目的
ステップ 5	ip arp inspection trust	スイッチ間の接続を、信頼できるものに設定します。
		デフォルトでは、すべてのインターフェイスは信頼できませ
		h_{\circ}
		スイッチは、信頼できるインターフェイスにあるもう1つの スイッチから受信した ARP パケットは確認しません。これ らのパケットを転送するだけです。
		信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッ シュを更新し、該当する宛先にパケットを転送する前に、代 行受信したパケットが有効な IP/MAC アドレス バインディ ングを持つかどうかを検証します。スイッチは、無効なパ ケットを廃棄し、ip arp inspection vlan logging グローバル
		に従ってログ バッファに記録します。詳細については、「ロ グ バッファの設定」(P.21-15)を参照してください。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show ip arp inspection interfaces	ダイナミック ARP インスペクションの設定を確認します。
	show ip arp inspection vlan vlan-range	
ステップ 8	show ip dhcp snooping binding	DHCP バインディングを確認します。
ステップ 9	show ip arp inspection statistics vlan <i>vlan-range</i>	ダイナミック ARP インスペクション統計情報を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

ダイナミック ARP インスペクションをディセーブルにするには、no ip arp inspection vlan vlan-range グローバル コンフィギュレーション コマンドを使用します。インターフェイスを untrusted ステートに戻すには、no ip arp inspection trust インターフェイス コンフィギュレーション コマンド を使用します。

次の例では、VLAN1のスイッチ A でダイナミック ARP インスペクションを設定する方法を示しま す。スイッチ B でも同様の手順を実行します。

Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust

非 DHCP 環境での ARP ACL の設定

この手順は、図 21-2 (P.21-4) に示すスイッチ B がダイナミック ARP インスペクション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インスペクションを設定する方法 を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、ス イッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。 これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホ スト 2 から ARP パケットを許可するには、ARP ACL を設定し、これを VLAN 1 に適用しなければな りません。ホスト 2 の IP アドレスがスタティックではない(スイッチ A で ACL 設定を適用すること は不可能である)場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを 使用してパケットをルートする必要があります。

スイッチ A 上で ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、 非 DHCP 環境では必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	arp access-list acl-name	ARP ACL を定義し、ARP アクセス リスト設定モードを開始します。デフォルトでは、ARP アクセス リストは定義されません。
		(注) ARP アクセス リストの末尾に暗黙的な deny ip any mac any コマンドが指定されています。
ステップ 3	permit ip host sender-ip mac host sender-mac [log]	指定されたホスト(ホスト2)からのARPパケットを許可 します。
		• <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。
		 sender-mac には、ホスト2の MAC アドレスを入力します。
		 (任意) パケットが Access Control Entry (ACE; アクセスコントロールエントリ)と一致するときに、ログバッファにこのパケットをログするには、logを指定します。ip arp inspection vlan logging グローバルコンフィギュレーションコマンドで matchlog キーワードも設定されている場合は、一致するパケットはログに記録されます。詳細については、「ログバッファの設定」(P.21-15)を参照してください。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	ip arp inspection filter <i>arp-acl-name</i> vlan <i>vlan-range</i> [static]	ARP ACL を VLAN に適用します。デフォルトでは、定義 済みの ARP ACL は、どのような VLAN にも適用されませ ん。
		 <i>arp-acl-name</i>には、ステップ2で作成したACLの名前を指定します。
		 <i>vlan-range</i>には、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号で識別された1つの VLAN、それぞれをハイフンで区切った VLAN 範囲、 またはカンマで区切った一連の VLAN を指定できます。 指定できる範囲は1~4094です。
		 (任意) ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、static を指定します。DHCP バインディングは使用されません。
		このキーワードを指定しない場合は、パケットを拒否す る明示的な拒否が ACL 内にないことを意味し、パケッ トが ACL 内の句に一致しないと DHCP バインディング がパケットの許可または拒否を決定します。
		IP/MAC アドレス バインディングだけを含む ARP パケット が ACL と比較されます。パケットが許可されるのは、アク セス リストで許可されている場合だけです。
ステップ 6	interface interface-id	スイッチ B に接続するスイッチ A インターフェイスを指定 し、インターフェイス コンフィギュレーション モードを開 始します。
ステップ 7	no ip arp inspection trust	スイッチ B に接続されたスイッチ A インターフェイスを信 頼できないものとして設定します。
		デフォルトでは、すべてのインターフェイスは信頼できま せん。
		信頼できないインターフェイスの場合、スイッチはすべて の ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する 前に、代行受信したパケットが有効な IP/MAC アドレス バ インディングを持つかどうかを検証します。スイッチは、 無効なパケットを廃棄し、ip arp inspection vlan logging グ ローバル コンフィギュレーション コマンドで指定されたロ ギング設定に従ってログ バッファに記録します。詳細につ いては、「ログ バッファの設定」(P.21-15) を参照してくだ さい。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show arp access-list [acl-name]	設定を確認します。
	show ip arp inspection vlan vlan-range	
	show ip arp inspection interfaces	
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ARP ACL を削除するには、no arp access-list グローバル コンフィギュレーション コマンドを使用し ます。VLAN に接続された ARP ACL を削除するには、no ip arp inspection filter *arp-acl-name* vlan *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチA で ARP ACL *host2* を設定して、ホスト2(IP アドレス 1.1.1.1、および MAC アドレス 0001.0001) からの ARP パケットを許可し、この ACL を VLAN 1 に適用してから、スイッチA のポート1 を信頼できないものに設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチ CPU は、ダイナミック ARP インスペクション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートに します。errordisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのス テートから自動的に抜け出すようにするまで、ポートはこのステートのままです。

(注)

インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、 レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、イン ターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。no ip arp inspection limit インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイス はデフォルトのレート制限に戻ります。

トランクポート、および EtherChannel ポートに対するレート制限設定時の注意事項については、「ダイナミック ARP インスペクション設定時の注意事項」(P.21-7)を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	レート制限されたインターフェイスを指定し、インターフェイス コ
		ンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	<pre>ip arp inspection limit {rate pps [burst interval seconds] none}</pre>	インターフェイスでの着信 ARP 要求および応答のレートを制限します。
		デフォルトのレートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト イン ターバルは 1 秒に設定されています。
		キーワードの意味は次のとおりです。
		 rate pps には、1 秒間に処理される着信パケット数の上限を指定します。指定できる範囲は 0 ~ 2048 pps です。
		 (任意) burst interval seconds は、レートの高い ARP パケットの有無についてインターフェイスが監視される間隔(秒)を指定します。指定できる範囲は 1 ~ 15 です。
		 rate none では、処理できる着信 ARP パケットのレートの上限 を設定しません。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	errdisable recovery cause arp-inspection interval interval	(任意)ダイナミック ARP インスペクション errordisable ステート からのエラー回復をイネーブルにします。
		デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。
		interval <i>interval</i> には、errordisable ステートから回復する時間を秒 単位で指定します。指定できる範囲は 30 ~ 86400 です。
ステップ 6	exit	特権 EXEC モードに戻ります。
ステップ 7	show ip arp inspection interfaces	設定値を確認します。
	show errdisable recovery	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのレート制限設定に戻るには、no ip arp inspection limit インターフェイス コンフィギュ レーション コマンドを使用します。ダイナミック ARP インスペクションのエラー回復をディセーブル にするには、no errdisable recovery cause arp-inspection グローバル コンフィギュレーション コマン ドを使用します。

確認検査の実行

ダイナミック ARP インスペクションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定の検証を実行するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip arp inspection validate {[src-mac] [dst-mac] [ip]}	着信 ARP パケットに対して特定の検証を実行します。デフォルトでは、検証は 実行されません。
		キーワードの意味は次のとおりです。
		 src-mac では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文 の送信元 MAC アドレスが比較されます。この検証は、ARP 要求と ARP 応 答に両方に対して実行されます。このチェックがイネーブルの場合、異な る MAC アドレスを持つパケットは無効として分類され、ドロップされま す。
		 dst-mac では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の 宛先 MAC アドレスが比較されます。この検証は、ARP 応答に対して実行 されます。このチェックがイネーブルの場合、異なる MAC アドレスを持 つパケットは無効として分類され、ドロップされます。
		• ip では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがな いかを確認します。0.0.0.0、255.255.255.255、およびすべての IP マルチ キャスト アドレスがこれに該当します。送信側 IP アドレスは、すべての ARP 要求および応答で検証され、宛先 IP アドレスは ARP 応答だけで検証 されます。
		少なくとも1つのキーワードを指定する必要があります。コマンドを実行する たびに、その前のコマンドの設定は上書きされます。つまり、コマンドが src および dst mac の検証をイネーブルにし、2番目のコマンドが IP 検証だけをイ ネーブルにすると、2番目のコマンドによって src および dst mac の検証がディ セーブルになります。
ステップ 3	exit	特権 EXEC モードに戻ります。
ステップ 4	show ip arp inspection vlan <i>vlan-range</i>	設定値を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

検証をディセーブルにするには、no ip arp inspection validate [src-mac] [dst-mac] [ip] グローバル コ ンフィギュレーション コマンドを使用します。転送されたパケット、廃棄されたパケット、MAC およ び IP 検証に失敗したパケットの統計を表示するには、show ip arp inspection statistics 特権 EXEC コ マンドを使用します。

ログ バッファの設定

スイッチがパケットを廃棄すると、ログ バッファにエントリが記録され、その割合に応じて、システムメッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信 VLAN、ポート番号、発信元および宛先 IP アドレス、発信元および宛先 MAC アドレスなどのフロー情報が含まれます。

1 つのログ バッファ エントリは複数のパケットを表す場合があります。たとえば、インターフェイス が同じ ARP パラメータを使用して同じ VLAN 上で多数のパケットを受信した場合、スイッチはこれら のパケットを組み合わせて1つのエントリとしてログ バッファに格納し、エントリとして1つのシス テム メッセージを生成します。

ログ バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味し ており、show ip arp inspection log 特権 EXEC コマンドの出力が影響を受けます。パケット数および 時間以外のすべてのデータの代わりに [--] が表示されます。このエントリに関してそれ以外の統計情報 は表示されません。このエントリに関する情報が表示されるようにするには、ログ バッファ内のエン トリの数を増やすか、またはロギング レートを高くします。

ログバッファを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip arp inspection log-buffer	ダイナミック ARP インスペクション ログ バッファを設定します。
{entries number logs number interval seconds}	デフォルトでは、ダイナミック ARP インスペクションがイネーブル化 されると、拒否またはコマンドされた ARP パケットが記録されます。 ログ エントリ数は、32 です。システム メッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート インターバルは、1 秒です。	
		キーワードの意味は次のとおりです。
		 entries number は、バッファに記録されるエントリ数を表します。 指定できる範囲は 0 ~ 1024 です。
		 logs number interval seconds は、指定されたインターバルでシス テム メッセージを生成するエントリの数を表します。
	logs <i>number</i> に指定できる範囲は 0 ~ 1024 です。値を 0 に設定す ると、エントリはログ バッファに配置されますが、システム メッ セージが生成されません。	
	指定できる interval <i>seconds</i> の範囲は 0 ~ 86400 秒(1 日)です。 値を 0 に設定すると、システム メッセージがただちに生成されます (ログ バッファは常に空になります)。	
		インターバルの設定0は、ログの設定0よりも優先されます。
	logs および interval の設定は、相互に作用します。logs number X が interval seconds Y より大きい場合は、X を Y で割って (X/Y) 求めら れたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合 は、Y を X で割って (Y/X) 求められた間隔(秒) で 1 つのシステム メッセージが送信されます。	

	コマンド	目的
ステップ 3	ip arp inspection vlan vlan-range logging {acl-match {matchlog none} dhcp-bindings {all none permit}}	VLAN 単位で記録するパケットのタイプを制御します。デフォルトでは、拒否または廃棄されたパケットは、すべて記録されます。ログに記録されるという表現は、エントリがログバッファに格納され、システムメッセージが生成されることを意味しています。
		キーワードの意味は次のとおりです。
		 vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイ フンで区切られた範囲の VLAN、またはカンマで区切られた一連 の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。
		 acl-match matchlog は、ACE ロギング設定に基づいてパケットを ログに記録します。このコマンドに matchlog キーワード、permit または deny ARP アクセス リスト コンフィギュレーション コマン ドに log キーワードを指定すると、ACL によって許可または拒否 された ARP パケットが記録されます。
		 acl-match none では、ACL に一致するパケットは記録されません。
		 dhcp-bindings all では、DHCP バインディングに一致するパケットがすべて記録されます。
		 dhcp-bindings none では、DHCP バインディングに一致するパケットは記録されません。
		 dhcp-bindings permit では、DHCP バインディングが許可された パケットが記録されます。
ステップ 4	exit	特権 EXEC モードに戻ります。
ステップ 5	show ip arp inspection log	設定値を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのログ バッファ設定に戻るには、no ip arp inspection log-buffer {entries | logs} グローバ ル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻るには、no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings} グローバル コンフィギュレー ション コマンドを使用します。ログ バッファをクリアするには、clear ip arp inspection log 特権 EXEC コマンドを使用します。

ダイナミック ARP インスペクション情報の表示

ダイナミック ARP インスペクション情報を表示するには、表 21-2 に記載された特権 EXEC コマンド を使用します。

表 21-2 ダイナミック ARP インスペクション情報を表示するためのコマンド

コマンド	説明
show arp access-list [acl-name]	ARP ACL に関する詳細を表示します。
show ip arp inspection interfaces [interface-id]	指定されたインターフェイスまたはすべてのインターフェイスに関して 信頼状態と ARP パケットのレート制限を表示します。
show ip arp inspection vlan vlan-range	指定された VLAN のダイナミック ARP インスペクションの設定および 動作ステートを表示します。VLAN が指定されていない場合、または範 囲が指定されている場合は、ダイナミック ARP インスペクションがイ ネーブルにされた(アクティブ)VLAN だけの情報を表示します。

ダイナミック ARP インスペクションの統計をクリア、または表示するには、表 21-3 に記載された特権 EXEC コマンドを使用します。

表 21-3 ダイナミック ARP インスペクション統計をクリアまたは表示するためのコマンド

コマンド	説明
clear ip arp inspection statistics	ダイナミック ARP インスペクション統計情報をクリアします。
<pre>show ip arp inspection statistics [vlan vlan-range]</pre>	指定された VLAN の転送済みパケット、廃棄されたパケット、MAC 検 証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許 可および拒否されたパケット、DHCP によって許可および拒否されたパ ケットの統計情報を表示します。VLAN が指定されていない場合、また は範囲が指定されている場合は、ダイナミック ARP インスペクション がイネーブルにされた (アクティブ) VLAN だけの情報を表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペク ション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチ は、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP インスペクションのログ情報をクリア、または表示するには、表 21-4 に記載され た特権 EXEC コマンドを使用します。

表 21-4	ダイナミック ARP インスペクション ログ情報をクリアまたは表示するためのコマンド
--------	--

コマンド	説明
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファを消去しま
	す。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内
	容を表示します。

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

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド





IGMP スヌーピングおよび MVR の設定

(注)

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

この章では、Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピングを Catalyst 2960 スイッチ上で設定する方法について、ローカル IGMP スヌーピング、 Multicast VLAN Registration (MVR) の適用を含めて説明します。また、IGMP フィルタリングを使 用したマルチキャスト グループ メンバシップの制御と、IGMP スロットリング アクションの設定手順 についても説明します。



この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンドリファレンスおよび『*Cisco IOS IP Command Reference, Volume 3 of 3:Multicast, Release 12.2*』の「IP Multicast Routing Commands」のセクションを参照してください。これには、Cisco.com のホームページ(Documentation > Cisco IOS Software > 12.2 Mainline > Command References) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「IGMP スヌーピングの概要」(P.22-2)
- 「IGMP スヌーピングの設定」(P.22-7)
- 「IGMP スヌーピング情報の表示」(P.22-18)
- 「MVR の概要」(P.22-19)
- 「MVR の設定」(P.22-22)
- 「MVR 情報の表示」(P.22-26)
- 「IGMP フィルタリングおよびスロットリングの設定」(P.22-27)
- 「IGMP フィルタリングおよび IGMP スロットリング設定の表示」(P.22-32)

(注)

IGMP スヌーピング、MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理することもできますし、スタティック IP アドレスを使用することもできます。

IGMP スヌーピングの概要

レイヤ2スイッチは IGMP スヌーピングを使用して、レイヤ2インターフェイスを動的に設定し、マ ルチキャストトラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにだけ転 送されるようにすることによって、マルチキャストトラフィックのフラッディングを制限できます。 名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送を スヌーピングし、マルチキャスト グループとメンバー ポートを追跡する必要があります。特定のマル チキャスト グループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番 号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合 は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メン バシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。



IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータは、すべての VLAN に一般クエリーを定期的に送信します。このマルチキャス トトラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加され ます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャス ト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC (メディア アクセス制御) アドレスに基づくグループではなく、IP マルチキャスト グループに基づくブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグルー プの場合、設定されている IP アドレスを設定済みの MAC アドレス (エイリアス) または予約済みの マルチキャスト MAC アドレス (224.0.0.xxx の範囲内) に変換すると、コマンドがエラーになります。 スイッチでは IP マルチキャスト グループを使用するので、アドレス エイリアスの問題は発生しませ ん。

IGMP スヌーピングによって、IP マルチキャスト グループは動的に学習されます。ただし、ip igmp snooping vlan vlan-id static ip_address interface interface-id グローバル コンフィギュレーション コ マンドを使用すると、マルチキャスト グループを静的に設定できます。グループ メンバシップをマル チキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作 より優先されます。マルチキャスト グループ メンバシップのリストは、ユーザが定義した設定値およ び IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャスト トラフィックはルーティングする必要がないのでマルチキャスト インターフェイスを 使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設 定できます。IGMP スヌーピング クエリーの詳細については、「IGMP スヌーピング クエリアの設定」 (P.22-15) を参照してください。

ポート スパニング ツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこの ポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

- 「IGMP バージョン」 (P.22-3)
- •「マルチキャストグループへの加入」(P.22-3)
- 「マルチキャスト グループからの脱退」(P.22-5)
- 「即時脱退」(P.22-6)
- 「IGMP 脱退タイマーの設定」(P.22-6)
- 「IGMP レポート抑制」(P.22-6)

IGMP バージョン

スイッチは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしてい ます。これら 3 つのバージョンは、スイッチ上でそれぞれ相互運用できます。たとえば、IGMPv2 ス イッチ上で IGMP スヌーピングがイネーブルの場合、このスイッチが IGMPv3 レポートをホストから 受信すると、この IGMPv3 レポートをマルチキャスト ルータへ転送できます。

(注)

スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support(BISS)をサポートしています。BISS は、 IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバシップ レポート メッセー ジをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャストト ラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

(注)

IGMP フィルタリングまたは MVR が実行されているスイッチは、IGMPv3 Join および Leave メッ セージをサポートしていません。

IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの 送受信を行うことができます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細について は、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a. html

マルチキャスト グループへの加入

スイッチに接続したホストが IP マルチキャスト グループに加入し、なおかつそのホストが IGMP バー ジョン 2 クライアントの場合、ホストは加入する IP マルチキャスト グループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリーを受信したスイッチ は、そのクエリーを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャスト グループに加入する場合、ホストはスイッチに Join メッセージを送信す ることによって応答します。スイッチの CPU は、そのグループのマルチキャスト転送テーブル エント リがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信 したインターフェイスを転送テーブル エントリに追加します。そのインターフェイスと対応付けられ たホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。図 22-1を 参照してください。



ルータ A がスイッチに一般クエリーを送り、スイッチはそのクエリーをポート 2 ~ 5、つまり同一 VLAN のすべてのメンバーに転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するた めに、グループに IGMP メンバシップ レポート (IGMP Join メッセージ)をマルチキャストします。 スイッチの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します(表 22-1 を参照)。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 22-1 IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2

スイッチのハードウェアは、マルチキャスト グループの他のパケットと IGMP 情報パケットを区別で きます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケットではないフ レームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジン に指示します。

別のホスト(たとえばホスト4)が同じグループに非請求の IGMP Join メッセージを送信する場合 (図 22-2 を参照)、CPU はメッセージを受信して、転送テーブルにホスト4のポート番号を追加します (表 22-2 を参照)。転送テーブルによって、CPU だけに IGMP メッセージが転送されるので、スイッチ 上の他のポートにメッセージがフラッディングされることはありません。既知のマルチキャストトラ フィックはすべて、CPU ではなくグループに転送されます。



図 22-2 2 番めのホストのマルチキャスト グループへの加入

表 22-2 更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータはマルチキャストー般クエリーを定期的に送信し、スイッチはそれらのクエリーを VLAN のす べてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくと も1つのホストがマルチキャスト トラフィックを受信しなければならない場合、ルータは VLAN に引 き続き、マルチキャスト トラフィックを転送します。スイッチは、その IGMP スヌーピングによって 維持された IP マルチキャスト グループの転送テーブルで指定されたホストに対してだけ、マルチキャ スト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッ セージを送信することもできます。ホストから Leave メッセージを受信したスイッチは、グループ固 有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャスト グループのトラフィックに関与しているかどうかを学習します。スイッチはさらに、転送テーブルでそ の MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のある ホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しな かった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

即時脱退機能をサポートするのは、IGMP バージョン2が稼動しているホストだけです。

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチからインターフェイスにグルー プ固有のクエリーを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルか ら削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマル チキャスト グループのマルチキャスト ツリーからプルーニングされます。即時脱退によって、複数の マルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホス トに最適な帯域幅管理が保証されます。

(注)

即時脱退機能を使用するのは、各ポートに接続されているホストが1つだけの VLAN に限定してくだ さい。1つのポートに複数のホストが接続されている VLAN で即時脱退機能をイネーブルにすると、 一部のホストが誤って切断される可能性があります。

設定手順については、「IGMP 即時脱退のイネーブル化」(P.22-11)を参照してください。

IGMP 脱退タイマーの設定

まだ指定のマルチキャスト グループに関心があるかどうかを確認するために、グループ固有のクエ リーを送信した後のスイッチの待機時間を設定できます。IGMP 脱退応答時間は、100 ~ 5000 ミリ秒 の間で設定できます。タイマーはグローバルにまたは VLAN 単位で設定できますが、VLAN に脱退時 間を設定すると、グローバルに設定した脱退時間は上書きされます。

設定手順については、「IGMP 脱退タイマーの設定」(P.22-12)を参照してください。

IGMP レポート抑制

(注)

IGMP レポート抑制がサポートされるのは、マルチキャスト クエリーが IGMPv1 および IGMPv2 レ ポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能はサポートされませ ん。

スイッチは、IGMP レポート抑制を使用して、1 つのマルチキャスト ルータ クエリーごとに IGMP レ ポートを 1 つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブルの場合 (デ フォルト)、このスイッチは、グループに対応するすべてのホストからの最初の IGMP レポートをすべ てのマルチキャスト ルータに送信します。スイッチは、グループに対応する残りの IGMP レポートに ついては、マルチキャスト ルータに送信しません。この機能により、重複したレポートがマルチキャ スト デバイスに送信されるのを防ぎます。

マルチキャスト ルータのクエリーに、IGMPv1 および IGMPv2 レポートだけに対応したレポートが含まれている場合、スイッチはグループ内のすべてのホストから、最初の IGMPv1 または IGMPv2 レポートだけを、すべてのマルチキャスト ルータに転送します。

また、マルチキャスト ルータ クエリーに、IGMPv3 レポートの要求も含まれている場合、スイッチは、 グループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送 します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。設定手順については、「IGMP レポート抑制のディセーブル化」(P.22-17)を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送 先を決定したりできます。ここでは、次の設定情報について説明します。

- 「IGMP スヌーピングのデフォルト設定」(P.22-7)
- 「IGMP スヌーピングのイネーブル化およびディセーブル化」(P.22-8)
- 「スヌーピング方法の設定」(P.22-9)
- 「マルチキャスト ルータ ポートの設定」(P.22-10)
- 「グループに加入するホストの静的な設定」(P.22-11)
- 「IGMP 即時脱退のイネーブル化」(P.22-11)
- 「IGMP 脱退タイマーの設定」(P.22-12)
- 「TCN 関連のコマンドの設定」(P.22-13)
- 「IGMP スヌーピング クエリアの設定」(P.22-15)
- 「IGMP レポート抑制のディセーブル化」(P.22-17)

IGMP スヌーピングのデフォルト設定

表 22-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 22-3 IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャストルータ	未設定
マルチキャスト ルータの学習(スヌーピング)方 式	PIM-DVMRP
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN ¹ フラッド クエリー カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN = Topology Change Notification (トポロジ変更通知)

IGMP スヌーピングのイネーブル化およびディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブルです。グローバルにイ ネーブルまたはディセーブルに設定されている場合、既存のすべての VLAN インターフェイスでもイ ネーブルまたはディセーブルです。デフォルトでは、IGMP スヌーピングはすべての VLAN でイネー ブルですが、VLAN 単位で IGMP スヌーピングをイネーブルおよびディセーブルに設定できます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングよりも優先されます。グローバル ス ヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。 グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブル に設定できます。

スイッチ上で IGMP スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping	既存のすべての VLAN インターフェイスで、IGMP スヌーピングを グローバルにイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、 no ip igmp snooping グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN インターフェイス上で IGMP スヌーピングをイネーブルにするには、特権 EXEC モード で次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
ip igmp snooping vlan vlan-id	 VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、IGMP スターピングをグローバルにイネーブルに設定しておく必要があります。
end	特権 EXEC モードに戻ります。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
	コマンド configure terminal ip igmp snooping vlan <i>vlan-id</i> end copy running-config startup-config

特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、no ip igmp snooping vlan vlan-id グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して 使用します。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ2マルチキャスト エントリごとに転送テーブルに追加 されます。スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol Independent Multicast (PIM) パケット、および Distance Vector Multicast Routing Protocol (DVMRP) パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol (CGMP) パケットの待ち受け
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャスト ルータ ポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パ ケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。デ フォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングし ます。CGMP パケットだけでマルチキャスト ルータ ポートを学習するには、ip igmp snooping vlan vlan-id mrouter learn cgmp グローバル コンフィギュレーション コマンドを使用します。このコマン ドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受 け、その他の CGMP パケットは待ち受けません。PIM パケットと DVMRP パケットだけでマルチキャ スト ルータ ポートを学習するには、ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp グロー バル コンフィギュレーション コマンドを使用します。

(注)

学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャスト ルータがない場合は、ip cgmp router-only コマンドを入力し、ルータに動的にアクセスする必要があ ります。

VLAN インターフェイスがマルチキャスト ルータに動的にアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp pim-dvmrp}	VLAN で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
		マルチキャスト ルータの学習方式を指定します。
		 cgmp: CGMP パケットを待ち受けます。この方法は、制御ト ラフィックを減らす場合に有用です。
		• pim-dvmrp : IGMP クエリーおよび PIM パケットと DVMRP パケットをスヌーピングします。これがデフォルトです。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの学習方式に戻すには、no ip igmp snooping vlan vlan-id mrouter learn cgmp グローバル コンフィギュレーション コマンドを使用します。

次に、CGMP パケットを学習方式として使用するように IGMP スヌーピングを設定する例を示します。

Switch# configure terminal Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp Switch(config)# end

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加(マルチキャスト ルータに静的な接続を追加)するには、スイッ チ上で ip igmp snooping vlan mrouter グローバル コンフィギュレーション コマンドを使用します。

マルチキャスト ルータへの静的な接続をイネーブルにするには、特権 EXEC モードで次の手順を実行 します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。
		 VLAN ID の範囲は1~1001および1006~4094です。
		 インターフェイスは物理インターフェイスにすることも ポートチャネルにすることもできます。指定できるポー トチャネルの範囲は1~6です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping mrouter [vlan vlan-id]	VLAN インターフェイス上で IGMP スヌーピングがイネーブ ルになっていることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

VLAN からマルチキャスト ルータ ポートを削除するには、no ip igmp snooping vlan *vlan-id* mrouter interface *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

Switch# configure terminal

Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2 Switch(config)# end

グループに加入するホストの静的な設定

ホストまたはレイヤ2ポートは通常、マルチキャストグループに動的に加入しますが、インターフェ イス上にホストを静的に設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan vlan-id static ip_address interface interface-id	マルチキャストグループのメンバーとしてレイヤ2ポートを 静的に設定します。
		 vlan-id は、マルチキャスト グループの VLAN ID です。 範囲は1~1001 および 1006~4094 です。
		• <i>ip-address</i> は、グループの IP アドレスです。
		 interface-id は、メンバー ポートです。物理インター フェイスまたはポート チャネル (1~6) に設定できま す。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping groups	メンバー ポートおよび IP アドレスを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除するには、no ip igmp snooping vlan vlan-id static *ip-address* interface *interface-id* グローバル コンフィギュレーション コマンドを使用します。

次に、ポート上のホストを静的に設定する例を示します。

Switch# configure terminal

Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
Switch(config)# end

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、スイッチはポート上で IGMP バージョン 2 の Leave メッ セージを検出した場合、ただちにそのポートを削除します。即時脱退機能を使用するのは、VLAN の 各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。

(注)

即時脱退機能をサポートするのは、IGMP バージョン2 が稼動しているホストだけです。

IGMP 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping vlan vlan-id	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにし
	Immediate-leave	
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	show ip igmp snooping vlan vlan-id	VLAN インターフェイス上で即時脱退がイネーブルになっている ことを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN 上で IGMP 即時脱退をディセーブルにするには、no ip igmp snooping vlan vlan-id immediate-leave グローバル コンフィギュレーション コマンドを使用します。

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end
```

IGMP 脱退タイマーの設定

IGMP 脱退タイマーを設定するときには、次の注意事項に従ってください。

- 脱退時間はグローバルまたは VLAN 単位で設定できます。
- VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
- デフォルトの脱退時間は1000ミリ秒です。
- IGMP の脱退時間の設定は、IGMP バージョン2 が稼動しているホストでのみサポートされます。
- ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

IGMP 脱退タイマーの設定をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping last-member-query-interval <i>time</i>	グローバルに IGMP 脱退タイマーを設定します。指定できる範囲 は 100 ~ 32768 ミリ秒です。デフォルト値は 1000 秒です。
ステップ 3	ip igmp snooping vlan vlan-id last-member-query-interval time	(任意) VLAN インターフェイス上で、IGMP 脱退タイマーを設定 します。指定できる範囲は 100 ~ 32768 ミリ秒です。
		(注) VLAN 上に脱退時間を設定すると、グローバルに設定され た内容は上書きされます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping	(任意)設定された IGMP 脱退タイマーを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、no ip igmp snooping last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。

特定の VLAN から IGMP 脱退タイマーの設定を削除するには、no ip igmp snooping vlan vlan-id last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。

TCN 関連のコマンドの設定

ここでは、TCN イベント中にフラッディングしたマルチキャスト トラフィックを制御する方法を説明 します。

- 「TCN イベント後のマルチキャスト フラッディング時間の制御」(P.22-13)
- 「フラッディングモードからの回復」(P.22-14)
- 「TCN イベント中のマルチキャスト フラッディングのディセーブル化」(P.22-14)

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping ten flood query count グローバル コンフィギュレーション コマンドを使用して、 TCN イベント後にフラッディングするマルチキャスト トラフィックの時間を制御できます。このコマ ンドは、TCN イベント後にフラッディングするマルチキャスト データのトラフィックに対し、一般ク エリー数を設定します。クライアントが場所を変更することで同ポートの受信者がブロックされたあ と、現在転送中の場合、またはポートが Leave メッセージを送信せずにダウンした場合などが、TCN イベントに該当します。

ip igmp snooping tcn flood query count コマンドを使用して、TCN フラッディング クエリー カウン トを1に設定した場合、一般クエリーを1 つ受信するまでフラッディングが続きます。カウントを7 に 設定した場合、一般クエリーを7 つ受信するまでフラッディングが続きます。グループは、TCN イベ ント中に受信した一般クエリーに基づいて再度学習されます。

TCN フラッディング クエリー カウントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping tcn flood query count count	マルチキャスト トラフィックのフラッディングに使用する一般 IGMP クエリー数を指定します。指定できる範囲は 1 ~ 10 です。 デフォルトのフラッディング クエリー カウントは 2 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	TCNの設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのフラッディング クエリー カウントに戻す場合は、no ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンド を使用します。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニング ツリーのルートは特別な IGMP Leave メッセージ (グ ローバル Leave メッセージ) をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、ip igmp snooping ten query solicit グローバル コンフィギュレーション コマンドをイネーブルにしてい る場合、スイッチはスパニング ツリーのルートであるかどうかに関わらず、グローバル Leave メッ セージを送信します。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを 送信して、TCN 中のフラッディング モードからの回復に努めます。スイッチがスパニング ツリーの ルートであれば、このコンフィギュレーション コマンドに関係なく、Leave メッセージが常に送信さ れます。デフォルトでは、クエリー送信要求はディセーブルに設定されています。

スイッチがスパニング ツリー ルートであるかどうかに関わらず、グローバル Leave メッセージを送信 するように設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping tcn query solicit	IGMP Leave (グローバル Leave) メッセージを送信し、TCN イ ベント中のフラッディング モードからの回復を促します。デフォ ルトでは、クエリー送信要求はディセーブルに設定されていま す。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	TCN の設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのクエリー送信要求に戻す場合は、no ip igmp snooping tcn query solicit グローバル コン フィギュレーション コマンド を使用します。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

スイッチは TCN を受信すると、一般クエリーを2つ受信するまで、すべてのポートに対してマルチ キャストトラフィックをフラッディングします。異なるマルチキャストグループのホストに接続して いるポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損 失が発生する可能性があります。その場合、ip igmp snooping tcn flood インターフェイス コンフィ ギュレーション コマンドを使用して、この状態を制御できます。

インターフェイス上でマルチキャスト フラッディングをディセーブルにするには、特権 EXEC モード で次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
no ip igmp snooping ten flood	スパニング ツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。
	デフォルトでは、インターフェイス上のマルチキャスト フラッ ディングはイネーブルです。
exit	特権 EXEC モードに戻ります。

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

インターフェイス上でマルチキャスト フラッディングを再度イネーブルにする場合、ip igmp snooping tcn flood インターフェイス コンフィギュレーション コマンドを使用します。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定するときには、次の注意事項に従ってください。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。イネーブルになると、IGMP ス ヌーピング クエリアはクエリー送信元アドレスとして IP アドレスを使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリア は IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP ア ドレスが指定されていない場合、IGMP クエリアは VLAN Switch Virtual Interface (SVI; スイッ チ仮想インターフェイス) IP アドレス(存在する場合)を使用しようとします。SVI IP アドレス が存在しない場合、スイッチはスイッチ上で設定された利用可能な最初の IP アドレスを使用しま す。利用可能な最初の IP アドレスは、show ip interface 特権 EXEC コマンドの出力に表示されま す。IGMP スヌーピング クエリアはスイッチ上で利用可能な IP アドレスを検出できない場合、 IGMP 一般クエリーを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
 - IGMP スヌーピングが VLAN でディセーブルの場合
 - PIM が、VLAN に対応する SVI でイネーブルの場合

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp snooping querier	IGMP スヌーピング クエリア機能をイネーブルにします。
ステップ 3	ip igmp snooping querier address <i>ip_address</i>	(任意)IGMP スヌーピング クエリアの IP アドレスを指定しま す。IP アドレスを指定しない場合、クエリアは IGMP クエリア に設定されたグローバル IP アドレスを使用しようとします。
		(注) IGMP スヌーピング クエリアはスイッチ上で IP アドレス を検出できない場合、IGMP 一般クエリーを生成しませ ん。
ステップ 4	ip igmp snooping querier query-interval <i>interval-count</i>	(任意) IGMP クエリアの間隔を設定します。指定できる範囲は1~1~18000 秒です。

	コマンド	目的
ステップ 5	ip igmp snooping querier tcn query [count count interval interval]	(任意) Topology Change Notification (TCN; トポロジ変更通知) クエリーの間隔を設定します。指定できる count の範囲は $1 \sim 10$ です。指定できる interval の範囲は $1 \sim 255$ 秒です。
ステップ 6	ip igmp snooping querier timer expiry <i>timeout</i>	(任意) IGMP クエリアが期限切れになるまでの時間を設定しま す。指定できる範囲は 60 ~ 300 秒です。
ステップ 7	ip igmp snooping querier version version	(任意) クエリア機能が使用する IGMP バージョン番号 1 または 2 を選択します。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show ip igmp snooping vlan vlan-id	(任意) VLAN インターフェイス上で IGMP スヌーピング クエリ アがイネーブルになっていることを確認します。VLAN ID の範 囲は1~1001 および 1006~4094 です。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

Switch# configure terminal Switch(config)# ip igmp snooping querier 10.0.0.64 Switch(config)# end

次に、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end

次に、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する例を示します。

Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end

IGMP レポート抑制のディセーブル化

(注)

IGMP レポート抑制がサポートされるのは、マルチキャスト クエリーが IGMPv1 および IGMPv2 レ ポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能はサポートされませ ん。

IGMP レポート抑制はデフォルトでイネーブルです。IGMP レポート抑制がイネーブルの場合、スイッチは、マルチキャスト ルータ クエリーごとに IGMP レポートを1 つだけ転送します。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。

IGMP レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no ip igmp snooping report-suppression	IGMP レポート抑制をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip igmp snooping	IGMP レポート抑制がディセーブルになっていることを確認 します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま す。

IGMP レポート抑制を再びイネーブルにする場合は、ip igmp snooping report-suppression グローバ ル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

動的に学習された、あるいは静的に設定されたルータ ポートおよび VLAN インターフェイスに関する IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP アド レス マルチキャスト エントリを表示することもできます。

IGMP スヌーピング情報を表示するには、表 22-4 の特権 EXEC コマンドを1 つまたは複数使用します。

表 22-4 IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
<pre>show ip igmp snooping [vlan vlan-id]</pre>	スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設 定情報を表示します。
	(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入 力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ip igmp snooping groups [count dynamic [count] user [count]]	スイッチまたは特定のパラメータに関して、マルチキャスト テーブル 情報を表示します。
	 count:実際のエントリではなく、特定のコマンドオプションに対応するエントリの総数を表示します。
	 dynamic : IGMP スヌーピングによって学習されたエントリを表示します。
	• user:ユーザによって設定されたマルチキャストエントリだけを 表示します。
show ip igmp snooping groups vlan vlan-id [ip_address count dynamic [count]	マルチキャスト VLAN またはその VLAN の特定のパラメータについ て、マルチキャスト テーブル情報を表示します。
user[count]]	• <i>vlan-id</i> : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
	 count:実際のエントリではなく、特定のコマンドオプションに対応するエントリの総数を表示します。
	 dynamic : IGMP スヌーピングによって学習されたエントリを表示します。
	 <i>ip_address</i>:指定のグループ IP アドレスのマルチキャスト グループ について、特性を表示します。
	 user:ユーザによって設定されたマルチキャストエントリだけを 表示します。
<pre>show ip igmp snooping mrouter [vlan vlan-id]</pre>	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。
	(注) IGMP スヌーピングをイネーブルにすると、スイッチはマルチ キャスト ルータの接続先インターフェイスを自動的に学習しま す。これらのインターフェイスは動的に学習されます。
	(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入 力します。
表 22-4 IGMP スヌーピング情報を表示するためのコマンド (続き)

コマンド	目的
<pre>show ip igmp snooping querier [vlan vlan-id]</pre>	IP アドレス、および VLAN で受信した最新の IGMP クエリー メッ セージの受信ポートに関する情報を表示します。
	(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入 力します。
show ip igmp snooping querier [vlan <i>vlan-id</i>] detail	IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセー ジの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリア の設定および動作ステートに関する情報を表示します。

各コマンドのキーワードおよびオプションの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

MVR の概要



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

MVR は、イーサネット リング ベースのサービス プロバイダー ネットワークにおいて、マルチキャス トトラフィックを大規模展開するアプリケーション(サービス プロバイダー ネットワークによる複数 のテレビ チャネルのブロードキャストなど)を想定して開発されました。MVR によってポート上の加 入者は、ネットワークワイドなマルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退 できます。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有 できます。MVR によって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力 が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されま す。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャ ストストリームへの加入および脱退 (Join および Leave) を行うことが前提です。これらのメッセー ジは、イーサネットで接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作しま す。それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。ただ し、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマル チキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

スイッチの CPU は、MVR IP マルチキャストストリームとそれに対応するスイッチ転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マ ルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。この転送動作により、異なる VLAN の間でトラフィック を選択して伝送できます。 スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポート に転送されます。MVR データ ポートの MVR ホスト メンバシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入して いるレシーバー ポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッ チに設定された MVR データ ポートから転送されることはありません。
- ダイナミックモードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、 IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアント ポートから転送されます。それ以外のポートからは転送されません。 MVR ホストから受信した IGMP レポートも、スイッチのすべての MVR データ ポートから転送さ れます。したがって、互換モードでスイッチを稼動させた場合と異なり、MVR データ ポート リン クで不要な帯域幅を使用しなくてすみます。

MVR に関与するのはレイヤ2ポートだけです。ポートを MVR レシーバー ポートとして設定する必要 があります。各スイッチ スタックでサポートされる MVR マルチキャスト VLAN は、1 つだけです。

マルチキャスト TV アプリケーションで MVR を使用する場合

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備したテレビでマル チキャスト ストリームを受信できます。1 つの加入者ポートに複数のセットトップ ボックスまたは PC を接続できます。加入者ポートは、MVR レシーバー ポートとして設定されたスイッチ ポートです。 図 22-3 に構成例を示します。Dynamic Host Configuration Protocol (DHCP) はセットトップ ボック スまたは PC に IP アドレスを割り当てます。加入者がチャネルを選択すると、セットトップ ボックス または PC からスイッチ A に、所定のマルチキャストに加入するための IGMP レポートが送信されま す。IGMP レポートが設定されている IP マルチキャスト グループ アドレスの1 つと一致すると、ス イッチの CPU がハードウェア アドレス テーブルを変更して、指定のマルチキャスト ストリームをマ ルチキャスト VLAN から受信したときの転送先として、レシーバー ポートと VLAN を追加します。 マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを MVR 送信 元ポートといいます。



図 22-3 MVRの例

加入者がチャネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップボッ クスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバー ポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、 同じグループに加入している別のセットトップ ボックスがある場合、そのセットトップ ボックスはク エリーに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はそのグループの転送先としてのレシーバー ポートを除外します。

即時脱退機能を使用しない場合、レシーバー ポートの加入者から IGMP Leave メッセージを受信した スイッチは、そのポートに IGMP クエリーを送信し、IGMP グループ メンバシップ レポートを待ちま す。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバ シップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバー ポートから IGMP クエリーが送信されません。Leave メッセージの受信後ただちに、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち時間が短縮されま す。即時脱退機能をイネーブルにするのは、接続されているレシーバー デバイスが 1 つだけのレシー バー ポートに限定してください。 MVR を使用すると、VLAN ごとに加入者用のテレビ チャネル マルチキャスト トラフィックを複製し なくてすみます。すべてのチャネル用のマルチキャスト トラフィックは、マルチキャスト VLAN 上で のみ、VLAN トランク全体で1回送信されます。IGMP Leave および Join メッセージは、加入者ポー トが割り当てられている VLAN に送られます。これらのメッセージは、レイヤ3デバイス上のマルチ キャスト VLAN のマルチキャスト トラフィック ストリームに対し、動的に登録します。アクセス レ イヤ スイッチ (スイッチ A) が転送動作を変更し、マルチキャスト VLAN から別個の VLAN 上の加 入者ポートへトラフィックを転送できるようにするので、選択されたトラフィックが2つの VLAN 間 を伝送されます。

IGMP レポートは、マルチキャスト データと同じ IP マルチキャスト グループ アドレスに送信されま す。スイッチ A の CPU は、レシーバー ポートから送られたすべての IGMP Join および Leave メッ セージを取り込み、MVR モードに基づいて、送信元(アップリンク)ポートのマルチキャスト VLAN に転送しなければなりません。

MVR の設定

ここでは、次の設定情報について説明します。

- 「MVR のデフォルト設定」(P.22-22)
- 「MVR 設定時の注意事項および制限事項」(P.22-23)
- 「MVR グローバル パラメータの設定」(P.22-23)
- 「MVR インターフェイスの設定」(P.22-25)

MVR のデフォルト設定

表 22-5 に、MVR のデフォルト設定を示します。

表 22-5 MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単
	位でディセーブル
マルチキャスト アドレス	未設定
クエリーの応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1
モード	compatible
インターフェイスのデフォルト	レシーバー ポートでも送信元ポートで
(ポート単位)	もない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

MVR を設定するときには、次の注意事項に従ってください。

- レシーバー ポートはアクセス ポートでなければなりません。トランク ポートにすることはできません。スイッチ上のレシーバー ポートは、異なる VLAN に所属していてもかまいませんが、マルチキャスト VLAN には所属させないでください。
- スイッチ上で設定できるマルチキャストエントリ(MVR グループアドレス)の最大数(受信できるテレビチャネルの最大数)は256です。
- 送信元 VLAN で受信され、レシーバー ポートから脱退する MVR マルチキャスト データは、ス イッチで Time to Live (TTL) が1 だけ少なくなります。
- スイッチ上の MVR は、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスを使用するので、スイッチ上でエイリアスの IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと相互運用している場合は、相互間でエイリアスとなる、または予約済みの IP マルチキャスト アドレス (224.0.0.xxx の範囲)を使用して IP アドレスを設定しないでください。
- MVR はスイッチ上で IGMP スヌーピングと共存できます。
- MVR レシーバー ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。

MVR グローバル パラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォ ルトのパラメータを変更する場合には(MVR VLAN 以外)、最初に MVR をイネーブルにする必要が あります。

(注)

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mvr	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	mvr group <i>ip-address</i> [count]	スイッチ上で IP マルチキャスト アドレスを設定するか、または count パ ラメータを使用して、連続する MVR グループ アドレスを設定します (count の範囲は 1 ~ 256、デフォルトは 1)。このアドレスに送信された マルチキャスト データは、スイッチ上のすべての送信元ポートおよびそ のマルチキャスト アドレスのデータを受信するために選ばれたすべての レシーバー ポートに送信されます。マルチキャスト アドレスとテレビ チャネルは 1 対 1 の対応です。
ステップ 4	mvr querytime value	(任意) マルチキャスト グループ メンバシップからポートを削除する前 に、レシーバー ポートで IGMP レポートのメンバシップを待機する最大 時間を設定します。この値は 10 分の 1 秒単位で設定します。範囲は 1 ~ 100、デフォルトは 10 分の 5 秒、すなわち 0.5 秒です。

	コマンド	目的
ステップ 5	mvr vlan vlan-id	(任意)マルチキャストデータを受信する VLAN を指定します。すべての送信元ポートをこの VLAN に所属させる必要があります。VLAN の範囲は 1 ~ 1001 および 1006 ~ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	mvr mode {dynamic	(任意)MVR の動作モードを指定します。
	compatible}	• dynamic:送信元ポートでダイナミック MVR メンバシップを使用できます。
		 compatible : Catalyst 3500 XL スイッチおよび Catalyst 2900 XL ス イッチとの互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。
		デフォルトは compatible モードです。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show mvr または show mvr members	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルトの設定に戻すには、**no mvr** [**mode** | **group** *ip-address* | **querytime** | **vlan**] グロー バル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにして、MVR グループ アドレスを設定し、クエリー タイムを1秒(10分の10秒)に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナ ミックに設定する例を示します。

Switch(config)# mvr Switch(config)# mvr group 228.1.23.4 Switch(config)# mvr querytime 10 Switch(config)# mvr vlan 22 Switch(config)# mvr mode dynamic Switch(config)# end

show mvr members 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

MVR インターフェイスの設定

レイヤ2MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mvr	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	interface interface-id	設定するレイヤ2ポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。
ステップ 4	mvr type {source receiver}	MVR ポートを次のいずれかに設定します。
		 source:マルチキャストデータを送受信するアップリンクポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。
		 receiver:加入者ポートであり、マルチキャストデータを受信するだけの場合、レシーバーポートとしてポートを設定します。静的に、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。レシーバーポートをマルチキャスト VLAN に所属させることはできません。
		デフォルトでは、非 MVR ポートとして設定されます。非 MVR ポート に MVR 特性を設定しようとしても、エラーになります。
ステップ 5	mvr vlan vlan-id group [ip-address]	(任意) マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。グループ メンバーとして静的に設定されたポートは、静的に削除されないかぎり、グループ メンバーのままです。
		(注) 互換モードでは、このコマンドが適用されるのはレシーバー ポートだけです。ダイナミック モードでは、レシーバー ポート および送信元ポートに適用されます。
		レシーバー ポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャスト グループに動的に加入することもできます。
ステップ 6	mvr immediate	(任意)ポート上で MVR の即時脱退機能をイネーブルにします。
		(注) このコマンドが適用されるのは、レシーバー ポートだけです。 また、イネーブルにするのは、単一のレシーバー デバイスが接続されているレシーバー ポートに限定してください。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show mvr	設定を確認します。
	show mvr interface または show mvr members	
ステップ 9	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの設定に戻すには、no mvr [type | immediate | vlan vlan-id | group] イ ンターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートをレシーバー ポートとして設定し、マルチキャスト グループ アドレスに送信されたマル チキャスト トラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、 結果を確認する例を示します。

```
Switch(config) # mvr
Switch(config) # interface gigabitethernet1/0/2
Switch(config-if)# mvr type receiver
Switch(config-if) # mvr vlan 22 group 228.1.23.4
Switch(config-if) # mvr immediate
Switch(config) # end
Switch# show mvr interface
Port
     Type
                 Status
                                 Immediate Leave
                  _____
____
       ____
                                  _____
Gi0/2 RECEIVER ACTIVE/DOWN
                                 ENABLED
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR の設定を表示するに は、特権 EXEC モードで表 22-6 のコマンドを使用します。

コマンド	目的	
show mvr	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまた はディセーブルの判別、マルチキャスト VLAN、マルチキャスト グループの最大数 (256) および現在の数 (0 ~ 256)、クエリーの応答時間、および MVR モードです。	
<pre>show mvr interface [interface-id] [members [vlan vlan-id]]</pre>	すべての MVR インターフェイスおよびそれぞれの MVR 設定を表示します。 特定のインターフェイスを指定すると、次の情報が表示されます。	
	• Status:次のいずれか1つ	
	- ACTIVE は、ポートが VLAN に含まれていることを意味します。	
	 UP/DOWN は、ボートが転送中または転送中ではないことを示します。 INACTIVE は、ポートが VLAN に含まれていないことを意味します。 	
	• Immediate Leave (即時脱退機能): イネーブルまたはディセーブル	
	members キーワードを入力すると、そのポート上のすべてのマルチキャスト グループ メンバーが表示されます。VLAN ID を入力した場合は、VLAN 上のすべてのマルチ キャスト グループ メンバーが表示されます。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。	
show mvr members [<i>ip-address</i>]	すべての IP マルチキャスト グループまたは指定した IP マルチキャスト グループ IP ア ドレスに含まれているレシーバー ポートおよび送信元ポートがすべて表示されます。	

表 22-6 MVR 情報を表示するためのコマンド

IGMP フィルタリングおよびスロットリングの設定

都市部や Multiple-Dwelling Unit (MDU) などの環境では、スイッチ ポート上のユーザが属する一連 のマルチキャスト グループを制御する必要があります。この機能を使用することにより、IP/TV など のマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。 また、マルチキャスト グループの数を、スイッチ ポート上でユーザが所属できる数に制限することも できます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各ス イッチ ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プ ロファイルにはマルチキャスト グループを1 つまたは複数格納して、グループへのアクセスを許可す るか拒否するかを指定できます。マルチキャスト グループへのアクセスを拒否する IGMP プロファイ ルがスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できな くなります。マルチキャスト グループへのアクセスがフィルタリング アクションで許可されている場 合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ2 インターフェ イスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバシップ レポート (Join および Leave レポートを含む) だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリ ングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。フィルタリング機能 は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されてい るかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合 だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ2インターフェイスが加入できる IGMP グループの 最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大 数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インター フェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートで ランダムに選択されたマルチキャスト エントリを上書きします。

(注)

IGMP フィルタリングが実行されているスイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

ここでは、次の設定情報について説明します。

- 「IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定」(P.22-28)
- 「IGMP プロファイルの設定」(P.22-28)(任意)
- 「IGMP プロファイルの適用」(P.22-29)(任意)
- 「IGMP グループの最大数の設定」(P.22-30)(任意)
- 「IGMP スロットリング アクションの設定」(P.22-31)(任意)

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

表 22-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 22-7 IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用されない
IGMP グループの最大数	最大数は設定されない
IGMP プロファイル	未設定
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

転送テーブルに登録されているグループが最大数に達していると、デフォルトの IGMP スロットリン グアクションは IGMP レポートを拒否します。設定時の注意事項については、「IGMP スロットリング アクションの設定」(P.22-31)を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、ip igmp profile グローバル コンフィギュレーション コマンドお よびプロファイル番号を使用して、IGMP プロファイルを作成し、IGMP プロファイル コンフィギュ レーション モードを開始します。ポートから送信される IGMP Join 要求をフィルタリングするために 使用される IGMP プロファイルのパラメータは、このモードから指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用して、プロファイルを作成できます。

- deny: 一致するアドレスを拒否します。デフォルトで設定されています。
- exit: IGMP プロファイル コンフィギュレーション モードを終了します。
- no: コマンドを否定するか、または設定をデフォルトに戻します。
- permit: 一致するアドレスを許可します。
- range: プロファイルの IP アドレス範囲を指定します。単一の IP アドレス、または開始アドレス と終了アドレスで指定された IP アドレス範囲を入力できます。

デフォルトでは、スイッチには IGMP プロファイルが設定されていません。プロファイルが設定され ており、permit および deny キーワードがいずれも指定されていない場合、デフォルトでは、IP アド レス範囲へのアクセスが拒否されます。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip igmp profile profile number	設定するプロファイルに番号を割り当て、IGMP プロファイル コン フィギュレーション モードを開始します。プロファイル番号の範囲 は 1 ~ 4294967295 です。
ステップ 3	permit deny	(任意) IP マルチキャスト アドレスへのアクセスを許可または拒否 するアクションを設定します。アクションを設定しないと、プロ ファイルのデフォルト設定はアクセス拒否になります。

	コマンド	目的
ステップ 4	range ip multicast address	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチ キャスト アドレス範囲を入力します。範囲を入力する場合は、IP マ ルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャス ト アドレスの上限値を入力します。
		range コマンドを複数回入力すると、複数のアドレスまたはアドレ ス範囲を入力できます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp profile profile number	プロファイルの設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、no range *ip multicast address*IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル4を作成して、 設定を確認する例を示します。アクションが拒否(デフォルト)である場合は、show ip igmp profile の出力には表示されません。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
permit
range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、ip igmp filter インターフェイス コン フィギュレーション コマンドを使用して、プロファイルを該当するインターフェイスに適用します。 IGMP プロファイルは、レイヤ 2 アクセス ポートにのみ適用できます。EtherChannel ポート グループ に所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のイン ターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	物理インターフェイスを指定し、インターフェイス コンフィギュ レーション モードを開始します。インターフェイスは、 EtherChannel ポート グループに所属していないレイヤ2ポートでな ければなりません。
ステップ 3	ip igmp filter profile number	指定された IGMP プロファイルをインターフェイスに適用します。 指定できる範囲は 1 ~ 4294967295 です。
ステップ 4	end	特権 EXEC モードに戻ります。

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

インターフェイスからプロファイルを削除するには、no ip igmp filter *profile number* インターフェイ ス コンフィギュレーション コマンドを使用します。

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

IGMP グループの最大数の設定

レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定するには、ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト 設定(208)に戻すには、このコマンドの no 形式を使用します。

このコマンドは、論理 EtherChannel インターフェイスでは使用できますが、EtherChannel ポート グ ループに属するポートでは使用できません。

転送テーブルの IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィ ギュレーション モードを開始します。インターフェイスは、 EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 3	ip igmp max-groups number	インターフェイスが加入できる IGMP グループの最大数を設定しま す。指定できる範囲は 0 ~ 4294967294 です。デフォルトでは最大 数は設定されません。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config interface <i>interface-id</i>	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

グループの最大数に関する制限を削除し、デフォルト設定(制限なし)に戻すには、no ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end

IGMP スロットリング アクションの設定

レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定したあと、ip igmp max-groups action replace インターフェイス コンフィギュレーション コマンドを使用して受信した IGMP レポートの新しいグループで、既存のグループを上書きします。IGMP Join レポートを廃棄する デフォルトの設定に戻すには、このコマンドの no 形式を使用します。

IGMP スロットリングを設定するときには、次の注意事項に従ってください。

- このコマンドは、論理 EtherChannel インターフェイスでは使用できますが、EtherChannel ポート グループに属するポートでは使用できません。
- グループの最大数に関する制限がデフォルト(制限なし)に設定されている場合、ip igmp max-groups action {deny | replace} コマンドを入力しても効果はありません。
- インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリングアクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリングアクションに応じて期限切れになるか削除されます。
 - スロットリングアクションを deny に設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、スイッチは、インターフェイスで受信した次の IGMP レポートを廃棄します。
 - スロットリング アクションを replace に設定すると、すでに転送テーブルに登録されていたエントリは削除されます。フォワーディング テーブルのエントリが最大数まで達したら、スイッチはランダムに選択したエントリを受信した IGMP レポートで上書きします。

スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送 テーブルにエントリが追加される前に、IGMP スロットリング アクションを設定します。

転送テーブルに最大数のエントリが登録されているときにスロットリング アクションを設定するには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	設定する物理インターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。インターフェイスは、 EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。	
ステップ 3 ip igmp max-groups action {deny replace}		インターフェイスが IGMP レポートを受信したときに、転送テーブ ルに最大数のエントリが登録されている場合は、次のいずれかのア クションをインターフェイスに指定します。	
		• deny :レポートを廃棄します。	
		• replace:既存のグループを、IGMP レポートを受信した新しい グループで上書きします。	
ステップ 4	end	特権 EXEC モードに戻ります。	
ステップ 5	show running-config interface interface-id	設定を確認します。	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

レポートの廃棄というデフォルトのアクションに戻すには、no ip igmp max-groups action インター フェイス コンフィギュレーション コマンドを使用します。

IGMP フィルタリングおよび IGMP スロットリング設定の表示

IGMP プロファイルの特性を表示したり、スイッチ上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。また、スイッチ上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 22-8 の特権 EXEC コマンドを使用して、IGMP フィルタリングおよび IGMP スロットリングの設定 を表示します。

表 22-8	IGMP フィルタリングおよび IGMP スロットリングの設定を表示するためのコマン	۴
--------	--	---

コマンド	目的
<pre>show ip igmp profile [profile number]</pre>	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファ イルを表示します。
<pre>show running-config [interface interface-id]</pre>	インターフェイスが所属できる IGMP グループの最大数(設定されている場合)や、イ ンターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまた はスイッチトのすべてのインターフェイスの設定を表示します。





ポート単位のトラフィック制御の設定

この章では、Catalyst 2960 スイッチにポートベースのトラフィック制御機能を設定する方法について 説明します。

(注)

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

この章で説明する内容は、次のとおりです。

- 「ストーム制御の設定」(P.23-1)
- 「保護ポートの設定」(P.23-7)
- 「ポートブロッキングの設定」(P.23-8)
- 「ポート セキュリティの設定」(P.23-9)
- 「ポート単位のトラフィック制御設定の表示」(P.23-20)

ストーム制御の設定

ここでは、次の概念と設定情報について説明します。

- 「ストーム制御の概要」(P.23-1)
- 「ストーム制御のデフォルト設定」(P.23-3)
- •「ストーム制御およびしきい値レベルの設定」(P.23-3)
- 「小さいフレームの着信レートの設定」(P.23-6)

ストーム制御の概要

ストーム制御は、物理インターフェイスの1つで発生したブロードキャスト、マルチキャスト、または ユニキャストストームによってLAN上のトラフィックが混乱することを防ぎます。LANストームは、 LANにパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えて ネットワークパフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の 間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御(またはトラフィック抑制)は、インターフェイスからスイッチングバスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅(ブロードキャスト、マルチキャスト、またはユニキャストトラフィックが使用できる ポートの総帯域幅の割合)
- ブロードキャスト、マルチキャスト、またはユニキャストパケットが受信されるトラフィックレートの秒単位のパケット数
- ブロードキャスト、マルチキャスト、またはユニキャストパケットが受信されるトラフィックレートの秒単位のビット数
- 小さいフレームのトラフィックレートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。 トラフィックレートが下限しきい値(指定されている場合)を下回らないかぎり、ポートはブロック されたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、ト ラフィックレートが上限抑制レベルを下回らないかぎり、スイッチはすべてのトラフィックをブロッ クします。一般に、そのレベルが高ければ高いほど、ブロードキャストストームに対する保護効果は 薄くなります。

<u>》</u> (注)

マルチキャスト トラフィックのストーム制御しきい値に達した場合、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)フレーム、Cisco Discovery Protocol (CDP) フレーム などの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。

図 23-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターン を示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも当てはまります。 この例では、T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラ フィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次の インターバルで、そのタイプのトラフィックがすべて廃棄されます。したがって、T2 と T5 のあとの インターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル (た とえば、T3) では、しきい値を上回らないかぎり、ブロードキャスト トラフィックが再び転送されま す。



ストーム制御抑制レベルと1秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を 制御します。しきい値が高いほど、通過するパケット数が多くなります。しきい値が100%であれば、 トラフィックに対する制限はありません。値を0.0にすると、そのポート上ではすべてのブロードキャ スト、マルチキャスト、またはユニキャストトラフィックがブロックされます。

(注)

パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する1秒間のイ ンターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、storm-control インターフェイス コンフィギュ レーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、ユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はスイッチ インターフェイス上でディセーブルになります。したがって、抑制レベルは 100% です。

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィックタイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題 があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズ によって、実際に適用されるしきい値は設定されたレベルに対して、数パーセントの差異が生じる可能 性があります。

(注)

ストーム制御は、物理インターフェイス上でサポートされます。また、EtherChannel 上でもストーム 制御を設定できます。ストーム制御が EtherChannel に設定されている場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的		
ステップ 3	storm-control {broadcast multicast unicast} level {level [level-low] bps bps [bps-low] pps	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制 御を設定します。デフォルトでは、ストーム制御はディセーブルに設定 されています。		
	pps [pps-low]}	キーワードの意味は次のとおりです。		
		 levelには、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します(小数点第2位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は、0.00~100.00です。 		
		 (任意) level-low には、下限しきい値レベルを帯域幅のパーセン テージで指定します(小数点第2位まで)。この値は上限抑制レベ ル以下の値である必要があります。トラフィックがこのレベルを下 回っていれば、ポートはトラフィックを転送します。下限抑制レベ ルを設定していない場合、上限抑制レベルと同じ値が設定されま す。指定できる範囲は、0.00~100.00です。 		
		しきい値に最大値(100%)を指定した場合、トラフィックの制限 はなくなります。しきい値に 0.0 を設定すると、そのポート上のす べてのブロードキャスト、マルチキャスト、またはユニキャスト ト ラフィックがブロックされます。		
		 bps bps には、ブロードキャスト、マルチキャスト、またはユニ キャストトラフィックの上限しきい値レベルをビット/秒で指定し ます(小数点第1位まで)。上限しきい値に到達すると、ポートは トラフィックをブロックします。指定できる範囲は0.0~ 1000000000.0です。 		
		 (任意) bps-lowには、下限しきい値レベルをビット/秒で指定します(小数点第1位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は0.0~1000000000.0です。 		
		 pps pps には、ブロードキャスト、マルチキャスト、またはユニ キャストトラフィックの上限しきい値レベルをパケット/秒で指定 します(小数点第1位まで)。上限しきい値に到達すると、ポート はトラフィックをブロックします。指定できる範囲は0.0~ 1000000000.0です。 		
		 (任意) pps-low には、下限しきい値レベルをパケット/秒で指定します(小数点第1位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は0.0~1000000000.0です。 		
		BPS および PPS の設定には、しきい値の数値を大きく設定できるよう に、サフィックスに測定記号(k、m、g など)を使用できます。		

	コマンド	目的
ステップ 4	storm-control action {shutdown trap}	ストームが検出された場合に実行するアクションを指定します。デフォ ルトではトラフィックにフィルタリングを実行し、トラップは送信しな い設定です。
		 ストーム中、ポートを errdisable の状態にするには、shutdown キーワードを選択します。
		 ストームが検出された場合、SNMP(簡易ネットワーク管理プロト コル)トラップを生成するには、trapキーワードを選択します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show storm-control [interface-id] [broadcast multicast unicast]	指定したトラフィック タイプについて、インターフェイスで設定した ストーム制御抑制レベルを確認します。トラフィック タイプを入力し なかった場合は、ブロードキャスト ストーム制御の設定が表示されま す。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、no storm-control {broadcast | multicast | unicast} level イ ンターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で、上限抑制レベルを 87%、下限抑制レベルを 65% に設定し、ユニキャスト ストーム 制御をイネーブルにする方法を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# storm-control unicast level 87 65

次に、ポート上で、ブロードキャスト アドレスのストーム制御を 20% のレベルでイネーブルにする例 を示します。ブロードキャスト トラフィックが、トラフィック ストーム制御インターバル内にポート で使用できる総帯域幅のうち、設定された 20% のレベルを超えた場合、トラフィック ストーム制御イ ンターバルが終わるまで、スイッチはすべてのブロードキャスト トラフィックを廃棄します。

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20

小さいフレームの着信レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、小さいフレームと見なされます。このパケットはス イッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定されたレート(しきい値)で到着した場合は、 ポートがディセーブルになるように設定できます。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパ ケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート(しきい値)で着信するパケットは、ポートがディセーブルにされた後は廃棄されます。

errdisable recovery cause small-frame global グローバル コンフィギュレーション コマンドが入力さ れると、指定された時間後にポートが再びイネーブルになります (errdisable recovery グローバル コ ンフィギュレーション コマンドを使用して、リカバリ時間を指定します)。

各インターフェイスのしきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause small-frame	スイッチ上の小さいフレームの着信レート機能をイネーブルに します。
ステップ 3	errdisable recovery interval interval	(任意) 指定された errdisable ステートから回復する時間を指 定します。
ステップ 4	errdisable recovery cause small-frame	(任意) 小さいフレームの着信によりポートが errdisable に なった後、そのポートを自動的に再イネーブルにするリカバリ 時間を設定します。
ステップ 5	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、 設定するインターフェイスを指定します。
ステップ 6	small violation-rate pps	インターフェイスが着信パケットを廃棄してポートを errdisable にするようにしきい値レートを設定します。範囲は、 $1 \sim 10,000$ Packets Per Second (pps; パケット/秒)です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show interfaces interface-id	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、小さいフレームの着信レート機能をイネーブルにし、ポートのリカバリ時間を設定し、ポートを errdisable にするしきい値を設定する例を示します。

Switch# configure terminal Switch# errdisable detect cause small-frame Switch# errdisable recovery cause small-frame Switch(config)# interface gigabitethernet0/1 Switch(config-if)# small-frame violation rate 10000 Switch(config-if)# end

保護ポートの設定

アプリケーションによっては、あるネイバが生成したトラフィックが別のネイバにわからないように、 同一スイッチ上のポート間でレイヤ2トラフィックが転送されないように設定する必要があります。こ のような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャス ト、またはマルチキャストトラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートである他のポートに、トラフィック(ユニキャスト、マルチキャスト、またはブロードキャスト)をすべて転送するわけではありません。レイヤ2では、保護ポート間でデータトラフックを転送できません。CPUで処理されてソフトウェアで転送される、Protocol Independent Multicast (PIM)パケットのような制御トラフィックのみが転送されます。保護ポート間を通過するトラフィックはすべて、レイヤ3デバイスを介して転送しなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。
- ここでは、次の設定情報について説明します。
- 「保護ポートのデフォルト設定」(P.23-7)
- 「保護ポート設定時の注意事項」(P.23-7)
- 「保護ポートの設定」(P.23-7)

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

保護ポート設定時の注意事項

保護ポートは、物理インターフェイス (GigabitEthernet ポート1 など) または EtherChannel グループ (port-channel 5 など) に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コ ンフィギュレーション モードを開始します。
ステップ 3	switchport protected	インターフェイスを保護ポートに設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces interface-id switchport	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し ます。

保護ポートをディセーブルにするには、no switchport protected インターフェイス コンフィギュレー ション コマンドを使用します。

次に、保護ポートとしてポートを設定する例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# switchport protected Switch(config-if)# end

ポート ブロッキングの設定

デフォルトでは、スイッチは未知の宛先 MAC (メディア アクセス制御) アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャストトラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャストトラフィックがあるポートから別のポートに転送されないようにするために、(保護または非保護) ポートをブロックし、未知のユニキャストまたはマルチキャストパケットが他のポートにフラッディングされないようにします。

(注)

マルチキャスト トラフィックを使用すると、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけ をブロックします。IPv4 情報または IPv6 情報をヘッダーに含んでいるマルチキャスト パケットはブ ロックされません。

ここでは、次の設定情報について説明します。

- 「ポートブロッキングのデフォルト設定」(P.23-8)
- 「インターフェイスでのフラッディングトラフィックのブロッキング」(P.23-8)

ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから未知のマルチキャストおよびユニキャスト トラフィックのフラッディン グがブロックされず、すべてのポートにこのようなパケットがフラッディングされます。

インターフェイスでのフラッディング トラフィックのブロッキング

(注)

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グ ループのすべてのポートでブロックされます。

ユニキャスト パケットおよびレイヤ2マルチキャスト パケットのインターフェイスからのフラッディ ングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	switchport block multicast	ポートからの未知のマルチキャストの転送をブロックしま す。
		(注) 純粋なレイヤ2マルチキャストトラフィックだけが ブロックされます。IPv4 情報または IPv6 情報をヘッ ダーに含んでいるマルチキャストパケットはブロッ クされません。
ステップ 4	switchport block unicast	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でトラフィックがブロックされずに、通常の転送が行われるデフォルトの状態にインターフェ イスを戻すには、no switchport block {multicast | unicast} インターフェイス コンフィギュレーショ ン コマンドを使用します。

次に、ポート上のユニキャストおよびレイヤ2マルチキャストフラッディングをブロックする例を示 します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポート セキュリティの設定

ポート セキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレ スを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパ ケットを転送しません。セキュア MAC アドレス数を1 つに制限し、単一のセキュア MAC アドレスを 割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにア クセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致 しないので、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレ スが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときに も、違反のフラグが立てられます。

ここでは、次の概念と設定情報について説明します。

- 「ポート セキュリティの概要」(P.23-10)
- 「ポート セキュリティのデフォルト設定」(P.23-12)
- 「ポート セキュリティの設定時の注意事項」(P.23-12)
- 「ポート セキュリティのイネーブル化および設定」(P.23-13)
- 「ポート セキュリティ エージングのイネーブル化および設定」(P.23-18)

ポート セキュリティの概要

ここでは、次の概要について説明します。

- 「セキュア MAC アドレス」 (P.23-10)
- 「セキュリティ違反」(P.23-11)

セキュア MAC アドレス

ポートで許可されるセキュア アドレスの最大数を設定するには、switchport port-security maximum value インターフェイス コンフィギュレーション コマンドを使用します。



最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しよ うとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス: switchport port-security mac-address mac-address イン ターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに 保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス:動的に設定されてアドレス テーブルにのみ保存され、ス イッチの再起動時に削除されます。
- スティッキーセキュア MAC アドレス:動的に学習することも、手動で設定することもできます。 アドレステーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコ ンフィギュレーションファイルに保存されていると、スイッチの再起動時にインターフェイスは これらを動的に再設定する必要がありません。

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュ ア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定で きます。スティッキー ラーニングをイネーブルにするには、switchport port-security mac-address sticky インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、 インターフェイスはスティッキー ラーニングがイネーブルになる前に学習したものを含め、すべての ダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべて のスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル (スイッチが再起動され るたびに使用されるスタートアップ コンフィギュレーション) に、自動的には反映されません。ス ティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再 起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキー セキュア アドレ スが保存されていない場合、アドレスは失われます。

スティッキー ラーニングをディセーブルにした場合、スティッキー セキュア MAC アドレスはダイナ ミック セキュア MAC アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレス の最大数によって決まります。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やイン ターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む)の総数を表します。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブル に未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュアインターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュ アインターフェイスで使用された場合。

違反が発生した場合のアクションに基づいて、次の4つの違反モードのいずれかにインターフェイスを 設定できます。

 protect(保護):セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最 大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない かぎり、未知の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が発生したこと は通知されません。



- E) トランク ポートに protect 違反モードを設定することは推奨しません。protect モードの場合、ポートが最大限度に達していなくてもいずれかの VLAN が最大限度に達すると、ラーニングをディセーブルにします。
- restict(制限):セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最 大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない かぎり、未知の送信元アドレスを持つパケットは廃棄されます。このモードでは、セキュリティ違 反が発生したことが通知されます。SNMP トラップが送信されて Syslog メッセージがログされ、 違反カウンタが増加します。
- shutdown (シャットダウン):ポート セキュリティ違反により、インターフェイスが errdisable になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、errdisable recovery cause *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。これがデフォルトのモードです。
- shutdown vlan (VLAN シャットダウン): VLAN 単位でセキュリティ違反モードを設定するため に使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になり ます。

表 23-1 に、ポート セキュリティをインターフェイスに設定した場合の違反モードおよび対処について 示します。

違反モード	トラフィック の転送 ¹	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージ の表示 ²	違反カウンタの 増加	ポートの シャットダウン
protect	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり
shutdown vlan	なし	あり	あり	なし	あり	なし3

表 23-1 セキュリティ違反モードの処置

1. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットが廃棄されます。

2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。

3. 違反が発生した VLAN のみシャットダウンします。

ポート セキュリティのデフォルト設定

表 23-2 に、インターフェイスに対するポート セキュリティのデフォルト設定を示します。

表 23-2 ポート セキュリティのデフォルト設定

機能	デフォルト設定
ポート セキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニン グ	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1
違反モード	shutdown(シャットダウン)。セキュア MAC アドレスが最大数を 上回ると、ポートがシャットダウンします。
ポート セキュリティ エージング	ディセーブル エージング タイムは 0。 スタティック エージングはディセーブル
	タイプは absolute

ポート セキュリティの設定時の注意事項

ポートセキュリティを設定するときには、次の注意事項に従ってください。

- ポートセキュリティを設定できるのは、スタティックアクセスポートまたはトランクポートに限られます。セキュアポートをダイナミックアクセスポートにすることはできません。
- セキュア ポートを Switched Port Analyzer (SPAN; スイッチド ポート アナライザ)の宛先ポート にすることはできません。
- セキュア ポートは、Fast EtherChannel やギガビット EtherChannel ポート グループに属すことができません。



音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN も設定されているインターフェイスでポート セキュリティをイネーブルにする際には、ポート上で許可されるセキュア アドレスの最大数を 2 に設定します。ポートを Cisco IP Phone に接続している場合、IP Phone には MAC アドレスが 1 つ必要になります。Cisco IP Phone アドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 つの PC を Cisco IP Phone に接続する場合、追加の MAC アドレスは不要です。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュア アドレスを設定する必要があります。
- トランク ポートをポート セキュリティで設定し、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス VLAN に割り当てられている場合は、switchport voice および switchport priority extend インターフェイス コンフィギュレーション コマンドを入力しても効果 はありません。

接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アド レスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。

- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が以前の値より小さく、インターフェイス上ですでに設定されているセキュアアドレスの数が新しい値を上回る場合は、コマンドが拒否されます。
- スイッチは、スティッキー セキュア MAC アドレスのポート セキュリティ エージングをサポート していません。

表 23-3 に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

表 23-3 他のスイッチ機能とポート セキュリティとの互換性

$DTP^{-1} \vec{x} = b^2$	
トランク ポート あり	
ダイナミック アクセス ポート3 なし	
Switched Port Analyzer (SPAN; スイッチド ポート アナラ あり イザ)送信元ポート	
SPAN 宛先ポート なし	
EtherChannel なし	
保護ポート あり	
IEEE 802.1x ポート あり	
音声 VLAN ポート ⁴ あり	
Flex Link あり	

1. DTP = Dynamic Trunking Protocol

- 2. switchport mode dynamic インターフェイス コンフィギュレーション コマンドで設定されたポート。
- 3. switchport access vlan dynamic インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol (VQP) ポート。
- 4. ポートに最大限可能なセキュアなアドレスを設定します(アクセス VLAN で可能なセキュアなアドレスの最大数 に 2 を加えた数)。

ポート セキュリティのイネーブル化および設定

ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ステップ 3	<pre>switchport mode {access trunk}</pre>	インターフェイス スイッチポート モードを access または trunk に設定し ます。デフォルト モード (dynamic auto) のインターフェイスは、セ キュア ポートとして設定できません。
ステップ 4	switchport voice vlan vlan-id	ポート上で音声 VLAN をイネーブルにします。
		<i>vlan-id</i> :音声トラフィックに使用する VLAN を指定します。
ステップ 5	switchport port-security	インターフェイス上でポート セキュリティをイネーブルにします。

	コマンド	目的
ステップ 6	switchport port-security [maximum value [vlan {vlan-list {access voice}}]]	(任意) インターフェイスに対するセキュア MAC アドレスの最大数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やイン ターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む)の総数を表します。
		(任意) vlan: VLAN 単位の最大値を設定します。
		vlan キーワードを入力したあと、次のオプションのいずれか 1 つを入力 してください。
		 vlan-list:トランクポート上で、ハイフンで区切った範囲の VLAN、 またはカンマで区切った一連の VLAN における、VLAN 単位の最大 値を設定できます。指定されなかった VLAN には、VLAN 単位の最 大値が使用されます。
		 access: アクセス ポート上で、アクセス VLAN として VLAN を指定します。
		 voice: アクセス ポート上で、音声 VLAN として VLAN を指定します。
		(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュアMAC アドレスの最大数を2に設定します。

	 コマンド	目的
ステップ 7	switchport port-security (任 [violation {protect restrict shutdown shutdown vlan}] (注 (注 (注 (注 (注 (注 (注	(任意)違反モード、すなわちセキュリティ違反が検出されたときの対応 を、次のいずれかに設定します。
		 protect(保護): ポート セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が発生したことは通知されません。
		 トランクポートに protect モードを設定することは推奨しません。 protect モードの場合、ポートが最大限度に達していなくてもい ずれかの VLAN が最大限度に達すると、ラーニングをディセー ブルにします。
		 restrict:セキュア MAC アドレスの数がポートで許可されている最 大限度に達すると、十分な数のセキュア MAC アドレスを削除する か、または許可アドレス数を増やさないかぎり、未知の送信元アド レスを持つパケットは廃棄されます。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加 します。
		 shutdown:違反が発生すると、インターフェイスが errdisable になり、ポートの LED が消灯します。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。
		 shutdown vlan: VLAN 単位でセキュリティ違反モードを設定する ために使用します。このモードで違反が発生すると、ポート全体で はなく、VLAN が errdisable になります。
		 (注) セキュア ポートが errdisable ステートになった場合は、 errdisable recovery cause psecure-violation グローバル コン フィギュレーション コマンドを入力して、このステートを解除し ます。手動で再びイネーブルにするには、shutdown および no shutdown インターフェイス コンフィギュレーション コマン ドを入力するか、clear errdisable interface vlan 特権 EXEC コ マンドを入力します。

	コマンド	目的
ステップ 8	<pre>switchport port-security [mac-address mac-address [vlan {vlan-id {access voice}}]</pre>	(任意) インターフェイスのセキュア MAC アドレスを入力します。この コマンドを使用すると、最大数のセキュア MAC アドレスを入力できま す。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。
		(注) このコマンドの入力後にスティッキー ラーニングをイネーブルに すると、動的に学習されたセキュア アドレスがスティッキー セ キュア MAC アドレスに変換されて実行コンフィギュレーション に追加されます。
		(任意) vlan: VLAN 単位の最大値を設定します。
		vlan キーワードを入力したあと、次のオプションのいずれか 1 つを入力 してください。
		 <i>vlan-id</i>: トランク ポートで、VLAN ID および MAC アドレスを指 定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使 用されます。
		 access: アクセス ポート上で、アクセス VLAN として VLAN を指 定します。
		 voice: アクセス ポート上で、音声 VLAN として VLAN を指定します。
		(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュアMAC アドレスの最大数を 2 に設定します。
ステップ 9	switchport port-security mac-address sticky	(任意) インターフェイスでスティッキー ラーニングをイネーブルにしま す。
ステップ 10	switchport port-security mac-address sticky [mac-address vlan {vlan-id {access voice}}]	(任意) スティッキー セキュア MAC アドレスを入力し、必要な回数だけ コマンドを繰り返します。設定したセキュア MAC アドレスの数が最大 数より少ない場合、残りの MAC アドレスは動的に学習されてスティッ キー セキュア MAC アドレスに変換され、実行コンフィギュレーション に追加されます。
		(注) このコマンドの入力前にスティッキー ラーニングをイネーブルに しないと、エラー メッセージが表示されてスティッキー セキュ ア MAC アドレスアドレスを入力できません。
		(任意) vlan : VLAN 単位の最大値を設定します。
		vlan キーワードを入力したあと、次のオプションのいずれか l つを入力 してください。
		 <i>vlan-id</i>: トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。
		 access: アクセス ポート上で、アクセス VLAN として VLAN を指 定します。
		 voice: アクセス ポート上で、音声 VLAN として VLAN を指定します。
		(注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

	コマンド	目的
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show port-security	設定を確認します。
ステップ 13	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

セキュア ポートではないデフォルトの状態にインターフェイスを戻す場合は、no switchport port-security インターフェイス コンフィギュレーション コマンドを使用します。スティッキー ラーニ ングがイネーブルの状態でこのコマンドを入力すると、スティッキー セキュア アドレスが実行コン フィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。ここですべてのア ドレスが動的に学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻す場合は、no switchport port-security maximum value インターフェイス コンフィギュレーション コマンドを使用します。違 反モードをデフォルト状態 (shutdown モード) に戻す場合は、no switchport port-security violation {protocol | restrict} インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでスティッキー ラーニングをディセーブルにするには、no switchport port-security mac-address sticky インターフェイス コンフィギュレーション コマンドを使用します。インターフェ イスがスティッキー セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただ し、スティッキー MAC アドレスによる設定を保存した場合、no switchport port-security mac-address sticky コマンドの入力後に設定をもう一度保存しないと、スイッチの再起動時にス ティッキー アドレスが復元されます。

MAC アドレス テーブルからスイッチまたはインターフェイス上のセキュア アドレスすべてまたは特定(設定、ダイナミック、スティッキー)のセキュア アドレスすべてを削除するには、clear port-security {all | configured | dynamic | sticky} 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、no switchport port-security mac-address mac-address インターフェイス コンフィギュレーション コマンドを使用します。イン ターフェイス上のすべてのダイナミック セキュア アドレスをアドレス テーブルから削除するには、no switchport port-security インターフェイス コンフィギュレーション コマンドのあとに、(インター フェイスでポート セキュリティを再びイネーブルにするために) switchport port-security コマンドを 入力します。no switchport port-security コマンドを使用する前に、no switchport port-security mac-address sticky インターフェイス コンフィギュレーション コマンドを使用してスティッキー セ キュア MAC アドレスをダイナミック セキュア MAC アドレスに変換した場合、手動で設定されたもの を除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

設定済みのセキュア MAC アドレスをアドレス テーブルから明確に削除する場合、no switchport port-security mac-address mac-address インターフェイス コンフィギュレーション コマンドを使用し なければなりません。

次に、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する 例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、ス ティッキー ラーニングはイネーブルです。

```
Switch(config) # interface gigabitethernet0/1
Switch(config-if) # switchport mode access
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security maximum 50
Switch(config-if) # switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポートのスティッキー ポート セキュリティをイネーブルにする例を示します。データ VLAN お よび音声 VLAN の MAC アドレスを手動で設定し、セキュア アドレスの総数を 20 に設定します (データ VLAN に 10、音声 VLAN に 10 を割り当てます)。

```
Switch(config) # interface gigabitethernet0/1
Switch(config-if) # switchport access vlan 21
Switch(config-if) # switchport mode access
Switch(config-if) # switchport voice vlan 22
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security maximum 20
Switch(config-if) # switchport port-security violation restrict
Switch(config-if) # switchport port-security mac-address sticky
Switch(config-if) # switchport port-security mac-address sticky
Switch(config-if) # switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if) # switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if) # switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if) # switchport port-security mac-address 0000.0000.0001 vlan voice
Switch(config-if) # switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if) # switchport port-security maximum 10 vlan access
Switch(config-if) # switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングのイネーブル化および設定

ポート上のすべてのセキュア アドレスにエージング タイムを設定するには、ポート セキュリティ エー ジングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- absolute:指定されたエージングタイムの経過後に、ポート上のセキュアアドレスが削除されます。
- inactivity:指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に 限り、ポート上のセキュアアドレスが削除されます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポート上 のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュア アドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

ポート セキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま ナ
ステップ 2	interface interface-id	9。 設定するインターフェイスを指定し、インターフェイス
		コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	<pre>switchport port-security aging {static time time type {absolute inactivity}}</pre>	セキュア ポートのスタティック エージングをイネーブル またはディセーブルにします。またはエージング タイム やタイプを設定します。
		(注) スイッチは、スティッキー セキュア アドレスの ポート セキュリティ エージングをサポートして いません。
		このポートに、スタティックに設定されたセキュア アド レスのエージングをイネーブルにする場合は、static を入 力します。
		<i>time</i> には、このポートのエージング タイムを指定します。 指定できる範囲は、 $0 \sim 1440$ 分です。
		type には、次のキーワードのいずれか1つを選択します。
		 absolute:エージングタイプを絶対エージングとして設定します。このポートのセキュアアドレスはすべて、指定した時間(分単位)が経過すると期限切れになり、セキュアアドレスリストから削除されます。
		 inactivity: エージング タイプを非アクティブ エージ ングとして設定します。指定された time 期間中にセ キュア送信元アドレスからのデータ トラフィックが ない場合に限り、このポートのセキュア アドレスが 期限切れになります。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	<pre>show port-security [interface interface-id] [address]</pre>	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存 します。

ポート上のすべてのセキュア アドレスに対してポート セキュリティ エージングをディセーブルにする には、no switchport port-security aging time インターフェイス コンフィギュレーション コマンドを 使用します。静的に設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、 no switchport port-security aging static インターフェイス コンフィギュレーション コマンドを使用し ます。

次に、ポート上のセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120

次に、このインターフェイスに設定されたセキュア アドレスに対して、エージングをイネーブルにし、 非アクティブ エージング タイプのエージング タイムを 2 分に設定する例を示します。

Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static

上記のコマンドを確認するには、**show port-security interface** *interface-id* 特権 EXEC コマンドを入 力します。

Switch(config)# interface gigabitethernet0/1

ポート単位のトラフィック制御設定の表示

show interfaces *interface-id* **switchport** 特権 EXEC コマンドを使用すると、(他の特性の中から) イン ターフェイス トラフィックの抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、ストーム制御およびポート セキュリティの設 定が表示されます。

トラフィックの制御情報を表示するには、表 23-4 の特権 EXEC コマンドを1つまたは複数使用します。

表 23-4 トラフィック制御ステータスおよび設定を表示するためのコマンド

コマンド	目的
show interfaces [interface-id] switchport	すべてのスイッチング(非ルーティング)ポートまたは指定された ポートの管理ステータスまたは動作ステータスを、ポートブロッキ ングおよびポート保護の設定を含めて表示します。
show storm-control [interface-id] [broadcast multicast unicast]	すべてのインターフェイスまたは指定されたインターフェイスに設 定されているストーム制御抑制レベルを、指定されたトラフィック タイプについて、またはブロードキャストトラフィック(トラ フィックタイプが入力されていない場合)について表示します。
show port-security [interface <i>interface-id</i>]	スイッチまたは指定されたインターフェイスのポート セキュリティ 設定を、各インターフェイスで許容されるセキュア MAC アドレスの 最大数、インターフェイスのセキュア MAC アドレスの数、発生した セキュリティ違反の数、違反モードを含めて表示します。
show port-security [interface interface-id] address	すべてのスイッチ インターフェイスまたは指定されたインターフェ イスに設定されたすべてのセキュア MAC アドレス、および各アドレ スのエージング情報を表示します。
show port-security interface interface-id vlan	指定されたインターフェイスに VLAN 単位で設定されているセキュ ア MAC アドレスの数を表示します。



снартег 24

UDLD の設定

この章では、Catalyst 2960 スイッチに Unidirectional Link Detection (UDLD; 単一方向リンク検出) プロトコルを設定する方法について説明します。

(注)

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

この章で説明する内容は、次のとおりです。

- 「UDLD の概要」(P.24-1)
- 「UDLD の設定」(P.24-4)
- 「UDLD ステータスの表示」(P.24-7)

UDLDの概要

UDLD は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスから ケーブルの物理設定をモニタしたり、単一方向リンクの存在を検出したりできるようにするためのレイ ヤ2プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接 続されたすべてのデバイスで UDLD プロトコルがサポートされていなければなりません。UDLD は単 一方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単一方向リ ンクは、スパニング ツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性がありま す。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常(デフォルト)とアグレッシブです。通常 モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できま す。アグレシップ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラ フィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ1のメカニズムを使用して、リンクの物理ス テータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーション によって処理されます。UDLD は、ネイバ ID の検出、誤って接続されたポートのシャットダウンな ど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両 方をイネーブルにすると、レイヤ1と2の検出機能が連動し、物理的および論理的な単一方向接続、お よび他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバが受信するにもかかわらず、ネイバから送信され たトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

通常モードの UDLD は、光ファイバ ポートの光ファイバが誤って接続されている場合に単一方向リン クを検出しますが、レイヤ1メカニズムは、この誤った接続を検出しません。ポートが正しく接続され ていてもトラフィックが片方向である場合、単一方向リンクを検出するはずのレイヤ1メカニズムがこ の状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不 確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションが アクティブであると、レイヤ1メカニズムがリンクの物理的な問題を検出するため、リンクは稼動状態 でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされま す。

アグレッシブ モードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシ ブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一 方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出 できます。

- 光ファイバリンクまたはツイストペアリンクで、ポートの1つがトラフィックを送受信できない。
- 光ファイバリンクまたはツイストペアリンクで、ポートの1つがダウンし、残りのインターフェ イスが稼動している。
- ケーブルのうち1本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイント リンクでは、UDLD Hello パケットをハートビートと見なすことができ、ハー トビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立 できないかぎり、リンクをシャットダウンする必要があることを意味しています。

レイヤ1の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブモードの UDLD はそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバ 間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ1で動作するため、こ のチェックは自動ネゴシエーションでは実行できません。
単一方向の検出方法

UDLD は2つのメカニズムを使用して動作します。

ネイバデータベースメンテナンス

UDLD は、アクティブな各ポート上で Hello パケット(別名アドバタイズまたはプローブ)を定 期的に送信して、他の UDLD 対応ネイバに関して学習し、各デバイスがネイバに関する情報を常 に維持できるようにします。

スイッチが Hello メッセージを受信すると、エージング タイム (ホールド タイムまたは Time To Live [TTL]) が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れ る前に、スイッチが新しい Hello メッセージを受信すると、古いエントリが新しいエントリで置き 換えられます。

UDLDの稼動中にポートがディセーブルになったり、ポート上で UDLD がディセーブルになった り、またはスイッチをリセットした場合、UDLD は設定変更の影響を受けるポートの既存の キャッシュ エントリをすべて消去します。UDLD は、ステータス変更の影響を受けるキャッシュ の一部をフラッシュするようにネイバに通知するメッセージを1つまたは複数送信します。この メッセージは、キャッシュを継続的に同期するためのものです。

イベントドリブン検出およびエコー

UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバを学習する か、または同期していないネイバから再同期要求を受信すると、接続の UDLD デバイス側の検出 ウィンドウを再起動して、エコーメッセージを返送します。この動作はすべての UDLD ネイバに 対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンク は不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードに ある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバのキャッシュ エン トリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバ との再同期を行います。

アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバがアドバタイズまたは検出段 階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバと の再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、 UDLD はポートをシャットダウンします。


図 24-1 に、単一方向リンク状態の例を示します。

UDLD の設定

ここでは、次の設定情報について説明します。

- 「UDLD のデフォルト設定」(P.24-4)
- 「設定時の注意事項」(P.24-5)
- 「UDLD のグローバルなイネーブル化」(P.24-5)
- 「インターフェイス上での UDLD のイネーブル化」(P.24-6)
- 「UDLD によってディセーブル化されたインターフェイスのリセット」(P.24-7)

UDLD のデフォルト設定

表 24-1 に、UDLD のデフォルト設定を示します。

表 24-1 UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート(光ファイバ メディ ア用)	すべてのイーサネット光ファイバ ポート上でディセーブル
ポート別の UDLD イネーブル ステート(ツイストペア [銅 線]メディア用)	すべてのイーサネット 10/100 および 1000BASE-TX ポート 上でディセーブル
UDLD アグレッシブ モード	ディセーブル

設定時の注意事項

UDLD 設定時の注意事項を次に示します。

- UDLD は Asynchronous Transfer Mode (ATM; 非同期転送モード) ポート上ではサポートされて いません。
- UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートも 単一方向リンクを検出できません。
- モード(通常またはアグレッシブ)を設定する場合、リンクの両側に同じモードを設定します。



ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、 STP を実行するデバイスを直接接続することを推奨します。

UDLD のグローバルなイネーブル化

アグレッシブ モードまたは標準モードで UDLD をイネーブルにし、スイッチのすべての光ファイバ ポートに設定可能なメッセージ タイマーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	udld {aggressive enable message	UDLD の動作モードを指定します。
	time <i>message-timer-interval</i> }	 aggressive: すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。
		 enable:スイッチ上のすべての光ファイバポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトで ディセーブルです。
		個々のインターフェイスの設定は、udld enable グローバル コ ンフィギュレーション コマンドの設定を上書きします。
		アグレッシブおよび通常モードの詳細については、「動作モー ド」 (P.24-2) を参照してください。
		 message time message-timer-interval: アドバタイズ フェーズ に存在し、双方向と検出されたポートにおける UDLD プロー ブメッセージ間の間隔を設定します。指定できる範囲は 7 ~ 90 秒です。
		 (注) このコマンドが作用するのは、光ファイバ ポートだけです。 他のポート タイプで UDLD をイネーブルにする場合は、 udld インターフェイス コンフィギュレーション コマンドを 使用します。詳細については、「インターフェイス上での UDLD のイネーブル化」(P.24-6) を参照してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show udld	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD をグローバルにディセーブルにするには、no udld enable グローバル コンフィギュレーション コマンドを使用して、すべての光ファイバ ポート上で標準モードの UDLD をディセーブルにします。 すべての光ファイバ ポート上でアグレッシブ モードの UDLD をディセーブルにする場合は、no udld aggressive グローバル コンフィギュレーション コマンドを使用します。

インターフェイス上での UDLD のイネーブル化

ポート上で、UDLD をアグレッシブ モードまたは通常モードでイネーブルにするか、または UDLD を ディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	UDLD のためにイネーブルにするポートを指定し、インターフェ イス コンフィギュレーション モードを開始します。
ステップ 3	udld port [aggressive]	UDLD はデフォルトでディセーブルです。
		 udld port:指定されたポート上で、UDLD を通常モードでイ ネーブルにします。
		 udld port aggressive:指定されたポート上で、UDLD をアグレッシブ モードでイネーブルにします。
		(注) 特定の光ファイバ ポート上で UDLD をディセーブルにす る場合は、no udld port インターフェイス コンフィギュ レーション コマンドを使用します。
		アグレッシブおよび通常モードの詳細については、「動作モー ド」(P.24-2)を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show udld interface-id	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

UDLD によってディセーブル化されたインターフェイスのリセット

UDLD によってディセーブルにされたすべてのポートをリセットするには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1	udld reset	UDLD によってディセーブルにされたすべてのポート
		をリセットします。
ステップ 2	show udld	設定を確認します。

次のコマンドを使用して、ポートを起動することもできます。

- shutdown インターフェイス コンフィギュレーション コマンドに続けて no shutdown インター フェイス コンフィギュレーション コマンドを入力すると、ディセーブルのポートを再起動できま す。
- no udld { aggressive | enable} グローバル コンフィギュレーション コマンドのあとに udld {aggressive | enable} グローバル コンフィギュレーション コマンドを実行すると、ディセーブル 化されたポートが再びイネーブルになります。
- no udld port インターフェイス コンフィギュレーション コマンドの後に udld port [aggressive] イ ンターフェイス コンフィギュレーション コマンドを実行すると、ディセーブル化された光ファイ バポートが再びイネーブルになります。
- errdisable recovery cause udld グローバル コンフィギュレーション コマンドを入力すると、 UDLD の errdisable ステートから自動回復するタイマーをイネーブルにできます。さらに、 errdisable recovery interval *interval* グローバル コンフィギュレーション コマンドを入力すると、 UDLD の errdisable ステートから回復する時間を指定できます。

UDLD ステータスの表示

指定されたポートまたはすべてのポートの UDLD ステータスを表示するには、show udld [*interface-id*] 特権 EXEC コマンドを使用します。

コマンド出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

■ UDLD ステータスの表示



CHAPTER **25**

CDP の設定

この章では、Catalyst 2960 スイッチに Cisco Discovery Protocol (CDP) を設定する方法について説明 します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の 「System Management Commands」を参照してください。

この章で説明する内容は、次のとおりです。

- 「CDP の概要」(P.25-1)
- 「CDP の設定」(P.25-2)
- 「CDP のモニタおよびメンテナンス」(P.25-5)

CDPの概要

CDP はすべてのシスコ製デバイス (ルータ、ブリッジ、アクセス サーバ、およびスイッチ)のレイヤ 2 (データ リンク レイヤ)で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーショ ンは CDP を使用することにより、既知のデバイスに近接しているシスコ製デバイスを検出できます。 また、下位レイヤのトランスペアレント プロトコルが稼動している近接デバイスのデバイス タイプや、 SNMP(簡易ネットワーク管理プロトコル)エージェント アドレスを学習することもできます。この 機能によって、アプリケーションから近接デバイスに SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol (SNAP) をサポートしているすべてのメディアで動作します。 CDP はデータ リンク レイヤでのみ動作するため、異なるネットワーク レイヤ プロトコルをサポート する 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャスト アドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを1つまたは複数アドバタイズします。このアドバタイズには、受信 側デバイスで CDP 情報を廃棄せずに保持する時間を表す Time To Live (TTL)、つまりホールドタイ ム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、近接デバイ スについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバー、およびコマンド スイッチから最大3台(デフォルト)離れたクラスタ対応の他のデバイスについての情報を維持しま す。

スイッチは CDP バージョン 2 をサポートします。

CDP の設定

ここでは、次の設定情報について説明します。

- 「CDP のデフォルト設定」(P.25-2)
- 「CDP の特性の設定」(P.25-2)
- 「CDP のディセーブル化およびイネーブル化」(P.25-3)
- 「インターフェイス上での CDP のディセーブル化およびイネーブル化」(P.25-4)

CDP のデフォルト設定

表 25-1 に、CDP のデフォルト設定を示します。

表	25-1	CDP	のデ	フォ	ル	ト設定
---	------	-----	----	----	---	-----

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー(パケット更新頻度)	60 秒
CDP ホールドタイム(廃棄までの時間)	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の特性の設定

CDP 更新の頻度、廃棄するまで情報を保持する期間、およびバージョン2アドバタイズを送信するか どうかを設定できます。

CDP タイマー、ホールドタイム、およびアドバタイズ タイプを設定するには、特権 EXEC モードで次の手順を実行します。



ステップ2~4はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp timer seconds	(任意) CDP 更新の送信頻度(秒)を設定します。
		指定できる範囲は 5 ~ 254 です。デフォルトは 60 秒です。
ステップ 3	cdp holdtime seconds	(任意) デバイスから送信された情報を受信側デバイスが廃棄するま で保持する期間を指定します。
		指定できる範囲は 10 ~ 255 秒です。デフォルトは 180 秒です。
ステップ 4	cdp advertise-v2	(任意) バージョン 2 アドバタイズを送信するように CDP を設定しま す。
		これがデフォルトのステートです。
ステップ 5	end	特権 EXEC モードに戻ります。

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

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

デフォルト設定に戻すには、CDP コマンドの no 形式を使用します。

次に、CDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

その他の CDP show コマンドについては、「CDP のモニタおよびメンテナンス」(P.25-5)を参照して ください。

CDP のディセーブル化およびイネーブル化

CDP はデフォルトでイネーブルです。



スイッチ クラスタと他のシスコ製デバイス (Cisco IP Phone など) は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。 詳細は、第5章「スイッチのクラスタ化」および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。

CDP デバイス検出機能をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run	CDP をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。

次に、ディセーブル化されている CDP をイネーブルにする例を示します。

Switch# configure terminal Switch(config)# cdp run Switch(config)# end

インターフェイス上での CDP のディセーブル化およびイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では **CDP** がデフォル トでイネーブルになっています。

ポート上で CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	CDP をディセーブルにするインターフェイスを指定し、イン ターフェイス コンフィギュレーション モードを開始します。	
ステップ 3	no cdp enable	インターフェイス上で CDP をディセーブルにします。	
ステップ 4	end	特権 EXEC モードに戻ります。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

特定のポート上で、ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	CDP をイネーブルにするインターフェイスを指定し、インター フェイス コンフィギュレーション モードを開始します。
ステップ 3	cdp enable	インターフェイス上で、ディセーブル化されている CDP をイ ネーブルにします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

次に、特定のポート上で、ディセーブル化されている CDP をイネーブルにする例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# cdp enable Switch(config-if)# end

第 25 章 CDP の設定

CDP のモニタおよびメンテナンス

デバイス上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは 複数実行します。

コマンド	説明	
clear cdp counters	トラフィック カウンタをゼロにリセットします。	
clear cdp table	ネイバに関する情報を格納する CDP テーブルを削除します。	
show cdp	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を 表示します。	
show cdp entry entry-name	特定のネイバに関する情報を表示します。	
[protocol version]	アスタリスク(*)を入力してすべての CDP ネイバを表示することも、情報が 必要なネイバの名前を入力することもできます。	
	また、指定されたネイバ上でイネーブルになっているプロトコルの情報や、デ バイス上で稼動しているソフトウェアのバージョン情報が表示されるように、 表示内容を制限することもできます。	
<pre>show cdp interface [interface-id]</pre>	CDP がイネーブルに設定されているインターフェイスに関する情報を表示します。	
	必要なインターフェイスの情報だけを表示できます。	
<pre>show cdp neighbors [interface-id] [detail]</pre>	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、 機能、プラットフォーム、ポート ID など、ネイバに関する情報を表示します。	
	特定のインターフェイスに関するネイバ情報だけを表示したり、詳細表示にす るため表示内容を拡張したりできます。	
show cdp traffic	CDP カウンタ(送受信されたパケット数、チェックサム エラーを含む)を表示 します。	

■ CDP のモニタおよびメンテナンス





LLDP、LLDP-MED、およびワイヤード ロ ケーション サービスの設定

(注)

LLDP-MED およびロケーション サービスを使用するには、スイッチが LAN Base イメージを実行して いる必要があります。

この章では、Catalyst 2960 スイッチで Link Layer Discovery Protocol (LLDP)、LLDP Media Endpoint Discovery (LLDP-MED)、およびワイヤード ロケーション サービスを設定する方法につい て説明します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の 「System Management Commands」を参照してください。

- 「LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要」(P.26-2)
- 「LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定」(P.26-5)
- 「LLDP、LLDP-MED、およびワイヤード ロケーション サービスのモニタリングおよびメンテナ ンス」(P.26-13)

LLDP、LLDP-MED、およびワイヤード ロケーション サー ビスの概要

LLDP

Cisco Discovery Protocol (CDP; シスコ検出プロトコル)は、すべてのシスコ製デバイス(ルータ、ブリッジ、アクセスサーバ、およびスイッチ)のレイヤ2(データリンクレイヤ)上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションはCDPを使用することにより、ネットワーク接続されている他のシスコ製デバイスを自動的に検出し、識別できます。

スイッチでは他社製のデバイスをサポートし他のデバイス間の相互運用性を確保するために、IEEE 802.1AB Link Layer Discovery Protocol(LLDP)をサポートしています。LLDP は、ネットワーク デ バイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用する近隣ディスカ バリ プロトコルです。このプロトコルはデータ リンク レイヤで動作するため、異なるネットワーク レ イヤ プロトコルが稼動する 2 つのシステムで互いの情報を学習できます。

LLDP は一連のアトリビュートをサポートし、これらを使用して隣接するデバイスを検出します。アト リビュートには Type、Length、および Value があり、これらを TLV と呼びます。LLDP をサポートする デバイスは、ネイバとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイ ス機能、およびデバイス ID などの 詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV (IEEE 802.1 に固有の TLV)
- MAC/PHY コンフィギュレーション/ステータス TLV (IEEE 802.3 に固有の TLV)



スイッチ スタックは、ネットワーク内で1つのスイッチと見なされます。したがって、LLDP は個々 のスタック メンバーではなく、スイッチ スタックを検出します。

LLDP-MED

(注)

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

LLDP for Media Endpoint Devices (LLDP-MED) は LLDP の拡張版で、IP 電話などのエンドポイン トデバイスとスイッチなどのネットワーク デバイスの間で動作します。特に VoIP アプリケーション をサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet (PoE)、コンポーネント管理、 およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV がイ ネーブルです。

LLDP-MED では、次の TLV がサポートされます。

• LLDP-MED 機能 TLV

LLDP-MED エンドポイントは、接続装置がサポートする機能と現在イネーブルになっている機能 を識別できます。

• ネットワーク ポリシー TLV

ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ2と レイヤ3アトリビュートをポート上の特定アプリケーションにアドバタイズできます。たとえば、 スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のスイッチに接続し、 VLAN 番号を取得してから、呼制御の通信を開始できます。

ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP)、およびタギング モードの 値を指定して、音声と音声信号のプロファイルを作成できます。この後、これらのプロファイル アトリビュートはスイッチ上で一元的に管理されて IP 電話に伝播されます。

• 電源管理 TLV

LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。ス イッチおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスの消費電力などの 電源情報を通知することができます。

LLDP-MED は拡張電源 TLV もサポートして、きめ細かな電力要件、エンドポイント電源プライ オリティ、およびエンドポイントとネットワークの接続デバイスの電源ステータスをアドバタイズ します。ただし、LLDP-MED はエンドポイントとネットワーク接続デバイスとの間のネゴシエー ションを実行しません。

Cisco IOS Release 12.2(52)SE から、LLDP がイネーブルにされてポートに電力が供給されると、 電源 TLV はエンドポイント デバイスの実際の電力要件を決定し、それに基づいてシステム パワー バジェットが調整できるようにします。スイッチは要求を処理し、現在のパワー バジェットに基 づいて電力を許可または拒否します。要求が許可されると、スイッチはパワー バジェットを更新 します。要求が拒否されると、スイッチはポートへの電力供給をオフにし、Syslog メッセージを 生成し、パワー バジェットを更新します。LLDP-MED がディセーブルにされる、またはエンドポ イントが LLDP-MED 電力 TLV をサポートしない場合は、接続中に初期割り当て値(15.4 W) が 使用されます。

power inline {auto [max max-wattage] | never | static [max max-wattage] } インターフェイス コ ンフィギュレーション コマンドを入力して、電力設定を変更できます。PoE インターフェイスは デフォルトで auto モードに設定されています。値を指定しない場合は、最大電力(15.4 W)が供 給されます。

• コンポーネント管理 TLV

エンドポイントは、スイッチにエンドポイントの詳細なコンポーネント情報を送信することが可能 です。コンポーネント情報には、ハードウェア リビジョン、ファームウェア バージョン、ソフト ウェア バージョン、シリアル番号、メーカー名、モデル名、Asset ID TLV などがあります。 LLDP、LLDP-MED、およびワイヤード ロケーション サービスの概要

• ロケーション TLV

スイッチからのロケーション情報をエンドポイント デバイスに提供します。ロケーション TLV は この情報を送信することができます。

- 都市ロケーション情報

都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、 番地、郵便番号などがあります。

- ELIN ロケーション情報

発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号 (ELIN) によって決定されます。これは、緊急通報を Public Safety Answering Point (PSAP) ヘルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすること ができます。

ワイヤード ロケーション サービス



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

スイッチはワイヤード ロケーション サービス機能を使用して、接続されたデバイスのロケーションお よび接続のトラッキング情報を Cisco Mobility Services Engine (MSE; モビリティ サービス エンジン) に送信します。トラッキングされたデバイスは、ワイヤレス エンドポイント、ワイヤード エンドポイ ント、またはワイヤード スイッチやワイヤード コントローラになります。スイッチは、MSE に Network Mobility Services Protocol (NMSP; ネットワーク モビリティ サービス プロトコル) のロケー ション通知および接続通知を介して、デバイスのリンク アップ イベントおよびリンク ダウン イベント を通知します。

MSE がスイッチに対して NMSP 接続を開始すると、サーバ ポートが開きます。MSE がスイッチに接続する場合は、バージョンの互換性を確保する1組のメッセージ交換およびサービス交換情報があり、 その後にロケーション情報の同期が続きます。接続後、スイッチは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンク アップ イベントまたはリンク ダウ ンイベントは、集約されてインターバルの最後に送信されます。

スイッチがリンク アップ イベントまたはリンク ダウン イベントでデバイスの有無を判断した場合は、 スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固有情報を取得しま す。クライアントが LLDP-MED または CDP に対応している場合は、スイッチは LLDP-MED ロケー ション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、スイッチは次のクライアント情報をリンク アップ時に取得します。

- ポート接続で指定されたスロットおよびポート
- クライアント MAC アドレスで指定された MAC アドレス
- ポート接続で指定された IP アドレス
- 802.1X ユーザ名(該当する場合)
- デバイス カテゴリは、wired station として指定されます。
- ステートは new として指定されます。
- シリアル番号、UDI
- モデル番号
- スイッチによる関連付け検出後の時間(秒)

デバイス機能に応じて、スイッチは次のクライアント情報をリンク ダウン時に取得します。

- 切断されたスロットおよびポート
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名(該当する場合)
- デバイス カテゴリは、wired station として指定されます。
- ステートは delete として指定されます。
- シリアル番号、UDI
- スイッチによる関連付け解除の検出後の時間(秒)

スイッチがシャットダウンする場合は、スイッチは、MSE との NMSP 接続を終了する前に、ステート delete および IP アドレスとともに接続情報通知を送信します。MSE は、この通知を、スイッチに関連 付けられているすべてのワイヤード クライアントに対する関連付け解除として解釈します。

スイッチ上のロケーションアドレスを変更すると、スイッチは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

LLDP、LLDP-MED、およびワイヤード ロケーション サー ビスの設定

- 「デフォルト LLDP 設定」(P.26-6)
- 「設定時の注意事項」(P.26-6)
- 「LLDP のイネーブル化」(P.26-7)
- 「LLDP 特性の設定」(P.26-8)
- 「LLDP-MED TLV の設定」(P.26-9)
- 「Network-Policy TLV の設定」(P.26-9)
- 「ロケーション TLV およびワイヤード ロケーション サービスの設定」(P.26-11)

デフォルト LLDP 設定

表 26-1 デフォルト LLDP 設定

機能	デフォルト設定
LLDP グローバル ステート	ディセーブル
LLDP ホールドタイム (廃棄までの時間)	120 秒
LLDP タイマー(パケット更新頻度)	30 秒
LLDP 再初期化遅延	2 秒
LLDP tlv-select	ディセーブル(すべての TLV との送受信)
LLDP インターフェイス ステート	ディセーブル
LLDP 受信	ディセーブル
LLDP 送信	ディセーブル
LLDP med-tlv-select	ディセーブル(すべての LLDP-MED TLV への 送信)LLDP がグローバルにイネーブルにされる と、LLDP-MED-TLV もイネーブルになります。

設定時の注意事項

- インターフェイスがトンネルポートに設定されていると、LLDPは自動的にディセーブルになります。
- ネットワーク ポリシー プロファイルを初めて設定したインターフェイスには、switchport voice vlan コマンドを適用できません。switchport voice vlan vlan-id がすでに設定されているインター フェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインター フェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用さ れます。
- ネットワーク ポリシー プロファイルを持つインターフェイス上では、スタティック セキュア MAC アドレスを設定できません。
- プライベート VLAN ポート上では、ネットワーク ポリシー プロファイルを設定できません。
- ワイヤードロケーションが機能するためには、まず、ip device tracking グローバル コンフィギュレーション コマンドを入力する必要があります。

LLDP のイネーブル化

LLDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lldp run	スイッチ上で LLDP をイネーブルに設定します。
ステップ 3	interface interface-id	LLDP をイネーブルにするインターフェイスを指定し、インター フェイス コンフィギュレーション モードを開始します。
ステップ 4	lldp transmit	LLDP パケットを送信するようにインターフェイスをイネーブル にします。
ステップ 5	lldp receive	LLDP パケットを受信するようにインターフェイスをイネーブル にします。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show lldp	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

LLDP をディセーブルにするには、no lldp run グローバル コンフィギュレーション コマンドを使用し ます。インターフェイス上の LLDP をディセーブルにするには、no lldp transmit および no lldp receive インターフェイス コンフィギュレーション コマンドを使用します。

次に、LLDP をグローバルにイネーブルにする例を示します。

Switch# configure terminal Switch(config)# lldp run Switch(config)# end

次に、インターフェイス上で LLDP をイネーブルにする例を示します。

Switch# configure terminal Switch(config)# interface gigabitethernet0/1 Switch(config-if)# lldp transmit Switch(config-if)# lldp receive Switch(config-if)# end

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。

LLDP 特性を設定するには、特権 EXEC モードで次の手順を実行します。



ステップ2~5は任意であり、どの順番で実行してもかまいません。

	コマント	日 的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lldp holdtime seconds	(任意) デバイスから送信された情報を受信側デバイスが廃棄するま で保持する必要がある期間を指定します。
		指定できる範囲は 0 ~ 65535 秒です。デフォルトは 120 秒です。
ステップ 3	lldp reinit delay	(任意)任意のインターフェイス上でLLDPの初期化の遅延時間 (秒)を指定します。
		指定できる範囲は2~5秒です。デフォルトは2秒です。
ステップ 4	lldp timer rate	(任意)インターフェイス上で LLDP の更新の遅延時間(秒)を指定 します。
		指定できる範囲は 5 ~ 65534 秒です。デフォルトは 30 秒です。
ステップ 5	lldp tlv-select	(任意)送受信する LLDP TLV を指定します。
ステップ 6	lldp med-tlv-select	(任意)送受信する LLDP-MED TLV を指定します。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show lldp	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各 LLDP コマンドの no 形式を使用します。

次に、LLDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

LLDP-MED TLV の設定

デフォルトでは、スイッチはエンド デバイスから LLDP-MED パケットを受信するまで、LLDP パ ケットだけを送信します。スイッチは、MED TLV を持つ LLDP も送信します。LLDP-MED エントリ が期限切れになった場合は、スイッチは再び LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用することで、表 26-2 に示された TLV を送信しないようにインターフェイスを設定できます。

表 26-2 LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED コンポーネント管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイス上で TLV をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	LLDP-MED TLV を設定するインターフェイスを指定し、イン ターフェイス コンフィギュレーション モードを開始します。
ステップ 3	lldp med-tlv-select <i>tlv</i>	イネーブルにする TLV を指定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

Network-Policy TLV の設定

ネットワーク ポリシー プロファイルの作成、ポリシー アトリビュートの設定、およびその設定のイン ターフェイスへの適用をおこなうには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	network-policy profile profile	ネットワーク ポリシー プロファイル番号を指定し、ネットワーク ポ
	number	リシー コンフィギュレーション モードを開始します。指定できる範
		囲は1~4294967295 です。

	コマンド	目的
ステップ3 {voice voice-signaling} vlan [vlan-id {cos cvalue dscp dvalue}] [[dot1n {cos cvalue dscp dvalue}]	ポリシー アトリビュートを設定します。	
	voice:音声アプリケーション タイプを指定します。	
	none untagged]	voice-signaling : 音声シグナリング アプリケーション タイプを指定 します。
		vlan:音声トラフィックのネイティブ VLAN を指定します。
		<i>vlan-id</i> :(任意)音声トラフィックの VLAN を指定します。指定できる範囲は1~4094です。
		cos <i>cvalue</i> : (任意) 設定された VLAN のレイヤ 2 プライオリティ サービス クラス (CoS) を指定します。指定できる範囲は 0 ~ 7 で す。デフォルト値は 0 です。
		dscp <i>dvalue</i> : (任意) 設定された VLAN の Differentiated Services Code Point (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 で す。デフォルト値は 0 です。
		dot1p : (任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように IP 電話を設定します。
		none : (任意) 音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
		untagged :(任意)タグなしの音声トラフィックを送信するように IP 電話を設定します。これが IP Phone のデフォルト設定になります。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	interface interface-id	ネットワーク ポリシー プロファイルを設定するインターフェイスを 指定し、インターフェイス コンフィギュレーション モードを開始し ます。
ステップ 6	network-policy profile number	ネットワーク ポリシー プロファイル番号を指定します。
ステップ 7	Ildp med-tlv-select network-policy	ネットワーク ポリシー TLV を指定します。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	show network-policy profile	 設定を確認します。
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの no 形式を使用します。

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワークポリシー プロファイルおよびネットワーク ポリシー TLV をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを使用したネイティブ VLAN に音声アプリケーション タイプを 設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dotlp cos 4
Switch(config-network-policy)# voice vlan dotlp dscp 34
```

ロケーション TLV およびワイヤード ロケーション サービスの設定

エンドポイントのロケーション情報を設定し、その設定をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	location {admin-tag string	エンドポイントにロケーション情報を設定します。
	civic-location identifier <i>id</i> elin-location string identifier <i>id</i> }	• admin-tag:管理タグまたはサイト情報を指定します。
		• civic-location :都市ロケーション情報を指定します。
		 elin-location: 緊急ロケーション情報(ELIN)を指定します。
		• identifier <i>id</i> : 都市ロケーションの ID を指定します。
		 <i>string</i>: サイト情報またはロケーション情報を英数字形式で 指定します。
ステップ 3	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	interface interface-id	ロケーション情報を設定するインターフェイスを指定し、イン ターフェイス コンフィギュレーション モードを開始します。
ステップ 5	location	インターフェイスにロケーション情報を入力します。
	{additional-location-information <i>word</i> civic-location-id <i>id</i> elin-location-id <i>id</i> }	additional-location-information :ロケーションまたは場所の追 加情報を指定します。
		civic-location-id :インターフェイスのグローバル都市ロケー ション情報を指定します。
		elin-location-id:インターフェイスの緊急ロケーション情報を指 定します。
		<i>id</i> : 都市ロケーションまたは ELIN ロケーションの ID を指定し ます。指定できる ID 範囲は 1 ~ 4095 です。
		<i>word</i> : 追加のロケーション情報を指定する語またはフレーズを指 定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show location	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、各コマンドの no 形式を使用します。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

第 26 章 🛛 LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 📗

スイッチ上でワイヤード ロケーション サービスをイネーブルにするには、特権 EXEC モードで次の手 順を実行します。

スイッチは暗号化されたソフトウェア イメージを実行して、nmsp グローバル コンフィギュレーショ ン コマンドをイネーブルにする必要があります。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	nmsp enable	スイッチで NMSP 機能をイネーブルにします。
ステップ 3	nmsp notification interval {attachment	NMSP 通知間隔を指定します。
	location } interval-seconds	attachment:接続通知間隔を指定します。
		location:位置通知間隔を指定します。
		<i>interval-seconds</i> :スイッチから MSE にロケーション更新または 接続更新が送信されるまでの期間(秒)。指定できる範囲は1~ 30です。デフォルト値は30です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show network-policy profile	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、スイッチ上で NMSP をイネーブルにして、位置通知間隔を 10 秒に設定する方法を示します。

Switch(config)# nmsp enable Switch(config)# nmsp notification interval location 10

<u>》</u> (注)

LLDP、LLDP-MED、およびワイヤード ロケーション サー ビスのモニタリングおよびメンテナンス

デバイス上の LLDP、LLDP-MED、およびワイヤード ロケーション サービスをモニタリングおよびメ ンテナンスするには、特権 EXEC モードで次の作業を1回以上実行します。

コマンド	説明	
clear lldp counters	トラフィック カウンタをゼロにリセットします。	
clear lldp table	LLDP ネイバ情報テーブルを削除します。	
clear nmsp statistics		
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間のよ うな、インターフェイス上のグローバル情報を表示します。	
show lldp entry entry-name	特定のネイバに関する情報を表示します。	
	アスタリスク(*)を入力すると、すべてのネイバの表示、またはネイバの名前 の入力が可能です。	
show lldp interface [interface-id]	LLDP がイネーブルに設定されているインターフェイスに関する情報を表示します。	
	表示対象を特定のインターフェイスに限定できます。	
<pre>show lldp neighbors [interface-id] [detail]</pre>	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバに関する情報を表示します。	
	特定のインターフェイスに関するネイバ情報だけを表示したり、詳細表示にす るため表示内容を拡張したりできます。	
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、 LLDP カウンタ類を表示します。	
show location	エンドポイントにロケーション情報を表示します。	
show network-policy profile	設定されたネットワーク ポリシー プロファイルを表示します。	
show nmsp	NMSP 情報を表示します。	

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド





SPAN および RSPAN の設定

(注)

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

この章では、Catalyst 2960 スイッチに Switched Port Analyzer (SPAN; スイッチド ポート アナライ ザ) および Remote SPAN (RSPAN; リモート SPAN) を設定する方法について説明します。



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

この章で説明する内容は、次のとおりです。

- 「SPAN および RSPAN の概要」(P.27-1)
- 「SPAN および RSPAN の設定」(P.27-10)
- 「SPAN および RSPAN のステータス表示」(P.27-24)

SPAN および RSPAN の概要

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を 使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセ キュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。 SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛 先ポートにコピー(ミラーリング)して、解析します。SPAN は送信元ポートまたは VLAN 上のネッ トワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があり ます。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信 したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に 出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできま せん。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティ ングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN に ルーティングされるトラフィックは、モニタできます。

ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先 ポートを使用できます。たとえば、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサ 装置を宛先ポートに接続すれば、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを閉じることができます。 ここでは、次の概要について説明します。

- 「ローカル SPAN」 (P.27-2)
- 「リモート SPAN」 (P.27-3)
- 「SPAN と RSPAN の概念および用語」(P.27-4)
- 「SPAN および RSPAN と他の機能の相互作用」(P.27-9)

ローカル SPAN

ローカル SPAN は1つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポー トまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意 の VLAN 上の1つまたは複数の送信元ポートからのトラフィック、あるいは1つまたは複数の VLAN からのトラフィックを解析するために宛先ポートヘコピーします。たとえば、図 27-1 の場合、ポート 5 (送信元ポート) 上のすべてのトラフィックがポート10 (宛先ポート) にミラーリングされます。 ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 から のすべてのネットワーク トラフィックを受信します。



図 27-1 単一スイッチでのローカル SPAN の設定例

リモート SPAN



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

RSPAN は異なるスイッチ(または異なるスイッチ スタック)上の送信元ポート、送信元 VLAN、お よび宛先ポートをサポートし、ネットワーク上にある複数のスイッチのリモート モニタリングを可能 にします。図 27-2 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッショ ンのトラフィックは、ユーザが指定した RSPAN VLAN 上で搬送されます。この RSPAN VLAN は、 参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介 して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、 RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 27-2 RSPAN の設定例



SPAN と RSPAN の概念および用語

ここでは、SPAN および RSPAN の設定に関連する概念および用語について説明します。

SPAN セッション

SPAN セッション(ローカルまたはリモート)を使用すると、1 つまたは複数のポート上、あるいは1 つまたは複数の VLAN 上でトラフィックをモニタし、そのモニタしたトラフィックを1 つまたは複数 の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN (すべて単一のネット ワーク デバイス上にある)を結び付けたものです。ローカル SPAN には、送信元セッションおよび宛 先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出 力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも1つの RSPAN 送信元セッション、1つの RSPAN VLAN、および少なくとも1 つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッショ ンは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを 設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッ ションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッショ ンは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームが転送される点を除き、ローカル SPAN セッション に非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再 設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギン グを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、(レイヤ 2 制御パケットを除 く) すべての RSPAN VLAN パケットを解析のためにユーザにコピーすることです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。 RSPAN 送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これ らのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要求に応答する必要があります (「RSPAN VLAN」(P.27-8)を参照)。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を 混在させることはできません。
- スイッチは最大2つの送信元セッションをサポートします(ローカル SPAN および RSPAN 送信元 セッション)。同じスイッチ内で、ローカル SPAN と RSPAN のソース セッションの両方を実行で きます。スイッチ は合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、設定できる宛先ポートは最大で 64 個です。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送 信元セッションを 2 つ個別に設定できます。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットの廃棄または消失を招くことがあります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは2回伝送されます(1回は標準トラフィックとして、もう1回はモニタされたパケットとして)。したがって、多数のポートまたはVLANをモニタすると、大量のネットワークトラフィックが生成されることがあります。

- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に 宛先ポートと少なくとも1つの送信元ポートまたは VLAN をイネーブルにしないかぎり、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行することはできません。

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプをモニタできます。

 RX(受信)SPAN:受信(または入力)SPANの役割は、送信元インターフェイスまたはVLAN が受信したすべてのパケットを、スイッチが変更または処理を行う前にできるだけ多くモニタする ことです。送信元が受信した各パケットのコピーがそのSPANセッションに対応する宛先ポート に送られます。

Differentiated Services Code Point (DSCP) の変更など、ルーティングや Quality of Service (QoS) が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットを廃棄する可能性のある機能は、入力 SPAN には影響を与えません。宛先 ポートは、実際の着信パケットが廃棄された場合でも、パケットのコピーを受信します。パケット を廃棄する可能性のある機能は、標準および拡張 IP 入力 Access Control List (ACL; アクセス制御 リスト)、入力 QoS ポリシング、および出力 QoS ポリシングです。

 TX(送信)SPAN:送信(または出力)SPANの役割は、スイッチによる変更および処理がすべて 完了したあとで、送信元インターフェイスが送信したすべてのパケットをできるだけ多くモニタす ることです。送信元が送信した各パケットのコピーがそのSPANセッションに対応する宛先ポー トに送られます。コピーはパケットの変更後に用意されます。

送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

 両方: SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これがデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。 通常、SPAN は Cisco Discovery Protocol (CDP)、VLAN Trunking Protocol (VTP; VLAN トランキ ング プロトコル)、Dynamic Trunking Protocol (DTP)、Spanning-Tree Protocol (STP; スパニング ツ リー プロトコル)、Port Aggregation Protocol (PAgP) などの Bridge Protocol Data Unit (BPDU; ブ リッジ プロトコル データ ユニット) パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、 宛先ポートを設定するときに encapsulation replicate キーワードを入力すると、次の変更が発生しま す。

- 送信元ポートの場合と同じカプセル化設定(タグなし、または IEEE 802.1Q)を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タ グなし、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケット が廃棄されることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニ タされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。

• スイッチの輻輳が原因で廃棄された出力パケットは、出力 SPAN からも廃棄されます。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。 たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向(RX と TX) SPAN セッ ションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にス イッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、両 方のパケットは同じものになります。

送信元ポート

送信元ポート(別名 監視対象ポート)は、ネットワークトラフィック分析のために監視するスイッチ ドポートです。1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポート または VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送 信元ポート(スイッチで利用可能なポートの最大数まで)と任意の数の送信元 VLAN(サポートされ ている VLAN の最大数まで)をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数は最大 2 つ(ローカルまたは RSPAN)であるため、単一のセッションに ポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向(入力、出力、または両方)を指定して、各送信元ポートを設定できます。
- すべてのポート タイプ(EtherChannel、ファスト イーサネット、ギガビット イーサネットなど) が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含ま れている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセス ポート、トランク ポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN (VSPAN) では、1 つまたは複数の VLAN のネットワーク トラフィックをモ ニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラ フィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方 向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN の トラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブな すべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。

- VLAN フィルタリングが適用されるのは、トランクポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベース セッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポートタイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートおよび VLAN からの トラフィックのコピーを受信し、SPAN パケットをユーザ(通常はネットワーク アナライザ)に送信 する宛先ポート(別名*モニタ側ポート*)が必要です。

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションのみを実行するスイッチには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定 を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している 間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。
- 任意のイーサネット物理ポートにできます。
- セキュアポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- 一度に1つの SPAN セッションにしか参加できません(ある SPAN セッションの宛先ポートは、 別の SPAN セッションの宛先ポートになることはできません)。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに 必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送し たりしません。
- 入力トラフィックの転送がネットワークセキュリティデバイスでイネーブルの場合、宛先ポートはレイヤ2でトラフィックを転送します。
- レイヤ2プロトコル (STP、VTP、CDP、DTP、PAgP) のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、 モニタされません。
- スイッチの宛先ポートの最大数は64です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化について次のとおり 動作が異なります。

- ローカル SPAN では、宛先ポートに encapsulation replicate キーワードが指定されている場合、 各パケットに元のカプセル化が使用されます(タグなし、または IEEE 802.1Q)。これらのキー ワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、 encapsulation replicate がイネーブルになっているローカル SPAN セッションの出力に、タグな し、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、**RSPAN** の送信元セッションと宛先セッション間で **SPAN** トラフィックを伝送しま す。**RSPAN VLAN** には次の特殊な特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC (メディア アクセス制御) アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、remote-span VLAN コンフィギュレーション モード コマンドを使用して、 VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。

VTP に対して可視である VLAN 1 ~ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP に よって伝播されます。拡張 VLAN 範囲(1006 ~ 4094) 内の RSPAN VLAN ID を割り当てる場合は、 すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク 全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対し て複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィッ クを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- STP: SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。
 SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送 信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送す るトランク ポート上でアクティブにできます。
- CDP: SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP: VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランキング:送信元ポート、または宛先ポートの VLAN メンバシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの VLAN メンバシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel: EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場 合、グループ全体がモニタされます。

モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポート リストに新 しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信 元ポート リストからそのポートが自動的に削除されます。

EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加し ているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含ま れる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。 SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。 EtherChannel グループから削除されたポートは、グループ メンバーのままですが、*inactive* また は *suspended* ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが 送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポート リストから削除されま す。

- マルチキャストトラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未 編集のパケットが1つだけ SPAN 宛先ポートに送信されます。マルチキャストパケットの送信回 数は反映されません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポート でポート セキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力を モニタしているポートでポート セキュリティをイネーブルにしないでください。

 IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイ ネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブ ルに設定されます。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポート で IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタ しているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN および RSPAN の設定

ここでは、次の設定情報について説明します。

- 「SPAN および RSPAN のデフォルト設定」(P.27-10)
- 「ローカル SPAN の設定」 (P.27-10)
- 「RSPAN の設定」(P.27-17)

SPAN および RSPAN のデフォルト設定

表 27-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 27-1 SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート (SPAN および RSPAN)	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方(both)
カプセル化タイプ (宛先ポート)	ネイティブ形式(タグなしパケット)
入力転送(宛先ポート)	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェ イス上で、すべての VLAN がモニタ対象
RSPAN VLAN	未設定

ローカル SPAN の設定

ここでは、次の設定情報について説明します。

- 「SPAN 設定時の注意事項」(P.27-10)
- 「ローカル SPAN セッションの作成」(P.27-11)
- 「ローカル SPAN セッションの作成および着信トラフィックの設定」(P.27-14)
- 「フィルタリングする VLAN の指定」(P.27-16)

SPAN 設定時の注意事項

SPAN を設定するときには、次の注意事項に従ってください。

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで2つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。 SPAN 宛先ポートを通過するトラフィックがモニタされるだけです。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、no monitor session {session_number | all | local | remote} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、encapsulation replicate キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー(タグなし、または IEEE 802.1Q)を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。 RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも1つの送信元ポートまたは送信元 VLAN がイ ネーブルになってからです。
- SPAN トラフィックを特定の VLAN に制限するには、filter vlan キーワードを使用します。トランクポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランクポート上のすべての VLAN がモニタされます。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元(モニタ対象)ポートまたは VLAN、および宛先(モニタ側) ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all	セッションに対する既存の SPAN 設定を削除します。
	local remote}	session_number の範囲は、 $1 \sim 66$ です。
		すべての SPAN セッションを削除する場合は all、すべてのロー カル セッションを削除する場合は local、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定しま す。

	コマンド	目的
ステップ 3	<pre>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</pre>	SPAN セッションおよび送信元ポート(モニタ対象ポート)を指定します。
		session_numberの範囲は、 $1 \sim 66$ です。
		<i>interface-id</i> には、モニタする送信元ポートまたは送信元 VLAN を指定します。
		 送信元 <i>interface-id</i> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス(port-channel port-channel-number)があります。有効なポートチャネル番号は1~6です。
		 <i>vlan-id</i>には、モニタする送信元 VLAN を指定します。指定 できる範囲は1~4094です(RSPAN VLAN は除く)。
		 (注) 1 つのセッションに、一連のコマンドで定義された複数 の送信元(ポートまたは VLAN)を含めることができま す。ただし、1 つのセッション内で送信元ポートと送信 元 VLAN を併用することはできません。
		(任意) [, -]:一連のインターフェイスまたはインターフェイス 範囲を指定します。カンマの前後およびハイフンの前後にスペー スを1つずつ入力します。
		(任意) モニタするトラフィックの方向を指定します。トラ フィックの方向を指定しなかった場合、SPAN は送信トラフィッ クと受信トラフィックの両方をモニタします。
		 both:送信トラフィックと受信トラフィックの両方をモニタ します。これがデフォルトです。
		• rx:受信トラフィックをモニタします。
		• tx:送信トラフィックをモニタします。
		(注) monitor session session_number source コマンドを複数 回使用すると、複数の送信元ポートを設定できます。

	コマンド	目的
ステップ 4	monitor session session_number destination {interface interface-id [, -] [encapsulation {dot1q replicate}]}	SPAN セッションおよび宛先ポート(モニタ側ポート)を指定します。
		session_number には、ステップ 3 で入力したセッション番号を 指定します。
		(注) ローカル SPAN の場合は、送信元および宛先インター フェイスに同じセッション番号を使用する必要がありま す。
		<i>interface-id</i> には、宛先ポートを指定します。宛先インターフェ イスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。
		(任意) [, -]: 一連のインターフェイスまたはインターフェイス 範囲を指定します。カンマの前後およびハイフンの前後にスペー スを1つずつ入力します。
		(任意) 宛先インターフェイスで IEEE 802.1Q カプセル化方式の 使用を指定するには、encapsulation dot1q を入力します。
		(任意)送信元インターフェイスのカプセル化方式が宛先イン ターフェイスで複製されるように指定するには、encapsulation replicate を入力します。これを選択しない場合、デフォルトで は、パケットがネイティブ形式(タグなし)で送信されます。
		(注) monitor session session_number destination コマンドを 複数回使用すると、複数の宛先ポートを設定できます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	<pre>show monitor [session session_number]</pre>	設定を確認します。
	show running-config	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、no monitor session session_number グローバル コンフィギュレー ション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削 除する場合は、no monitor session session_number source {interface interface-id | vlan vlan-id} グ ローバル コンフィギュレーション コマンドまたは no monitor session session_number destination interface interface-id グローバル コンフィギュレーション コマンドを使用します。宛先インターフェ イスの場合、このコマンドの no 形式では、encapsulation オプションは無視されます。

次に、SPAN セッション1を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例 を示します。最初に、セッション1の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、 双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 ヘミラーリン グします。

Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
Switch(config)# end

次に、SPAN セッション1の SPAN 送信元としてのポート1を削除する例を示します。

Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end

次に、双方向モニタが設定されていたポート1で、受信トラフィックのモニタをディセーブルにする例 を示します。

Switch(config) # no monitor session 1 source interface gigabitethernet0/1 rx

ポート1で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるト ラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ~ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートで すべてのトラフィックをモニタするよう変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定したあと、宛 先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサ装置等) 用に着信トラフィックを イネーブルにするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「ローカル SPAN セッションの作成」 (P.27-11)を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all local remote}	セッションに対する既存の SPAN 設定を削除します。
ステップ 3	<pre>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</pre>	SPAN セッションおよび送信元ポート(モニタ対象ポート)を指 定します。

	コマンド	目的
ステップ 4	monitor session session_number destination { interface interface-id [, -]	SPAN セッション、宛先ポート、パケットカプセル化、および入 力 VLAN とカプセル化を指定します。
	[encapsulation {dot1q replicate}] [ingress {dot1q vlan vlan-id untagged vlan vlan-id vlan vlan-id}]}	session_number には、ステップ 3 で入力したセッション番号を 指定します。
		<i>interface-id</i> には、宛先ポートを指定します。宛先インターフェ イスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。
		(任意) [, -]: 一連のインターフェイスまたはインターフェイス 範囲を指定します。カンマまたはハイフンの前後にスペースを1 つずつ入力します。
		(任意) 宛先インターフェイスで IEEE 802.1Q カプセル化方式の 使用を指定するには、encapsulation dot1q を入力します。
		(任意)送信元インターフェイスのカプセル化方式が宛先イン ターフェイスで複製されるように指定するには、encapsulation replicate を入力します。これを選択しない場合、デフォルトで は、パケットがネイティブ形式(タグなし)で送信されます。
		宛先ポートでの着信トラフィックの転送をイネーブルにして、カ プセル化タイプを指定するには、ingress をキーワードと一緒に 入力します。
		 dot1q vlan vlan-id: デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケット を受信します。
		 untagged vlan vlan-id または vlan vlan-id: デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化さ れた着信パケットを受信します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	<pre>show monitor [session session_number]</pre>	設定を確認します。
	show running-config	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、no monitor session session_number グローバル コンフィギュレー ション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削 除する場合は、no monitor session session_number source {interface interface-id | vlan vlan-id} グ ローバル コンフィギュレーション コマンドまたは no monitor session session_number destination interface interface-id グローバル コンフィギュレーション コマンドを使用します。宛先インターフェ イスの場合、このコマンドの no 形式を使用すると、カプセル化および入力オプションは無視されま す。

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるト ラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方 式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN とし て IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all	セッションに対する既存の SPAN 設定を削除します。
	local remote}	session_number の範囲は、 $1 \sim 66$ です。
		すべての SPAN セッションを削除する場合は all、すべてのローカ ル セッションを削除する場合は local、すべてのリモート SPAN
		セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3	monitor session session_number source interface interface-id	送信元ポート(モニタ対象ポート)と SPAN セッションの特性を 指定します。
		session_number の範囲は、 $1 \sim 66$ です。
		<i>interface-id</i> には、モニタする送信元ポートを指定します。指定さ れたインターフェイスは、あらかじめトランク ポートとして設定 されていなければなりません。
ステップ 4	monitor session session_number filter vlan vlan-id [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。
		<i>session_number</i> には、ステップ3で指定したセッション番号を入力します。
		<i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
		(任意) カンマ(,) を使用して一連の VLAN を指定するか、ハイ フン(-) を使用して VLAN 範囲を指定します。カンマの前後お よびハイフンの前後にスペースを l つずつ入力します。
ステップ 5	monitor session session_number destination { interface interface-id [, -] [encapsulation { dot1q replicate }]}	SPAN セッションおよび宛先ポート(モニタ側ポート)を指定し ます。
		<i>session_number</i> には、ステップ3で入力したセッション番号を指定します。
		<i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannelや VLAN は指定できません。
		(任意) [, -]:一連のインターフェイスまたはインターフェイス 範囲を指定します。カンマの前後およびハイフンの前後にスペー スを1つずつ入力します。
		(任意) 宛先インターフェイスで IEEE 802.1Q カプセル化方式の 使用を指定するには、 encapsulation dot1q を入力します。
		(任意)送信元インターフェイスのカプセル化方式が宛先インター フェイスで複製されるように指定するには、encapsulation replicate を入力します。これを選択しない場合、デフォルトで は、パケットがネイティブ形式(タグなし)で送信されます。
ステップ 6	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<pre>show monitor [session session_number]</pre>	設定を確認します。
	show running-config	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、no monitor session session_number filter グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config) # no monitor session 2
Switch(config) # monitor session 2 source interface gigabitethernet0/2 rx
Switch(config) # monitor session 2 filter vlan 1 - 5, 9
Switch(config) # monitor session 2 destination interface gigabitethernet0/1
Switch(config) # end
```

RSPAN の設定

ここでは、次の設定情報について説明します。

- 「RSPAN 設定時の注意事項」(P.27-17)
- 「RSPAN VLAN としての VLAN の設定」(P.27-18)
- 「RSPAN 送信元セッションの作成」(P.27-19)
- 「RSPAN 宛先セッションの作成」(P.27-20)
- 「RSPAN 宛先セッションの作成および着信トラフィックの設定」(P.27-21)
- 「フィルタリングする VLAN の指定」(P.27-23)

RSPAN 設定時の注意事項

RSPAN を設定するときには、次の注意事項に従ってください。

- 「SPAN 設定時の注意事項」(P.27-10)のすべての項目は RSPAN にも当てはまります。
- RSPAN VLAN には特殊な特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたは モニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに 分散させることができます。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート(音声 VLAN ポートを含む)は、非アクティブ ステートにな ります。

- 送信元トランクポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。
- 次の条件を満たすかぎり、任意の VLAN を RSPAN VLAN として設定できます。
 - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加するすべてのスイッチで RSPAN がサポートされている。
- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプ ルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィック のフラッディングが防止されます。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッションの RSPAN VLAN となる VLAN を新規に作成します。RSPAN に参加する すべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲(1005 未満) であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できま す。拡張範囲 VLAN (1005 を超える ID) の場合、送信元と宛先の両方のスイッチ、および中間スイッ チに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

RSPAN VLAN を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan vlan-id	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーショ ン モードを開始します。有効範囲は 2 ~ 1001 および 1006 ~ 4094 です。
		RSPAN VLAN を VLAN 1 (デフォルト VLAN) または VLAN ID 1002 ~ 1005 (トークンリングおよび Fiber Distributed Data Interface [FDDI] VLAN 専用) にすることはできません。
ステップ 3	remote-span	VLAN を RSPAN VLAN として設定します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、no remote-span VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all local remote}	セッションに対する既存の RSPAN 設定を削除します。
		session_number の範囲は、 $1 \sim 66$ です。
		すべての RSPAN セッションを削除する場合は all、すべての ローカル セッションを削除する場合は local、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定しま す。
ステップ 3	monitor session session_number source {interface interface-id vlan vlan-id} [, -] Fine (1) [, -]	RSPAN セッションおよび送信元ポート(モニタ対象ポート)を 指定します。
	[both rx tx]	session_number の範囲は、 $1 \sim 66$ です。
		RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。
		 <i>interface-id</i>には、モニタする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよび ポート チャネル論理インターフェイス (port-channel port-channel-number) があります。有効なポートチャネル 番号は1~6です。
		 <i>vlan-id</i>には、モニタする送信元 VLAN を指定します。指定 できる範囲は1~4094です(RSPAN VLAN は除く)。
		 1 つのセッションに、一連のコマンドで定義された複数の送 信元(ポートまたは VLAN)を含めることができます。た だし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。
		(任意) [, -]:一連のインターフェイスまたはインターフェイス 範囲を指定します。カンマの前後およびハイフンの前後にスペー スを1つずつ入力します。
		(任意) モニタするトラフィックの方向を指定します。トラ フィックの方向を指定しなかった場合、送信元インターフェイス は送信トラフィックと受信トラフィックの両方を送信します。
		 both:送信トラフィックと受信トラフィックの両方をモニタ します。
		• rx:受信トラフィックをモニタします。
		• tx:送信トラフィックをモニタします。
ステップ 4	monitor session session_number	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。
	destination remote vlan vlan-id	session_number には、ステップ 3 で指定した番号を入力します。
		vlan-id には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。

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

SPAN セッションを削除するには、no monitor session session_number グローバル コンフィギュレー ション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、no monitor session *session_number* source {interface-*id* | vlan *vlan-id*} グローバル コンフィギュレーション コ マンドを使用します。セッションから RSPAN VLAN を削除するには、no monitor session *session number* destination remote vlan *vlan-id* コマンドを使用します。

次に、セッション1に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタ するように RSPAN セッション1を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示しま す。

Switch(config) # no monitor session 1
Switch(config) # monitor session 1 source interface gigabitethernet0/1 tx
Switch(config) # monitor session 1 source interface gigabitethernet0/2 rx

Switch(config) # monitor session 1 source interface port-channel 2
Switch(config) # monitor session 1 destination remote vlan 901
Switch(config) # end

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチ(送信元セッションが設定されていないスイッチ)に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan vlan-id	送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力 し、VLAN コンフィギュレーション モードを開始します。
		両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ~ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ~ 4 は不要です。
ステップ 3	remote-span	VLAN を RSPAN VLAN として識別します。
ステップ 4	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	no monitor session {session_number all local remote}	セッションに対する既存の RSPAN 設定を削除します。
		session_number の範囲は、 $1 \sim 66$ です。
		すべての RSPAN セッションを削除する場合は all、すべての ローカル セッションを削除する場合は local、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定しま す。

	コマンド	目的
ステップ 6	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。
		session_numberの範囲は、 $1 \sim 66$ です。
		<i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	monitor session session_number destination interface interface-id	RSPAN セッションおよび宛先インターフェイスを指定します。
		session_number には、ステップ 6 で指定した番号を入力します。
		RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先 ポートに同じセッション番号を使用する必要があります。
		<i>interface-id</i> には、宛先インターフェイスを指定します。宛先イ ンターフェイスは物理インターフェイスでなければなりません。
		encapsulation replicate はコマンドラインのヘルプ ストリング に表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート 上のすべてのパケットはタグなしになります。
ステップ 8	end	特権 EXEC モードに戻ります。
ステップ 9	<pre>show monitor [session session_number]</pre>	設定を確認します。
	show running-config	
ステップ 10	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SPAN セッションを削除するには、no monitor session *session_number* グローバル コンフィギュレー ション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、no monitor session *session_number* destination interface *interface-id* グローバル コンフィギュレーション コマンドを使用 します。セッションから RSPAN VLAN を削除するには、no monitor session *session_number* source remote vlan *vlan-id* コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例 を示します。

Switch(config) # monitor session 1 source remote vlan 901
Switch(config) # monitor session 1 destination interface gigabitethernet0/1
Switch(config) # end

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートで ネットワーク セキュリティ デバイス (Cisco IDS センサ装置等) 用に着信トラフィックをイネーブル にするには、特権 EXEC モードで次の手順を実行します。

着信トラフィックに関係しないキーワードの詳細については、「RSPAN 宛先セッションの作成」 (P.27-20)を参照してください。この手順は、RSPAN VLAN がすでに設定されていることを前提にし ています。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all local remote}	セッションに対する既存の SPAN 設定を削除します。

	コマンド	目的
ステップ 3	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i>	RSPAN セッションおよび送信元 RSPAN VLAN を指定します。
		session_numberの範囲は、 $1 \sim 66$ です。
		<i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 4	monitor session session_number destination { interface interface-id	SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。
	[, -] [ingress {dot1q vlan vlan-id	session_number には、ステップ 4 で指定した番号を入力します。
	vlan-id}]}	RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに 同じセッション番号を使用する必要があります。
		<i>interface-id</i> には、宛先インターフェイスを指定します。宛先インター フェイスは物理インターフェイスでなければなりません。
		encapsulation replicate はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケッ トはタグなしになります。
		(任意) [, -]:一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。
		宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル 化タイプを指定するには、ingress を追加のキーワードと一緒に入力しま す。
		 dot1q vlan vlan-id : VLAN をデフォルトの VLAN として指定し、 IEEE 802.1Q カプセル化を使用して着信パケットを転送します。
		 untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show monitor [session session_number]	設定を確認します。
	show running-config	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

RSPAN セッションを削除する場合は、no monitor session session_number グローバル コンフィギュ レーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、no monitor session session_number destination interface interface-id グローバル コンフィギュレーション コマン ドを使用します。入力オプションは、no 形式では無視されます。

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として 着信トラフィックの転送をイネーブルにする例を示します。

Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6
Switch(config)# end

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するに は、特権 EXEC モードで次の手順を実行します。

		目的
フテップィ	aonfigure terminal	
ステップ 2	configure terminal	クローハルコンノイキュレーションモートを開始します。
	no monitor session {session_number all local remote}	セッションに対する既存の SPAN 設定を削除します。
		session_number の範囲は、 $1 \sim 66$ です。
		すべての SPAN セッションを削除する場合は all、すべてのローカ ル セッションを削除する場合は local、すべてのリモート SPAN セッションを削除する場合は remote をそれぞれ指定します。
ステップ 3	monitor session session_number source interface interface-id	送信元ポート(モニタ対象ポート)と SPAN セッションの特性を 指定します。
		session_number の範囲は、 $1 \sim 66$ です。
		<i>interface-id</i> には、モニタする送信元ポートを指定します。指定さ れたインターフェイスは、あらかじめトランク ポートとして設定 されていなければなりません。
ステップ 4	monitor session session_number filter vlan vlan-id [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。
		<i>session_number</i> には、ステップ3で指定したセッション番号を入力します。
		<i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
		(任意) カンマ(,) を使用して一連の VLAN を指定するか、ハイ フン(-) を使用して VLAN 範囲を指定します。カンマの前後お よびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i>	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。
		session_number には、ステップ 3 で指定したセッション番号を入力します。
		<i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	<pre>show monitor [session session_number]</pre>	設定を確認します。
	show running-config	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

トランク ポート上のすべての VLAN をモニタするには、no monitor session_number filter vlan グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモ ニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛 先 RSPAN VLAN 902 に送信する例を示します。

Switch(config) # no monitor session 2
Switch(config) # monitor session 2 source interface gigabitethernet0/2 rx
Switch(config) # monitor session 2 filter vlan 1 - 5, 9
Switch(config) # monitor session 2 destination remote vlan 902
Switch(config) # end

SPAN および RSPAN のステータス表示

現在の SPAN または RSPAN 設定を表示するには、show monitor ユーザ EXEC コマンドを使用しま す。また、設定された SPAN および RSPAN セッションを表示するには、show running-config 特権 EXEC コマンドを使用できます。



CHAPTER **28**

RMON の設定

この章では、Catalyst スイッチに Remote Network Monitoring (RMON)を設定する方法について説 明します。2960

RMON は、RMON 準拠のコンソール システムとネットワーク プローブ間で交換可能な一連の統計情報と機能を定義した標準モニタリング仕様です。RMON によって、総合的なネットワーク障害診断、 プランニング、パフォーマンス チューニングに関する情報が得られます。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」のセクションを参照してください。これには、Cisco.com のホームページ (**Documentation > Cisco IOS Software > 12.2 Mainline > Command References**) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「RMON の概要」(P.28-1)
- 「RMON の設定」(P.28-3)
- 「RMON ステータスの表示」(P.28-7)

RMONの概要

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリン グ データを交換できるようにするための、Internet Engineering Task Force (IETF) 標準モニタリング 仕様です。図 28-1 のように、RMON 機能をスイッチの SNMP(簡易ネットワーク管理プロトコル) エージェントと組み合わせて使用することによって、接続されているすべての LAN セグメント上のス イッチ間で流れるすべてのトラフィックを監視できます。



スイッチは次の RMON グループ (RFC 1757 で定義)をサポートしています。

- 統計情報(RMON グループ1): インターフェイス上のイーサネットの統計情報(スイッチタイプ とサポートされているインターフェイスに応じて、ファストイーサネットやギガビットイーサ ネット統計情報など)を収集します。
- 履歴(RMON グループ2):指定されたポーリング間隔で、イーサネットポート上(スイッチタイプおよびサポートされるインターフェイスに応じた、ファストイーサネットおよびギガビットイーサネット統計情報を含む)の統計情報グループの履歴を収集します。
- アラーム(RMON グループ 3):指定された期間、特定の MIB(管理情報ベース)オブジェクトを 監視し、指定された値(上限しきい値)でアラームを発生し、別の値(下限しきい値)でアラーム をリセットします。アラームはイベントと組み合わせて使用できます。アラームがイベントを発生 させ、イベントによってログエントリまたは SNMPトラップが生成されるようにできます。
- イベント(RMON グループ9): アラームによってイベントが発生したときのアクションを指定します。アクションは、ログエントリまたはSNMPトラップを生成できます。

このソフトウェア リリースがサポートするスイッチは、RMON データの処理にハードウェア カウンタ を使用するので、モニタが効率的になり、処理能力はほとんど必要ありません。



64 ビット カウンタは、RMON アラームではサポートされていません。

RMON の設定

ここでは、次の設定情報について説明します。

- 「RMON のデフォルト設定」(P.28-3)
- 「RMON アラームおよびイベントの設定」(P.28-3)(必須)
- •「インターフェイス上でのグループ履歴統計情報の収集」(P.28-5)(任意)
- 「インターフェイス上でのイーサネット グループ統計情報の収集」(P.28-6)(任意)

RMON のデフォルト設定

RMON はデフォルトでディセーブルです。アラームまたはイベントは設定されていません。

RMON アラームおよびイベントの設定

スイッチを RMON 対応として設定するには、CLI (コマンドライン インターフェイス) または SNMP 準拠の Network Management Station (NMS; ネットワーク管理ステーション) を使用します。NMS 上 で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用するこ とを推奨します。RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定する ことも必要です。詳細は、第 30 章「SNMP の設定」を参照してください。



64 ビット カウンタは、RMON アラームではサポートされていません。

RMON アラームおよびイベントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開 始します。
ステップ 2	rmon alarm number variable interval { absolute delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner string]	MIB オブジェクトにアラームを設定します。
		 number には、アラーム番号を指定します。 指定できる範囲は 1 ~ 65535 です。
		 variable には、モニタ対象の MIB オブジェ クトを指定します。
		 interval には、アラームが MIB 変数を監視 する時間を秒数で指定します。指定できる範 囲は1~4294967295 秒です。
		 各 MIB 変数を直接テストする場合は、 absolute キーワードを指定します。MIB 変 数のサンプル間の変動をテストする場合は、 delta キーワードを指定します。
		 value には、アラームを発生させる値および アラームがリセットされる値を指定します。 上限および下限しきい値に指定できる範囲は -2147483648 ~ 2147483647 です。
		 (任意) event-number には、上限および下限 しきい値が限度を超えた場合に発生させるイ ベントの番号を指定します。
		 (任意) owner string には、アラームの所有 者を指定します。
ステップ 3	rmon event number [description string] [log] [owner string] [trap community]	RMON イベント番号に対応付けられた RMON イベント テーブルにイベントを追加します。
		 number には、イベント番号を割り当てます。指定できる範囲は1~65535です。
		 (任意) description string には、イベントの 説明を指定します。
		 (任意) イベント発生時に RMON ログ エン トリを生成する場合は、log キーワードを使 用します。
		 (任意) owner <i>string</i> には、イベントの所有 者を指定します。
		 (任意) trap community には、このトラップ 用の SNMP コミュニティ ストリングを入力 します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定 を保存します。

アラームをディセーブルにするには、設定した各アラームに対して、normon alarm number グローバ ル コンフィギュレーション コマンドを使用します。設定したすべてのアラームを一度にディセーブル にすることはできません。イベントをディセーブルにするには、normon event number グローバル コ ンフィギュレーション コマンドを使用します。アラームおよびイベントの詳細および相互作用につい ては、RFC 1757 を参照してください。

任意の MIB オブジェクトにアラームを設定できます。次の例では、rmon alarm コマンドを使用して、 RMON アラーム番号 10 を設定します。このアラームは、ディセーブルにされないかぎり、20 秒ごと に 1 度の間隔で MIB 変数 *ifEntry.20.1* を監視し、変数の上下の変動をチェックします。*ifEntry.20.1* 値 で MIB カウンタが 100000 から 100015 になるなど、15 以上増加すると、アラームが発生します。そ のアラームによってさらにイベント番号 1 が発生します。イベント番号 1 は、rmon event コマンドで 設定されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。*ifEntry.20.1* 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

Switch(config) # rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner jjohnson

次に、**rmon event** コマンドを使用して **RMON** イベント番号 1 を作成する例を示します。このイベン トは *High ifOutErrors* と定義され、アラームによってイベントが発生したときに、ログ エントリが生 成されます。ユーザ *jjones* が、このコマンドによってイベント テーブルに作成される行を所有します。 次の例の場合も、イベント発生時に **SNMP** トラップが生成されます。

Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones

インターフェイス上でのグループ履歴統計情報の収集

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

インターフェイス上でグループ履歴統計情報を収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	履歴を収集するインターフェイスを指定し、インターフェイ ス コンフィギュレーション モードを開始します。
ステップ 3	rmon collection history <i>index</i> [buckets <i>bucket-number</i>] [interval <i>seconds</i>] [owner <i>ownername</i>]	 指定されたバケット数および時間で、履歴収集をイネーブルにします。 <i>index</i>には、RMON 統計グループを指定します。指定できる範囲は1~65535です。
		 (任意) buckets bucket-number には、RMON 統計グ ループ履歴収集に必要な最大バケット数を指定します。 指定できる範囲は1~65535です。デフォルトのバケッ ト数は50です。
		 (任意) interval seconds には、ポーリング サイクルを秒 数で指定します。指定できる範囲は1~3600 です。デ フォルトは 1800 秒です。
		 (任意) owner ownername には、RMON 統計グループの 所有者名を入力します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。

	コマンド	目的
ステップ 6	show rmon history	スイッチ履歴テーブルの内容を表示します。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま
		す。

履歴収集をディセーブルにするには、no rmon collection history *index* インターフェイス コンフィ ギュレーション コマンドを使用します。

インターフェイス上でのイーサネット グループ統計情報の収集

インターフェイス上でイーサネット統計グループを収集するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	統計情報を収集するインターフェイスを指定し、インター フェイス コンフィギュレーション モードを開始します。
ステップ 3	rmon collection stats <i>index</i> [owner <i>ownername</i>]	インターフェイス上で RMON 統計情報収集をイネーブルに します。
		 <i>index</i>には、RMON 統計グループを指定します。指定で きる範囲は1~65535です。
		 (任意) owner ownername には、RMON 統計グループの 所有者名を入力します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	show rmon statistics	スイッチ統計テーブルの内容を表示します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

イーサネット統計グループの収集をディセーブルにするには、no rmon collection stats *index* インター フェイス コンフィギュレーション コマンドを使用します。

次に、所有者 root の RMON 統計情報を収集する例を示します。

Switch(config) # interface gigabitethernet0/1
Switch(config-if) # rmon collection stats 2 owner root

RMON ステータスの表示

RMON ステータスを表示するには、表 28-1 の特権 EXEC コマンドを1つまたは複数使用します。

表 28-1 RMON ステータスを表示するコマンド

コマンド	目的
show rmon	汎用 RMON 統計情報を表示します。
show rmon alarms	RMON アラーム テーブルを表示します。
show rmon events	RMON イベント テーブルを表示します。
show rmon history	RMON 履歴テーブルを表示します。
show rmon statistics	RMON 統計情報テーブルを表示します。

これらの表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「System Management Commands」のセクションを参照してく ださい。これには、Cisco.com のホームページ(Documentation > Cisco IOS Software > 12.2 Mainline > Command References)からアクセス可能です。 ■ RMON ステータスの表示





システム メッセージ ロギングの設定

この章では、Catalyst 2960 スイッチにシステム メッセージ ロギングを設定する方法について説明します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。これには、Cisco.com のホームページ (**Documentation > Cisco IOS Software > 12.2 Mainline > Command References**) からア クセス可能です。

この章で説明する内容は、次のとおりです。

- 「システム メッセージ ロギングの概要」(P.29-2)
- 「システム メッセージ ロギングの設定」(P.29-2)
- 「ロギング設定の表示」(P.29-15)



高レートでコンソールへのメッセージを記録すると、CPU の利用率が高くなり、スイッチの動作に 悪影響を与える可能性があります。

システム メッセージ ロギングの概要

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギング プロセスに送信します。ロギング プロセスはログ メッセージを各宛先(設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど)に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。



Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

ロギングプロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージ は生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割 り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してか らです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログメッセージにタイムスタンプを設定したり、Syslog送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステムメッセージガイドを参照してください。

記録されたシステム メッセージにアクセスするには、スイッチの CLI (コマンドライン インターフェ イス)を使用するか、正しく設定された Syslog サーバにシステム メッセージを保存します。スイッチ ソフトウェアは Syslog メッセージを内部バッファに保存します。

システム メッセージをリモートでモニタするには、Syslog サーバ上でログを表示するか、または Telnet あるいはコンソール ポート経由でスイッチにアクセスします。

システム メッセージ ロギングの設定

ここでは、次の設定情報について説明します。

- 「システム ログ メッセージのフォーマット」(P.29-3)
- 「システム メッセージ ロギングのデフォルト設定」(P.29-4)
- 「メッセージ ロギングのディセーブル化」(P.29-4)(任意)
- •「メッセージ表示宛先デバイスの設定」(P.29-5)(任意)
- 「ログメッセージの同期化」(P.29-6)(任意)
- 「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」(P.29-8)(任意)
- 「ログメッセージのシーケンス番号のイネーブル化およびディセーブル化」(P.29-8)(任意)
- •「メッセージ重大度の定義」(P.29-9)(任意)
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」(P.29-11)(任意)
- 「設定変更ロガーのイネーブル化」(P.29-11)(任意)
- 「UNIX Syslog サーバの設定」(P.29-13)(任意)

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字とパーセント記号(%)、およびその前に配置されるオプションのシーケンス番号やタイム スタンプ情報(設定されている場合)で構成されています。メッセージは、次のフォーマットで表示されます。

seq no:timestamp: %facility-severity-MNEMONIC:description

パーセント記号の前のメッセージ部分は、service sequence-numbers、service timestamps log datetime、service timestamps log datetime [localtime] [msec] [show-timezone]、または service timestamps log uptime グローバル コンフィギュレーション コマンドの設定によって変わります。

表 29-1 に、Syslog メッセージの要素を示します。

表 29-1 システム ログ メッセージの要素

要素	説明	
seq no:	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合 だけ、ログ メッセージにシーケンス番号をスタンプします。	
	詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」 (P.29-8)を参照してください。	
timestamp のフォーマット:	メッセージまたはイベントの日時です。service timestamps log [datetime log] グローバル コン フィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。	
mm/dd hh:mm:ss	詳細については、「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」	
または	(P.29-8)を参照してください。	
<i>hh:mm:ss</i> (短時間)		
または		
<i>d</i> h (長時間)		
facility	メッセージが参照するファシリティ(SNMP、SYS など)です。サポートされるファシリティの 一覧については、表 29-4 (P.29-14)を参照してください。	
severity	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。重大度の詳細については、表 29-3 (P.29-10)を参照してください。	
MNEMONIC	メッセージを一意に示すテキスト ストリングです。	
description	レポートされているイベントの詳細を示すテキスト ストリングです。	

次に、スイッチ システム メッセージの一部を示します。

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up 00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up 00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up 00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down 00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down 2 *Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) 18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) *Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG I: Configured from console by vty2 (10.34.195.36)

システム メッセージ ロギングのデフォルト設定

表 29-2 に、システム メッセージ ロギングのデフォルト設定を示します。

表 29-2 システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	debugging (および数値的により低いレベル。 表 29-3 (P.29-10) を参照)
ログ ファイル設定	ファイル名の指定なし
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1メッセージ
タイム スタンプ	ディセーブル
同期ロギング	ディセーブル
ログ サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
設定変更ロガー	ディセーブル
サーバ ファシリティ	Local7 (表 29-4 (P.29-14) を参照)
サーバの重大度	informational (および数値的により低いレベル。 表 29-3 (P.29-10) を参照)

メッセージ ロギングのディセーブル化

メッセージ ロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛 先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。メッ セージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

メッセージ ロギングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no logging console	メッセージ ロギングをディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
	または	
	show logging	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ロギング プロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは 処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギング プロ セスがディセーブルの場合、メッセージは生成後すぐに(通常はコマンド出力に割り込む形で)コン ソールに表示されます。 **logging synchronous** グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。詳細については、「ログメッセージの同期化」(P.29-6)を参照してください。

メッセージ ロギングをディセーブルにしたあとに再びイネーブルにするには、logging on グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先デバイスの設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信で きます。メッセージの受信場所を指定するには、特権 EXEC モードで次のコマンドを1つまたは複数 使用します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging buffered [size]	スイッチの内部バッファにメッセージをロギングします。指定できる 範囲は 4096 ~ 2147483647 バイトです。デフォルトのバッファ サイ ズは 4096 バイトです。
		スイッチに障害が発生すると、フラッシュ メモリに保存していなけ れば、ログ ファイルは失われます。ステップ4を参照してください。
		 バッファサイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサメモリを表示するには、show memory 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファサイズをこの値に設定しないでください。
ステップ 3	logging host	UNIX Syslog サーバ ホストにメッセージを記録します。
		<i>host</i> には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。
		ログ メッセージを受信する Syslog サーバのリストを作成するには、 このコマンドを複数回入力します。
		Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」 (P.29-13) を参照してください。

	コマンド	目的
ステップ 4	logging file flash:filename [max-file-size [min-file-size]] [severity-level-number type]	フラッシュ メモリ内のファイルにログ メッセージを保存します。
		• filename には、ログ メッセージのファイル名を入力します。
		 (任意) max-file-size には、ログファイルの最大サイズを指定します。指定できる範囲は 4096 ~ 2147483647 です。デフォルトは 4096 バイトです。
		 (任意) min-file-size には、ログファイルの最小サイズを指定します。指定できる範囲は 1024 ~ 2147483647 です。デフォルトは 2048 バイトです。
		 (任意) severity-level-number type には、ロギングの重大度また はロギングタイプを指定します。重大度に指定できる範囲は0~ 7です。ロギングタイプキーワードの一覧については、表 29-3 (P.29-10) を参照してください。デフォルトでは、デバッグメッ セージ、および数値的により低いレベルのメッセージがログファ イルに送信されます。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	terminal monitor	現在のセッション中に、コンソール以外の端末にメッセージを記録します。
		端末パラメータ設定コマンドはローカルに設定され、セッションの終 了後は無効になります。デバッグメッセージを表示する場合は、 セッションごとにこのステップを実行する必要があります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ログ メッセージが内部 バッファにコピーされます。循環バッファなので、バッファが一杯になると、古いメッセージが新しい メッセージで置き換えられます。バッファに記録されたメッセージを表示するには、show logging 特 権 EXEC コマンドを使用します。バッファ内の最も古いメッセージが最初に表示されます。バッファ の内容をクリアするには、clear logging 特権 EXEC コマンドを使用します。

特定の PoE に対応したポートで Power over Ethernet (PoE) イベントのロギングをイネーブルにした りディセーブルにしたりするには、logging event power-inline-status インターフェイス コンフィギュ レーション コマンドを使用します。これらのポートへのロギングは、デフォルトでイネーブルです。

コンソールへのロギングをディセーブルにするには、no logging console グローバル コンフィギュレー ション コマンドを使用します。ファイルへのロギングをディセーブルにするには、no logging file [severity-level-number | type] グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージの同期化

特定のコンソール ポート回線または仮想端末回線に対して、非送信請求メッセージおよび debug 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重 大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージ が削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび debug コマンド出力の同期ロギングがイネーブルの場合、送信請求デバ イス出力がコンソールに表示または印刷されたあとに、非送信請求デバイスからの出力が表示または印 刷されます。非送信請求メッセージおよび debug コマンドの出力は、ユーザ入力用プロンプトが返さ れたあとに、コンソールに表示されます。したがって、非送信請求メッセージおよび debug コマンド の出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッ セージが表示されたあとに、コンソールはユーザ プロンプトを再表示します。

同期ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的	
configure terminal	グローバル コンフィギュレーション モードを開始します。	
line [console vty] line-number [ending-line-number]	メッセージの同期ロギングを行うように、回線を設定します。	
	 スイッチのコンソール ポートを介して行われる設定には、 console キーワードを使用します。 	
	 同期ロギングをイネーブルにする vty 回線を指定するには、 line vty <i>line-number</i> コマンドを使用します。Telnet セッショ ンを介して行われる設定には、vty 接続を使用します。回線 番号に指定できる範囲は 0 ~ 15 です。 	
	16 個の vty 回線の設定をすべて一度に変更するには、次のように 入力します。	
	line vty 0 15	
	また、現在の接続に使用されている 1 つの vty 回線の設定を変更 することもできます。たとえば、vty 回線 2 の設定を変更するに は、次のように入力します。	
	line vty 2	
	このコマンドを入力すると、ライン コンフィギュレーション モードになります。	
logging synchronous [level [severity-level all] limit number-of-buffers]	メッセージの同期ロギングをイネーブルにします。	
	• (任意) level severity-level には、メッセージの重大度を指定 します。重大度がこの値以上であるメッセージは、非同期に 出力されます。値が小さいほど重大度は大きく、値が大きい ほど重大度は小さくなります。デフォルトは2です。	
	 (任意) level all を指定すると、重大度に関係なく、すべての メッセージが非同期に出力されます。 	
	 (任意) limit number-of-buffers には、キューイングされる端 末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ~ 2147483647 で す。デフォルトは 20 です。 	
end	特権 EXEC モードに戻ります。	
show running-config	設定を確認します。	
copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。	
	コマンド configure terminal line [console vty] line-number [ending-line-number] logging synchronous [level [severity-level all] limit number-of-buffers] end show running-config copy running-config startup-config	

非送信請求メッセージおよびデバッグ出力の同期をディセーブルにするには、no logging synchronous [level severity-level | all] [limit number-of-buffers] ライン コンフィギュレーション コマンドを使用しま す。

ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化

デフォルトでは、ログ メッセージにはタイム スタンプが適用されません。

ログ メッセージのタイム スタンプをイネーブルにするには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始しま
	す。
service timestamps log uptime	ログのタイム スタンプをイネーブルにします。
または	最初のコマンドを実行するとログ メッセージのタイム ス
service timestamps log datetime [msec] [localtime] [show-timezone]	タンプがイネーブルになり、システムを再起動したあと の経過時間が表示されます。
	2番めのコマンドを実行すると、ログメッセージのタイ
	ムスタンブがイネーブルになります。選択したオブショ
	「シに応して、ローカル タイム ノーンを基準とした日刊、 時間(ミリ秒) タイム ゾーン名をタイム スタンプとし
	て表示できます。
end	特権 EXEC モードに戻ります。
show running-config	設定を確認します。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存し
	ます。

デバッグ メッセージとログ メッセージの両方のタイム スタンプをディセーブルにするには、no service timestamps グローバル コンフィギュレーション コマンドを使用します。

次に、service timestamps log datetime グローバル コンフィギュレーション コマンドをイネーブルに した場合のログ表示の一部を示します。

*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

次に、service timestamps log uptime グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージのタイム スタンプが同じになることがあるため、1 つのメッセージを正確に識 別できるように、メッセージにシーケンス番号を表示できます。デフォルトでは、ログ メッセージに シーケンス番号は表示されません。

ログメッセージのシーケンス番号をイネーブルにするには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
ステップ 2	service sequence-numbers	シーケンス番号をイネーブルにします。

	コマンド	目的		
ステップ 3	end	特権 EXEC モードに戻ります。		
ステップ 4	show running-config	設定を確認します。		
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存		
		します。		

シーケンス番号をディセーブルにするには、no service sequence-numbers グローバル コンフィギュ レーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します (表 29-3を参照)。

メッセージの重大度を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	 目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	logging console level	コンソールに記録されるメッセージを制限します。		
		デフォルトで、コンソールはデバッグ メッセージ、および数値的に より低いレベルのメッセージを受信します(表 29-3 (P.29-10)を参 照)。		
ステップ 3	logging monitor level	端末回線に記録されるメッセージを制限します。		
		デフォルトで、端末はデバッグメッセージ、および数値的により低 いレベルのメッセージを受信します(表 29-3 (P.29-10)を参照)。		
ステップ 4	logging trap level	Syslog サーバに記録されるメッセージを制限します。		
		デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します(表 29-3 (P.29-10)を参照)。		
		Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」 (P.29-13) を参照してください。		
ステップ 5	end	特権 EXEC モードに戻ります。		
ステップ 6	show running-config	設定を確認します。		
	または			
	show logging			
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。		

(注)

*level*を指定すると、このレベルのメッセージ、および数値的により低いレベルのメッセージが宛先に表示されます。

コンソールへのロギングをディセーブルにするには、no logging console グローバル コンフィギュレー ション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、no logging monitor グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギ ングをディセーブルにするには、no logging trap グローバル コンフィギュレーション コマンドを使用 します。

表 29-3 に *level* キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 29-3 メッセージ ロギング level キーワード

level キーワード	レベル	説明	Syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	ただちに対処が必要な状態	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー	LOG_ERR
warnings	4	警告	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	通知メッセージ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の4つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラーメッセージ:warnings ~ emergencies の重大度で表示されます。このタイプのメッセージは、スイッチの機能に影響があることを示しま す。この誤動作からの回復手順については、このリリースに対応するシステムメッセージガイド を参照してください。
- **debug** コマンドの出力: **debugging** の重大度で表示されます。通常、デバッグ コマンドは Technical Assistance Center (TAC) でのみ使用されます。
- インターフェイスのアップまたはダウントランジションメッセージおよびシステム再起動メッセージ: notifications の重大度で表示されます。このメッセージは単なる情報であり、スイッチの機能には影響がありません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

snmp-server enable trap グローバル コンフィギュレーション コマンドを使用して、SNMP Network Management Station (NMS; ネットワーク管理ステーション) に送信されるように Syslog メッセージ トラップがイネーブルに設定されている場合は、スイッチの履歴テーブルに送信および格納されるメッ セージの重大度を変更できます。また、履歴テーブルに格納されるメッセージの数を変更することもで きます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。 デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が warnings のメッセージ、およ び数値的により低いメッセージ(表 29-3 (P.29-10)を参照)が、履歴テーブルに1つ格納されます。

重大度および履歴テーブル サイズのデフォルト値を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	logging history level ¹	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。		
		<i>level</i> キーワードのリストについては、表 29-3 (P.29-10) を参照して ください。		
		デフォルトでは、warnings、errors、critical、alerts、および emergencies のメッセージが送信されます。		
ステップ 3	logging history size number	履歴テーブルに格納できる Syslog メッセージ数を指定します。		
		デフォルトでは1つのメッセージが格納されます。指定できる範囲は 0~500です。		
ステップ 4	end	特権 EXEC モードに戻ります。		
ステップ 5	show running-config	設定を確認します。		
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。		

1. 表 29-3 に、level キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、 *emergencies* は 0 ではなく 1 に、*critical* は 2 ではなく 3 になります。

> 履歴テーブルがいっぱいの場合(logging history size グローバル コンフィギュレーション コマンドで 指定した最大メッセージ エントリ数が格納されている場合)は、新しいメッセージ エントリを格納で きるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのロギングをデフォルトの重大度に戻すには、no logging history グローバル コン フィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すに は、no logging history size グローバル コンフィギュレーション コマンドを使用します。

設定変更ロガーのイネーブル化

CLI (コマンドライン インターフェイス) で行った設定変更をトラッキングするために設定ロガーをイ ネーブルにすることができます。logging enable 設定変更ロガー コンフィギュレーション コマンドを 入力すると、設定変更用に入力されたセッション、ユーザおよびコマンドがログに記録されます。設定 ログのサイズは1~1000 エントリの間で設定することができます (デフォルトは 100)。no logging enable コマンドの後に logging enable コマンドを入力してロギングをディセーブルにして再びイネー ブルにすることで、いつでもログをクリアすることができます。 **show archive log config** {**all** | *number* [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**] 特権 EXEC コマンドを使用して、設定ログ全体または指定したパラメータのログを表示します。

デフォルトで設定ロギングはディセーブルになっています。

コマンドの詳細については、次の URL にある『Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter0918 6a00801a8086.html#wp1114989

設定ロギングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	archive	アーカイブコンフィギュレーション モードを開始します。		
ステップ 3	log config	設定変更ロガー コンフィギュレーション モードを開始します。		
ステップ 4	logging enable	設定変更ロギングをイネーブルにします。		
ステップ 5	logging size entries	(任意) 設定ログで取得するエントリ数を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 100 です。		
		(注) 設定ログがいっぱいになると、新規エントリが入力されるたびに最も古いログ エントリが削除されます。		
ステップ 6	end	特権 EXEC モードに戻ります。		
ステップ 7	show archive log config	設定ログを表示することでエントリを確認します。		

次に、設定変更ロガーをイネーブルにして、ログのエントリ数を 500 に設定する例を示します。

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

設定ログの出力例は次のとおりです。

show	archive log config	all
sess	user@line	Logged command
11	unknown user@vty3	no aaa authorization config-commands
12	unknown user@vty3	no aaa authorization network default group radius
12	unknown user@vty3	<pre>Ino aaa accounting dot1x default start-stop group</pre>
13	unknown user@vty3	no aaa accounting system default
14	temi@vty4	interface GigabitEthernet4/0/1
14	temi@vty4	switchport mode trunk
14	temi@vty4	exit
16	temi@vty5	interface FastEthernet5/0/1
16	temi@vty5	switchport mode trunk
16	temi@vty5	exit
	sess 11 12 12 13 14 14 14 16 16 16	show archive log config sess user@line 11 unknown user@vty3 12 unknown user@vty3 12 unknown user@vty3 13 unknown user@vty3 14 temi@vty4 14 temi@vty4 14 temi@vty4 16 temi@vty5 16 temi@vty5

UNIX Syslog サーバの設定

次に、UNIX サーバの Syslog デーモンを設定し、UNIX システム ロギング ファシリティを定義する手順について説明します。

UNIX Syslog デーモンへのログ メッセージ

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモン を設定する必要があります。この手順は任意です。

root としてログインし、次のステップを実行します。

(注)

最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケット を受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモート ロギン グをイネーブルにするには、Syslog コマンド ラインに追加または削除する必要があるオプションを、 UNIX の man syslogd コマンドを使用して判別します。

ステップ1 /etc/syslog.conf ファイルに次のような行を1行追加します。

local7.debug /usr/adm/logs/*cisco.log*

local7キーワードは、使用するロギングファシリティを指定します。ファシリティの詳細については、 表 29-4 (P.29-14)を参照してください。**debug**キーワードは、Syslogの重大度を指定します。重大度 の詳細については、表 29-3 (P.29-10)を参照してください。Syslog デーモンは、これ以上の重大度の 場合に、次のフィールドで指定されたファイルにメッセージを送信します。このファイルは、Syslog デーモンに書き込み権限がある既存ファイルでなければなりません。

ステップ 2 UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

\$ touch /var/log/cisco.log
\$ chmod 666 /var/log/cisco.log

ステップ3 Syslog デーモンに新しい設定を認識させます。

\$ kill -HUP `cat /etc/syslog.pid`

詳細については、ご使用の UNIX システムの man syslog.conf および man syslogd コマンドを参照し てください。

UNIX システム ロギング ファシリティの設定

システム ログ メッセージを外部デバイスに送信する場合は、メッセージを UNIX Syslog ファシリティ から送信されたメッセージとして特定するようにシステムを設定できます。

UNIX システム ファシリティ メッセージ ロギングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	logging host	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを 記録します。		
		ログ メッセージを受信する Syslog サーバのリストを作成するには、 このコマンドを複数回入力します。		
ステップ 3	logging trap level	Syslog サーバに記録されるメッセージを制限します。		
		デフォルトでは、Syslog サーバは通知メッセージおよびそれ以下の メッセージを受信します。 <i>level</i> キーワードについては、表 29-3 (P.29-10)を参照してください。		
ステップ 4	logging facility facility-type	Syslog ファシリティを設定します。 <i>facility-type</i> キーワードについて は、表 29-4 (P.29-14) を参照してください。		
		デフォルトはlocal7です。		
ステップ 5	end	特権 EXEC モードに戻ります。		
ステップ 6	show running-config	設定を確認します。		
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。		

Syslog サーバを削除するには、no logging host グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのロギングをディセーブルにするには、no logging trap グローバル コンフィギュレーション コマンドを入力します。

表 29-4 に、ソフトウェアでサポートされている UNIX システム ファシリティを示します。これらの ファシリティの詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照 してください。

表	29-4	ロギング	facility-type	キーワー	۴
---	------	------	---------------	------	---

facility-type キーワード	説明
auth	許可システム
cron	cron ファシリティ
daemon	システム デーモン
kern	カーネル
local0 \sim local7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9 ~ sys14	システムで使用
syslog	システム ログ
facility-type キーワード	説明
---------------------	-------------------------
user	ユーザ プロセス
uucp	UNIX から UNIX へのコピー システム

表 29-4 ロギング facility-type キーワード (続き)

ロギング設定の表示

ロギング設定およびログ バッファの内容を表示するには、show logging 特権 EXEC コマンドを使用し ます。この表示のフィールドに関する詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release* 12.2』を参照してください。これには、Cisco.com のホームページ (Documentation > Cisco IOS Software > 12.2 Mainline> Command References) からアクセス可能 です。 ■ ロギング設定の表示



CHAPTER 30

SNMP の設定

この章では、Catalyst 2960 スイッチに Simple Network Management Protocol (SNMP; 簡易ネット ワーク管理プロトコル)を設定する方法について説明します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS Network Management Command Reference, Release 12.4*』を参照して ください。これには、Cisco.com の次の URL からアクセス可能です。 http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

- 「SNMP の概要」(P.30-1)
- 「SNMP の設定」(P.30-6)
- 「SNMP ステータスの表示」(P.30-20)

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージフォーマットを提供するアプリケーショ ンレイヤ プロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB (管理情報ベース)で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System (NMS; ネットワーク管理システム)に統合できます。エージェントおよび MIB は、スイッチ に常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できま す。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エー ジェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。 エージェントはマネージャからのデータ取得要求または設定要求に応答します。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある 状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス (アップまたはダウン)、MAC (メディア アクセス制御) アドレス追跡、TCP 接続の終了、 ネイバとの接続の切断などの重要なイベントの発生を意味する場合があります。

ここでは、次の概要について説明します。

- 「SNMP バージョン」 (P.30-2)
- 「SNMP マネージャ機能」(P.30-3)
- 「SNMP エージェント機能」(P.30-4)
- 「SNMP コミュニティ ストリング」(P.30-4)
- 「SNMP を使用して MIB 変数にアクセスする方法」(P.30-5)

- 「SNMP 通知」(P.30-5)
- 「SNMP ifIndex MIB オブジェクト値」(P.30-6)

SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1: RFC1157 に定められた SNMP (完全インターネット標準)
- SNMPv2Cは、SNMPv2Classicのバルク検索機能を残し、エラー処理を改善したうえで、 SNMPv2Classicのパーティベースの管理およびセキュリティフレームワークをコミュニティストリングベースの管理フレームワークに置き換えたものです。次の機能があります。
 - SNMPv2: RFC 1902 ~ 1907 に定められた SNMP バージョン 2 (ドラフト版インターネット 標準)
 - SNMPv2C: RFC 1901 に定められた SNMPv2 のコミュニティ ストリング ベースの管理フレームワーク(試験版インターネットプロトコル)
- SNMPv3: SNMPのバージョン3は、RFC 2273~2275に規定されている相互運用可能な標準 ベースプロトコルです。SNMPv3は、ネットワーク上のパケットを認証、暗号化することでデバ イスへのアクセスに対するセキュリティを提供します。SNMPv3は、次のセキュリティ機能を備 えています。
 - メッセージの完全性:パケットが伝送中に改ざんされないようにします。
 - 認証:メッセージの送信元が有効かどうかを判別します。
 - ・ 暗号化:パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを
 防止します。



(注) 暗号化を選択するには、priv キーワードを入力します。このキーワードは、暗号化ソ フトウェア イメージがインストールされている場合のみ使用可能です。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス Access Control List (ACL; アクセス コントロール リスト) およびパスワードによって定義されます。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラー コードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。 SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 は、セキュリティモデルとセキュリティレベルの両方を提供します。セキュリティモデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティレベルは、セキュリティモデル内で許可されたセキュリティのレベルです。セキュリティレベルとセキュリティモデルの組み合わせにより、SNMPパケットを扱うときに使用するセキュリティメカニズムが決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

表 30-1 に、セキュリティモデルとセキュリティレベルのさまざまな組み合わせについて、その特性を示します。

表 30-1 SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ	なし	コミュニティ ストリングの照合を使用して認証します。
		ストリング		
SNMPv2C	noAuthNoPriv	コミュニティ	なし	コミュニティ ストリングの照合を使用して認証します。
		ストリング		
SNMPv3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づ
		(MD5) または		いて認証します。
		Secure Hash		
_		Algorithm (SHA)		
SNMPv3	authPriv	MD5 または SHA	Data Encryption	HMAC-MD5 または HMAC-SHA アルゴリズムに基づ
	(暗号化		Standard (DES;	いて認証します。次の暗号化アルゴリズムで、
	ソフトウェア		データ暗号化規	User-based Security Model (USM) を指定できます。
	イメージが		格)または	 CBC-DES(DES-56)規格に基づく認証に加えた
	必要)		Advanced	DES 56 ビット暗号化
			Encryption	
		Standard (AES;	• JDED 108 ビット喧方化	
			局度暗号化規格)	• AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設 定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、 および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 30-2 に示す動作を実行します。

表 30-2 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。1
get-bulk-request ²	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要が ある巨大なデータ ブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッ セージです。

1. この動作では、SNMPマネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。

2. get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得: SNMP エージェントは NMS からの要求に応答して、この機能を開始します。 エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定: SNMP エージェントは NMS からのメッセージに応答して、この機能を開始し ます。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送 信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップ またはダウン状態になった場合、スパニング ツリー トポロジが変更された場合、認証に失敗した場合 などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ ストリング定義が、スイッチ上の3つのコミュニティ ストリング定義の少なくとも1つと一致していなければなりません。

コミュニティストリングのアトリビュートは、次の3つのいずれかです。

- Read-Only (RO):許可された管理ステーションに、コミュニティストリングを除く MIB 内のす べてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write (RW):許可された管理ステーションに、MIB内のすべてのオブジェクトへの読み書 きアクセスを許可しますが、コミュニティストリングに対するアクセスは許可しません。
- クラスタを作成すると、コマンドスイッチがメンバースイッチと SNMP アプリケーション間の メッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に 設定された RW および RO コミュニティ ストリングにメンバー スイッチ番号 (@esN、N はスイッ チ番号)を追加し、これらのストリングをメンバー スイッチに伝播します。詳細は、第5章「ス イッチのクラスタ化」および Cisco.com から入手できる『Getting Started with Cisco Network Assistant』を参照してください。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフト ウェアは、スイッチの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポー リングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析 して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマン スの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 30-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ(特定イベントの通知)を送信でき、SNMP マネージャはトラップを受 信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ス テータス(アップまたはダウン)、MAC アドレス トラッキングなどの状況を SNMP マネージャに通知 します。SNMP エージェントはさらに、SNMP マネージャから get-request、get-next-request、および set-request 形式で送信される MIB 関連のクエリーに応答します。





サポート対象の MIB の詳細、およびアクセス手順については、付録 A「サポート対象 MIB」を参照してください。

SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送 信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、ト ラップまたは情報を選択するオプションがコマンドにないかぎり、キーワード *traps* はトラップ、情 報、またはその両方を表します。snmp-server host コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。



SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが 受信されたかどうかが送信側にわからないからです。通知要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット)でメッセージを確認します。送信 側が応答を受信しなかった場合は、再び通知要求を送信できます。再送信できるので、通知の方がト ラップより意図した宛先に届く可能性が高くなります。

通知の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費すると いう特性にも理由があります。送信と同時に廃棄されるトラップと異なり、通知要求は応答を受信する まで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は1回限りで すが、情報は数回にわたって再送信すなわち再試行が可能です。再試行によってトラフィックが増え、 ネットワークのオーバーヘッドが大きくなります。したがって、トラップにするか通知にするかは、信 頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信する ことが重要な場合は、通知要求を使用してください。ネットワークまたはスイッチ メモリ上のトラ フィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい 一意の値である interface index (ifIndex) オブジェクト値の生成および割り当てを行います。スイッチ の再起動またはスイッチのソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれ と同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられてい ると、スイッチの再起動後も同じ値が使用されます。

スイッチは、表 30-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

インターフェイス タイプ	ifIndex 範囲
SVI ¹	$1 \sim 4999$
EtherChannel	$5000 \sim 5012$
ループバック	$5013 \sim 5077$
トンネル	$5078 \sim 5142$
物理(ギガビット イーサネットまたは SFP ² モジュール インター フェイス)	$10000 \sim 14500$
<u></u> ヌル	14501

表 30-3 ifIndex 値

- 1. SVI = Switch Virtual Interface
- 2. SFP = Small Form-Factor Pluggable

(注)

スイッチは、範囲内の連続した値を使用しない場合があります。

SNMP の設定

- 「SNMP のデフォルト設定」(P.30-7)
- 「SNMP 設定時の注意事項」(P.30-7)
- 「SNMP エージェントのディセーブル化」(P.30-8)
- 「コミュニティストリングの設定」(P.30-9)
- 「SNMP グループおよびユーザの設定」(P.30-10)
- 「SNMP 通知の設定」(P.30-13)
- 「CPU しきい値通知のタイプと値の設定」(P.30-17)
- 「エージェント コンタクトおよびロケーションの設定」(P.30-17)
- 「SNMP を通して使用する TFTP サーバの制限」(P.30-18)
- 「SNMP の例」 (P.30-19)

SNMP のデフォルト設定

表 30-4 に、SNMP のデフォルト設定を示します。

表 30-4 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル1
SNMP トラップ レシーバー	未設定
SNMP トラップ	TCP 接続のトラップ(tty)以外は、イネーブルではありません。
SNMP バージョン	version キーワードがない場合、デフォルトはバージョン l になりま す。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルト で noauth (noAuthNoPriv) になります。
SNMP 通知タイプ	タイプを指定しなかった場合、すべての通知が送信されます。

1. これは、スイッチが起動し、スタートアップ コンフィギュレーションに snmp-server グローバル コンフィギュ レーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも1つの snmp-server グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェン トはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、 SNMP グループのメンバーです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジ ンID は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。snmp-server host グローバル コ ンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザを対応するグ ループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべて のユーザが影響を受けます。通知ビューの設定が必要な状況については、『Cisco IOS Network Management Command Reference』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに 対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、snmp-server engineID グローバル コン フィギュレーション コマンドを remote オプションとともに使用して、SNMP エンジン ID を設定 してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードを使用して 認証およびプライバシ ダイジェストが算出されます。先にリモート エンジン ID を設定しておかな いと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモートエージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカルユーザとリモートホストに関連がない場合、スイッチは、auth (authNoPriv)および priv (authPriv)認証レベルの通知を送信しません。

 SNMP エンジン ID の値を変更すると、重大な影響が生じます。(コマンド ラインで入力された) ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セ キュリティ ダイジェストに変換されます。コマンド ラインのパスワードは、RFC 2274 の規定に 従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、snmp-server user username グロー バル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要がでてきます。 エンジン ID を変更した場合は、同様の制限によってコミュニティ ストリングも再設定する必要が あります。

SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no snmp-server	SNMP エージェントの動作をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

no snmp-server グローバル コンフィギュレーション コマンドを使用すると、デバイス上で稼動してい るすべてのバージョン (バージョン 1、バージョン 2C、バージョン 3) がディセーブルになります。 SNMP をイネーブルにする特定の Cisco IOS コマンドは存在しません。最初に入力する snmp-server グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルに なります。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用しま す。コミュニティ ストリングは、スイッチ上のエージェントへのアクセスを許可するパスワードと同 様に機能します。ストリングに対応する次の特性を1つまたは複数指定することもできます。

- コミュニティストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティ ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server community <i>string</i> [view <i>view-name</i>] [ro rw] [<i>access-list-number</i>]	コミュニティ ストリングを設定します。
		(注) @ 記号は、コンテキスト情報を区切る場合に使用されます。こ のコマンドを設定するとき、@ 記号を SNMP コミュニティス トリングの一部として使用しないでください。
		 string には、パスワードと同様に機能し、SNMP プロトコルへの アクセスを許可するストリングを指定します。任意の長さのコ ミュニティ ストリングを1つまたは複数設定できます。
		 (任意) view には、コミュニティがアクセスできるビュー レコー ドを指定します。
		 (任意)許可された管理ステーションで MIB オブジェクトを取得 する場合は読み取り専用 (ro)、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き (rw)を 指定します。デフォルトでは、コミュニティ ストリングはすべて のオブジェクトに対する読み取り専用アクセスを許可します。
		 (任意) access-list-number には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	access-list access-list-number {deny permit} source [source-wildcard]	(任意) ステップ 2 で標準 IP アクセス リスト番号を指定してリストを 作成した場合は、必要に応じてコマンドを繰り返します。
		 access-list-number には、ステップ2で指定したアクセスリスト番号を入力します。
		 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。
		 sourceには、コミュニティストリングを使用してエージェントに アクセスできる SNMP マネージャの IP アドレスを入力します。
		 (任意) source-wildcard には、source に適用されるワイルドカー ドビットをドット付き 10 進表記で入力します。無視するビット位 置には1を入れます。
		アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメン トが常に存在することに注意してください。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

(注)

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリ ングをヌル ストリングに設定します (コミュニティ ストリングに値を入力しないでください)。

特定のコミュニティ ストリングを削除するには、no snmp-server community string グローバル コン フィギュレーション コマンドを使用します。

次に、ストリング comaccess を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト4 がこのコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスできるよう に指定する例を示します。

Switch(config) # snmp-server community comaccess ro 4

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名 (エンジン ID) を指定できま す。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバ グループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上で SNMP を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID { local <i>engineid-string</i> remote <i>ip-address</i> [udp-port <i>port-number</i>] <i>engineid-string</i> }	 SNMP のローカル コピーまたはリモート コピーの名前を設定します。 engineid-string は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。たとえば、1234000000000000000000000000000000000000
		• remote を相定した場合、SNMP のリモートコピーが置か れているデバイスの <i>ip-address</i> を指定し、任意でリモート デバイスの UDP ポートを指定します。デフォルト値は 162 です。

	コマンド	目的
ステップ 3	<pre>snmp-server group groupname {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list]</pre>	リモート デバイスに新規 SNMP グループを設定します。
		• groupname には、グループを指定します。
		 セキュリティモデルを指定します。
		- v1 は、最も安全性の低いセキュリティ モデルです。
		 v2cは、2番めに安全性の低いセキュリティモデルです。標準の2倍の幅で情報および整数を伝送できます。
		 最も安全な v3 の場合、認証レベルを選択する必要があります。
		auth :MD5 および SHA によるパケット認証が可能で す。
		noauth : noAuthNoPriv というセキュリティ レベルを イネーブルにします。キーワードを指定しなかった場 合、これがデフォルトです。
		priv :DES によるパケット暗号化をイネーブルにしま す(<i>privacy</i> とも呼ばれます)。
		(注) priv キーワードは、暗号化ソフトウェア イメージがイ ンストールされている場合のみ使用可能です。
		 (任意) read readview とともに、エージェントの内容を表示できるビューの名前を表すストリング(64 文字以下)を入力します。
		 (任意) write writeview とともに、データを入力し、エージェントの内容を表示できるビューの名前を表すストリング(64 文字以下)を入力します。
		 (任意) notify notifyview とともに、通知、情報、またはト ラップを指定するビューの名前を表すストリング(64 文字 以下)を入力します。
		 (任意) access access-list とともに、アクセス リスト名の ストリング(64 文字以下)を入力します。

	コマンド	目的
ステップ 4	<pre>snmp-server user username groupname {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]} [priv {des 3des aes {128 192 256}} priv-password]</pre>	 SNMP グループに対して新規ユーザを追加します。 username は、エージェントに接続するホスト上のユーザ名です。 groupname は、ユーザが対応付けられるグループの名前です。 remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルト値は 162 です。
		 SNMP バージョン番号(v1、v2c、または v3)を入力します。v3 を入力する場合は、次のオプションを追加します。
		 encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードが指定されている場合のみ使用可能です。
		 auth は認証レベル設定セッションで、 HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。パスワード ストリ ング auth-password (64 文字以下) が必要です。
		 v3 を入力してスイッチが暗号化ソフトウェアイメージを実行中の場合は、プライベート(priv)暗号化およびパス ワードストリング priv-password (64 文字以下)の設定も できます。
		- priv は、User-based Security Model (USM) を指定します。
		 des は、56 ビット DES アルゴリズムの使用を指定します。
		 - 3des は、168 ビット DES アルゴリズムの使用を指定します。
		 aesは、DESアルゴリズムの使用を指定します。128 ビット暗号化、192ビット暗号化、または256ビット 暗号化のいずれかを選択する必要があります。
		 (任意) access access-list とともに、アクセス リスト名の ストリング(64 文字以下)を入力します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
		(注) auth noauth priv モード設定に関する SNMPv3 情報 を表示するには、show snmp user 特権 EXEC コマンド を入力する必要があります。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP 通知の設定

トラップマネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイ ベントが発生したときにスイッチが生成するシステムアラートです。デフォルトでは、トラップマ ネージャは定義されず、トラップは送信されません。この Cisco IOS リリースが稼動しているスイッチ では、トラップマネージャを無制限に設定できます。

(注)

コマンド構文で *traps* というワードを使用するコマンドは多数あります。トラップまたは情報を選択す るオプションがコマンドにないかぎり、キーワード **traps** はトラップ、情報のいずれか、またはその両 方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップ または情報として SNMP 通知を送信するかどうかを指定します。

表 30-5 に、サポートされているスイッチ トラップ(通知タイプ)を示します。これらのトラップの一 部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。 SNMP 情報通知の送信をイネーブルにするには、snmp-server enable traps グローバル コンフィギュ レーション コマンドと snmp-server host *host-addr* informs グローバル コンフィギュレーション コマ ンドを組み合わせて使用します。

表 30-5 スイッチの通知タイプ

通知タイプの キーワード	 説明	
bridge	Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) ブリッジ MIB トラップを生成します。	
cluster	クラスタ設定が変更された場合に、トラップを生成します。	
config	SNMP 設定が変更された場合に、トラップを生成します。	
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。	
entity	SNMP エンティティが変更された場合に、トラップを生成します。	
cpu threshold	CPU に関連したトラップをイネーブルにします。このトラップを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。	
envmon	環境モニタ トラップを生成します。ファン (fan)、シャットダウン (shutdown)、ステータス (status)、 電源 (supply)、温度 (temperature) の環境トラップのいずれかまたはすべてをイネーブルにできます。	
errdisable	ポート VLAN が errdisable ステートになった場合に、トラップを生成します。1 分あたりの最大トラッ プ速度も設定できます。指定できる範囲は 0 ~ 10000 です。デフォルトは 0 で、レート制限がないとい う意味です。	
flash	SNMP FLASH 通知を生成します。	
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。	
mac-notification	MAC アドレス通知のトラップを生成します。	
msdp	Multicast Source Discovery Protocol (MSDP) が変更された場合に、トラップを生成します。	
ospf	Open Shortest Path First (OSPF) が変更された場合に、トラップを生成します。シスコ固有、エラー、 リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブ ルにできます。	
pim	Protocol-Independent Multicast (PIM) が変更された場合に、トラップを生成します。無効な PIM メッ セージ、ネイバ変更、および Rendezvous Point (RP; ランデブー ポイント) マッピングの変更に関する トラップを任意にイネーブルにできます。	

■ SNMP の設定

表 30-5 スイッチの通知タイプ (続き)

通知タイプの キーワード	 説明	
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。	
	(注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラッ プを設定して、次に以下のポート セキュリティ トラップ レートを設定します。	
	• snmp-server enable traps port-security	
	• snmp-server enable traps port-security trap-rate rate	
rtr	SNMP Response Time Reporter (RTR) のトラップを生成します。このトラップを使用できるのは、ス イッチで LAN Base イメージが実行されている場合だけです。	
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。	
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定で きる範囲は 0 ~ 1000 です。デフォルトは 0 に設定されています(制限なしの状態では、発生ごとにト ラップが送信されます)。	
stpx	SNMP STP 拡張 MIB トラップを生成します。	
syslog	SNMP の Syslog トラップを生成します。	
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。	
vlan-membershi	SNMP VLAN メンバシップが変更された場合に、トラップを生成します。	
р		
vlancreate	SNMP VLAN 作成トラップを生成します。	
vlandelete	SNMP VLAN 削除トラップを生成します。	
vtp	VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) が変更された場合に、トラップを生成します。	

(注)

insertion および removal キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サ ポートされていません。

表 30-5 に示す通知タイプを受信する場合は、特定のホストに対して snmp-server host グローバル コ ンフィギュレーション コマンドを実行します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID remote <i>ip-address engineid-string</i>	リモート ホスト用のエンジン ID を指定します。

	コマンド	目的
ステップ 3	snmp-server user usernamegroupname {remote host [udp-portport]} {v1 [access access-list] v2c[access access-list] v3 [encrypted][access access-list] [auth {md5 sha}auth-password]}	 ステップ2で設定したリモートホストと対応付ける SNMP ユーザを設定します。 (注) アドレスに対応するリモートユーザを設定するには、先にリモートホストのエンジン ID を設定しておく必要があります。このようにしないと、エラーメッセージが表示され、コマンドが実行されません。
ステップ 4	snmp-server group groupname {v1 v2c v3 {auth noauth priv}} [readreadview] [write writeview] [notifynotifyview] [access access-list]	SNMP グループを設定します。
ステップ 5	<pre>snmp-server host host-addr [informs traps] [version {1 2c 3 {auth noauth priv}}] community-string [notification-type]</pre>	 SNMP トラップ動作の受信側を指定します。 host-addr には、ホスト(対象となる受信側)の名前またはインターネットアドレスを指定します。 (任意)SNMP 情報をホストに送信するには、informs を指定します。 (任意)SNMP トラップをホストに送信するには、traps(デフォルト)を指定します。 (任意)SNMP version (1、2c、または3)を指定します。 SNMPv1は informs をサポートしていません。 (任意)バージョン3の場合、認証レベルとして auth、noauth、または priv を選択します。 (注) priv キーワードは、暗号化ソフトウェアイメージがインストールされている場合のみ使用可能です。 <i>community-string</i>には、version 1 または version 2c が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティストリングを入力します。version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。 (注) @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティストリングの一部として使用しないでください。 (任意) notification-type には、表 30-5 (P.30-13) に記載されているキーワードを使用します。タイプを指定しなかった場合、すべての通知が送信されます。

	コマンド	目的	
ステップ 6	snmp-server enable traps <i>notification-types</i>	スイッチがトラップまたは情報を送信できるようにし、送信する通知 のタイプを指定します。通知タイプの一覧については、表 30-5 (P.30-13)を参照するか、snmp-server enable traps?と入力してく ださい。	
		複数のトラップ タイプをイネーブルにするには、トラップ タイプご とに snmp-server enable traps コマンドを個別に入力する必要があ ります。	
		 (注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 	
		• snmp-server enable traps port-security	
		• snmp-server enable traps port-security trap-rate rate	
ステップ 7	snmp-server trap-source interface-id	(任意)送信元インターフェイスを指定します。そこからトラップ メッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。	
ステップ 8	snmp-server queue-length length	(任意) 各トラップ ホストのメッセージ キュー長を設定します。指定 できる範囲は 1 ~ 1000 です。デフォルトは 10 です。	
ステップ 9	snmp-server trap-timeout seconds	(任意) トラップ メッセージを再送信する間隔を設定します。指定で きる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。	
ステップ 10	end	特権 EXEC モードに戻ります。	
ステップ 11	show running-config	設定を確認します。	
		(注) auth noauth priv モード設定に関する SNMPv3 情報を表示 するには、show snmp user 特権 EXEC コマンドを入力する 必要があります。	
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

snmp-server host コマンドでは、通知を受信するホストを指定します。snmp-server enable trap コマ ンドによって、指定された通知メカニズム(トラップおよび情報)がグローバルでイネーブルになりま す。ホストが情報を受信できるようにするには、そのホストに対応する snmp-server host informs コ マンドを設定し、snmp-server enable traps コマンドを使用して情報をグローバルにイネーブルにす る必要があります。

指定したホストがトラップを受信しないようにするには、no snmp-server host host グローバル コン フィギュレーション コマンドを使用します。キーワードを指定しないで no snmp-server host コマン ドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりませ ん。情報をディセーブルにするには、no snmp-server host informs グローバル コンフィギュレーショ ン コマンドを使用してください。特定のトラップ タイプをディセーブルにするには、no snmp-server enable traps notification-types グローバル コンフィギュレーション コマンドを使用します。

CPU しきい値通知のタイプと値の設定

CPU しきい値通知のタイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	process cpu threshold type {total process interrupt} rising percentage interval seconds [falling fall-percentage interval seconds]	CPU しきい値通知のタイプと値を設定します。
		 total: 通知タイプを CPU 使用率の合計に設定します。
		• process:通知タイプを CPU プロセス使用率に設定します。
		• interrupt : 通知タイプを CPU 割り込み使用率に設定します。
		 rising percentage : CPU リソースのパーセント (1 ~ 100)。 設定された間隔を過ぎると CPU しきい値通知を送信します。
		 interval seconds : CPU しきい値超過の秒単位の持続時間(5 ~ 86400)。この条件が満たされると CPU しきい値通知を送 信します。
		 falling fall-percentage: CPU リソースのパーセント(1~ 100)。設定された間隔の間、使用率がこのレベルより低下す ると、CPU しきい値通知を送信します。
		この値は、 rising <i>percentage</i> の値以下である必要があります。 この値を指定しないと、 falling <i>fall-percentage</i> の値は rising <i>percentage</i> の値と同じになります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行し ます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server contact text	システム コンタクトを表すストリングを設定します。
		次に例を示します。
		snmp-server contact Dial System Operator at beeper 21555.
ステップ 3	snmp-server location text	システム ロケーションを表すストリングを設定します。
		次に例を示します。
		snmp-server location Building 3/Room 222
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SNMP を通して使用する TFTP サーバの制限

SNMP を通してコンフィギュレーション ファイルを保存およびロードするために使用する TFTP(簡易ファイル転送プロトコル)サーバを、アクセス リストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
snmp-server tftp-server-list access-list-number	SNMP を通してコンフィギュレーション ファイルをコピーする ために使用する TFTP サーバを、アクセス リスト内のサーバに 限定します。
	access-list-number には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
access-list access-list-number {deny permit} source [source-wildcard]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り 返します。
	 access-list-number には、ステップ2で指定したアクセスリスト番号を入力します。
	 deny キーワードは、条件が一致した場合にアクセスを拒否 します。permit キーワードは、条件が一致した場合にアク セスを許可します。
	 source には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。
	 (任意) source-wildcard には、source に適用されるワイル ドカード ビットをドット付き 10 進表記で入力します。無視 するビット位置には1を入れます。
	アクセス リストの末尾には、すべてに対する暗黙の拒否ステー トメントが常に存在することに注意してください。
end	特権 EXEC モードに戻ります。
show running-config	設定を確認します。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
	コマンド configure terminal snmp-server tftp-server-list access-list-number access-list access-list-number {deny permit} source [source-wildcard] end show running-config copy running-config startup-config

SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクト にアクセスできます。この設定では、スイッチはトラップを送信しません。

Switch(config) # snmp-server community public

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限です べてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33 (SNMPv1 を使用) や、ホスト 192.180.1.27 (SNMPv2C を使用) へ VTP トラップを送 信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、comaccess コミュニティ ストリングを使用するアクセス リスト 4 のメンバーに、すべてのオブ ジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオ ブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリ ング public を使用してホスト cisco.com に送信します。

Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public

次に、エンティティ MIB トラップをホスト cisco.com に送信する例を示します。コミュニティ ストリ ングは制限されます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行めはこれらのトラップの宛先を 指定し、ホスト cisco.com に対する以前の snmp-server host コマンドを無効にします。

Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity

次に、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送 信するようにスイッチをイネーブルにする例を示します。

Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public

次に、ユーザとリモート ホストを関連付けて、ユーザがグローバル コンフィギュレーション モードの時に auth (authNoPriv) 認証レベルで情報を送信する例を示します。

Switch(config)# snmp-server engineID remote 192.180.1.27 0000063000100alc0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0

SNMP ステータスの表示

不正なコミュニティストリングエントリ、エラー、要求変数の数など、SNMPの入出力統計情報を表示するには、show snmp 特権 EXEC コマンドを使用します。また、表 30-6 に記載されたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。この場合に表示されるフィールドの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

表 30-6 SNMP 情報を表示するためのコマンド

機能	デフォルト設定	
show snmp	SNMP 統計情報を表示します。	
show snmp engineID [local remote]	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エ ンジンに関する情報を表示します。	
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。	
show snmp pending	保留中の SNMP 要求の情報を表示します。	
show snmp sessions	現在の SNMP セッションの情報を表示します。	
show snmp user	SNMP ユーザテーブルの各 SNMP ユーザ名に関する情報を表示します。	
	 (注) このコマンドは、auth noauth priv モードの SNMPv3 設定情報を表示 するときに使用する必要があります。この情報は、show running-config の出力には表示されません。 	





ACL によるネットワーク セキュリティの設定

この章では、Catalyst 2960 スイッチにおいて、Access Control List (ACL; アクセス コントロール リ スト)を使用してネットワーク セキュリティを設定する方法について説明します。ACL はアクセス リ ストとも呼ばれます。

(注)

スイッチが LAN Lite イメージを実行中の場合、ACL を設定できますが、その ACL を物理インター フェイスに接続できません。LAN Lite イメージまたは LAN Base イメージのいずれかを実行する場合 は、ACL を VLAN インターフェイスに接続して CPU へのトラフィックをフィルタリングします。

この章では、IP ACL の参考資料は IP Version 4 (IPv4) の ACL を対象としています。

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンス、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』を参照してください。Cisco IOS のドキュメントには、Cisco.com ホームページ (**Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides** または **Command References**) からアクセスできます。

この章で説明する内容は、次のとおりです。

- 「ACL の概要」(P.31-22)
- 「IPv4 ACL の設定」(P.31-25)
- 「名前付き MAC 拡張 ACL の作成」(P.31-43)
- 「IPv4 ACL の設定の表示」(P.31-46)

■ ACL の概要

ACL の概要

パケットフィルタリングは、ネットワークトラフィックを限定し、特定のユーザまたはデバイスによ るネットワークの使用を制限するうえで役立ちます。ACLは、トラフィックをスイッチの通過時に フィルタリングし、パケットが指定されたインターフェイスを通過することを許可または拒否します。 ACLは、パケットに適用される許可条件および拒否条件の順序付けられたコレクションです。パケッ トがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較 し、アクセスリストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどう かを確認します。アクセスリスト内の条件を1つずつ調べ、パケットをテストします。最初に一致し た条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する 最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちま す。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合は パケットを転送し、制限条件がある場合はパケットを廃棄します。スイッチは、転送するすべてのパ ケットに ACL を使用できます。

スイッチにアクセスリストを設定することにより、ネットワークの基本的なセキュリティを確保できます。ACLを設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACLを使用すると、どのホストがネットワークのどの部分にアクセスできるかを制御したり、トラフィックの種類ごとに転送するかブロックするかを指定したりできます。たとえば、電子メールトラフィックの転送を許可し、Telnetトラフィックの転送を拒否することもできます。

ACL には、アクセス制御エントリ(ACE)の順序付けられたリストが含まれています。各ACE には、 permit または deny と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。 permit または deny の意味は、ACL が使用されるコンテキストによって変わります。

スイッチは、IP ACL とイーサネット (MAC) ACL をサポートしています。

- IP ACL は、TCP、User Datagram Protocol (UDP; ユーザ データグラム プロトコル)、Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル)、および Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) などの IPv4 トラ フィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。



) MAC ACL を使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

このスイッチは、Quality of Service (QoS; サービス品質)分類 ACL もサポートしています。詳細に ついては、「QoS ACL に基づく分類」(P.33-8)を参照してください。

ここでは、次の概要について説明します。

- 「ポート ACL」 (P.31-23)
- 「フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理」 (P.31-24)

ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL がサポー トされるのは物理インターフェイスだけで、EtherChannel インターフェイスではサポートされず、着 信方向のインターフェイスだけに適用されます。以下のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコルタイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先のMACアドレスと任意でプロトコルタイプ情報を使用できるMAC拡張アクセスリスト

<u>》</u> (注)

MAC ACL を使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

スイッチは、インターフェイスに設定されたすべての着信機能に関連付けられた ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。 このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。図 31-1 に、 すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのア クセスを制御する例を示します。レイヤ 2 入力に適用される ACL は、Host A に Human Resources ネットワークへのアクセスを許可しますが、Host B には同じネットワークへのアクセスを禁止します。 ポート ACL は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

図 31-1 ACL によるネットワークへのトラフィックの制御



ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラ フィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。 ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アド レスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アク セス リストと MAC アクセス リストの両方を適用します。

(注)

レイヤ2 インターフェイスに適用できるのは、IP アクセス リスト1 つと MAC アクセス リスト1 つだ けです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ2 インター フェイスに新しい IP アクセス リストまたは MAC アクセス リストを適用すると、設定済みの ACL が新 しい ACL に置き換えられます。

フラグメント化されたトラフィックとフラグメント化されていないトラ フィックの処理

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、 TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部 分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

ACE には、レイヤ4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものが あります。レイヤ4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメン トに標準的な方法では適用できません。フラグメントにレイヤ4 情報が含まれておらず、ACE が一部 のレイヤ4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ3 情報(TCP や UDP などのプロトコル タイプを含む)をチェックする許可 ACE は、含まれていないレイヤ4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ4情報をチェックする拒否 ACE は、フラグメントにレイヤ4情報が含まれていない限り、 フラグメントと一致しません。

以下のコマンドで構成され、フラグメント化された3つのパケットに適用されるアクセスリスト102 を例に取って説明します。

```
Switch(config) # access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config) # access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config) # access-list 102 permit tcp any host 10.1.1.2
Switch(config) # access-list 102 deny tcp any any
```

(注)

最初の2つのACEには宛先アドレスの後に *eq*キーワードがありますが、これは既知のTCP 宛先ポート番号がそれぞれ Simple Mail Transfer Protocol (SMTP; シンプルメール転送プロトコル)および Telnet と一致するかどうかをチェックすることを意味します。

 パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃ってい るため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE (permit) と 一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけを チェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 である ことです。 パケットBは、ホスト10.2.2.2のポート65001からホスト10.1.1.2のTelnetポートに送信されます。このパケットがフラグメント化された場合、レイヤ3情報とレイヤ4情報がすべて揃っているため、最初のフラグメントが2つめのACE(deny)と一致します。残りのフラグメントは、レイヤ4情報が含まれていないため、2つめのACEと一致しません。残りのフラグメントは3つめのACE(permit)と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域 幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費され ます。

フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE (deny) と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

IPv4 ACL の設定

(注)

スイッチが LAN Lite イメージを実行中の場合、ACL を設定できますが、その ACL を物理インター フェイスに接続できません。LAN Lite イメージまたは LAN Base イメージのいずれかを実行する場合 は、ACL を VLAN インターフェイスに接続して CPU へのトラフィックをフィルタリングします。

このスイッチで IP v4ACL を設定する手順は、シスコの他のスイッチやルータで IP v4ACL を設定する 手順と同じです。ここでは、その設定手順を簡単に説明します。ACL の設定の詳細については、 『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」にある 「Configuring IP Services」を参照してください。コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*』を参照してください。Cisco IOS の ドキュメントには、Cisco.com ホームページ (Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides または Command References) からアクセスできます。

このスイッチは、Cisco IOS ルータの ACL に関連する以下の機能をサポートしていません。

- 非 IP プロトコル ACL (表 31-1 (P.31-26) を参照) またはブリッジ グループ ACL
- IP アカウンティング
- 着信および発信レート制限(QoS ACL によるレート制限を除く)
- リフレクシブ ACL またはダイナミック ACL (スイッチ クラスタリング機能で使用される専用の ダイナミック ACL を除く)
- ACL ロギング

このスイッチで IP ACL を使用する手順は次のとおりです。

ステップ1 アクセスリストの番号または名前とアクセス条件を指定して、ACL を作成します。

ステップ2 その ACL をインターフェイスまたは端末回線に適用します。

IPv4 ACL の設定

ここでは、次の設定情報について説明します。

- 「標準 IPv4 ACL および拡張 IPv4 ACL の作成」(P.31-26)
- 「端末回線への IPv4 ACL の適用」(P.31-37)
- 「インターフェイスへの IPv4 ACL の適用」(P.31-38)
- 「ハードウェアおよびソフトウェアによる IP ACL の処理」(P.31-39)
- 「ACL のトラブルシューティング」(P.31-40)
- 「IPv4 ACL の設定例」(P.31-41)

標準 IPv4 ACL および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL は、許可条件と拒否条件の順序付けられたコレクション です。スイッチは、アクセスリスト内の条件を1つずつ調べ、パケットをテストします。最初に一致 した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致す る最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちま す。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について以下の ACL (アクセス リスト)をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロト コル タイプ情報を使用して制御のきめ細かさを高めることもできます。

ここでは、アクセス リストとその作成方法について説明します。

- •「アクセスリスト番号」(P.31-26)
- 「番号付き標準 ACL の作成」(P.31-27)
- 「番号付き拡張 ACL の作成」(P.31-29)
- 「ACL 内の ACE の並べ替え」(P.31-33)
- 「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.31-33)
- 「ACL での時間範囲の使用」(P.31-35)
- 「ACL へのコメントの挿入」(P.31-37)

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。表 31-1 に、 アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているか どうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト(1~ 199 および 1300~ 2699)をサポートします。

表 31-1 アクセス リスト番号

アクセス リスト番号	タイプ	サポート状況
$1 \sim 99$	IP 標準アクセス リスト	あり
$100 \sim 199$	IP 拡張アクセス リスト	あり
$200 \sim 299$	プロトコル タイプコード アクセス リスト	なし
$300 \sim 399$	DECnet アクセス リスト	なし
$400 \sim 499$	XNS 標準アクセス リスト	なし

アクセス リスト番号	タイプ	サポート状況
$500 \sim 599$	XNS 拡張アクセス リスト	なし
$600 \sim 699$	AppleTalk アクセス リスト	なし
$700 \sim 799$	48 ビット MAC アドレス アクセス リスト	なし
800 ~ 899	IPX 標準アクセス リスト	なし
$900 \sim 999$	IPX 拡張アクセス リスト	なし
$1000 \sim 1099$	IPX SAP アクセス リスト	なし
$1100 \sim 1199$	拡張 48 ビット MAC サマリー アドレス アクセ	なし
	スリスト	
$1200 \sim 1299$	IPX サマリー アドレス アクセス リスト	なし
1300 ~ 1999	IP 標準アクセス リスト(拡張範囲)	あり
$2000 \sim 2699$	IP 拡張アクセス リスト(拡張範囲)	あり

表 31-1 アクセス リスト番号 (続き)



番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名 前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別 に削除できるという利点があります。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number {deny permit} source [source-wildcard]	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセスリストを定義します。
		<i>access-list-number</i> には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。
		条件が一致した場合にアクセスを拒否する場合は deny、許可 する場合は permit を指定します。
		<i>source</i> には、パケットの送信元となるネットワークまたはホ ストのアドレスを次の形式で指定します。
		 ドット付き 10 進表記による 32 ビット長の値。
		 source および source-wildcard の 0.0.0.0 255.255.255 の省略形を意味するキーワード any。source-wildcard を 入力する必要はありません。
		 source および source-wildcard の値 source 0.0.0.0 の省略 形を意味するキーワード host。
		(任意) source-wildcard は、ワイルドカード ビットを送信元ア ドレスに適用します。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	show access-lists [number name]	アクセス リストの設定を表示します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま
		す。

ACL 全体を削除するには、no access-list access-list-number グローバル コンフィギュレーション コマ ンドを使用します。番号付きアクセス リストから個々の ACE は削除できません。

(注)

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、 ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに 注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマ スクを省略すると、0.0.0.0 がマスクと見なされます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、他のすべてのホストへのアクセスを許可し、 結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny 171.69.198.102
    20 permit any
```

スイッチは、host 一致条件があるエントリと don't care マスク 0.0.0.0 を含む一致条件があるエントリ がリストの先頭に移動し、0 以外の don't care マスクを含むエントリよりも前に位置するように、標準 アクセス リストの順序を書き換えます。そのため、show コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を端末回線(「端末回線への IPv4 ACL の適用」(P.31-37)を参照) やインターフェイス(「インターフェイスへの IPv4 ACL の適用」(P.31-38)を参照)に適用できます。

番号付き拡張 ACL の作成

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスを宛先アドレスを使用でき、任意でプロトコルタイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの 末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト 内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

以下の IP プロトコルがサポートされます (プロトコル キーワードはカッコ内に太字で示してあります)。

認証ヘッダー プロトコル (**ahp**)、Enhanced IGRP (**eigrp**)、Encapsulating Security Payload (**esp**)、 Generic Routing Encapsulation (**gre**)、インターネット制御メッセージ プロトコル (**icmp**)、インター ネット グループ管理プロトコル (**igmp**)、任意の内部プロトコル (**ip**)、IP-in-IP トンネリング (**ipinip**)、KA9Q NOS 互換 IP over IP トンネリング (**nos**)、Open Shortest Path First ルーティング (**ospf**)、Payload Compression Protocol (**pcp**)、Protocol Independent Multicast (**pim**)、Transmission Control Protocol (**tcp**)、ユーザ データグラム プロトコル (**udp**)

(注) ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべて フィルタリングできます。

各プロトコルのキーワードの詳細については、以下のコマンドリファレンスを参照してください。

- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2
- Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2

これらのドキュメントには、Cisco.com ホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**) からアクセスできます。



このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、 Type of Service (ToS; サービス タイプ)の minimize-monetary-cost ビットに基づくフィルタリングも サポートしていません。

サポートされているパラメータのカテゴリは、TCP、UDP、ICMP、IGMP、その他の IP です。

拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド		目的
ステップ 1	configure terminal		グローバル コンフィギュレーション モードを開始します。
ステップ 2a	ステップ 2a access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]		拡張 IPv4 アクセス リストおよびアクセス条件を定義します。
			<i>access-list-number</i> には、100 ~ 199 または 2000 ~ 2699 の 10 進数を指定 します。
			条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。
			「 protocol には、IP プロトコルの名前または番号を入力します。使用できる
	(注)	dscp 値を入力した場合、 tos または precedence は入力できません。 dscp を入力しない場合	値は、 ahp eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、nos、ospf、 pcp、pim、tcp、udp、 および IP プロトコル番号を表す 0 ~ 255 の整数で す。一致条件としてインターネット プロトコル (ICMP、TCP、UDP など) を指定するには、キーワード ip を使用します。
		は、 tos と precedence 値の両方を入力できま す。	(注) この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加のパラメータについては、手順 2b ~ 2e を参照してください。
			<i>source</i> には、パラメータの送信元であるネットワークまたはホストの番号を 指定します。
			source-wildcard は、ワイルドカード ビットを送信元アドレスに適用します。
			<i>destination</i> には、パラメータの宛先であるネットワークまたはホストの番 号を指定します。
			<i>destination-wildcard</i> は、ワイルドカード ビットを宛先アドレスに適用します。
			source、source-wildcard、destination、および destination-wildcard の値は、 次の形式で指定します。
			 ドット付き 10 進表記による 32 ビット長の値。
			• 0.0.0.0 255.255.255 (任意のホスト)を表すキーワード any。
			• 単一のホスト 0.0.0.0 を表すキーワード host。
			その他のキーワードはオプションであり、次の意味を持ちます。
			 precedence:パケットを0~7の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、routine (0)、priority (1)、immediate (2)、flash (3)、flash-override (4)、critical (5)、internet (6)、network (7)です。
			 fragments: 2 つめ以降のフラグメントをチェックする場合に入力します。
			 tos:パケットを0~15の番号または名前で指定するサービスタイプレベルと一致させる場合に入力します。指定できる値は、normal(0)、max-reliability(2)、max-throughput(4)、min-delay(8)です。
			 time-range:このキーワードの詳細については、「ACL での時間範囲の 使用」(P.31-35)を参照してください。
			 dscp:パケットを0~63の番号で指定するDSCP値と一致させる場合 に入力します。また、指定できる値のリストを表示するには、疑問符 (?)を使用します。

	コマンド	目的
または	access-list access-list-number {deny permit} protocol any any [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]	アクセスリスト コンフィギュレーション モードで、source および source wildcard の値 0.0.00 255.255.255 の省略形と destination および destination wildcard の値 0.0.00 255.255.255.255 の省略形を使用して、拡 張 IP アクセス リストを定義します。 送信示と気先のアドレスお上びロイルドカードの代わりに any キーロード
		を使用できます。
または	access-list access-list-number {deny permit} protocol host source host destination [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscn dscn]	source および source wildcard の値 <i>source</i> 0.0.0.0 の省略形と destination お よび destination wildcard の値 <i>destination</i> 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに host キーワードを 使用できます。
手順 2b	access-list access-list-number	(任音) 拡張 TCP アクセス リストお上びアクセス条件を定義します
JARED	{deny permit} tcp source	TCP の場合は ten を入力します。
	source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] [flag]	以下の例外を除き、手順 2a の説明にあるパラメータと同じパラメータを使用します。
		(任意) operator および port を入力すると、送信元ポート (source source-wildcard の後に入力した場合) または宛先ポート (destination destination-wildcard の後に入力した場合) が比較されます。使用可能な演算子は、eq (等しい)、gt (より大きい)、lt (より小さい)、neq (等しくない)、range (包含範囲) などです。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。
		<i>port</i> には、10進数(0~65535)のポート番号または TCP ポート名を入力 します。TCP ポート名を確認するには、?を使用するか、『 <i>Cisco IOS IP</i> <i>Configuration Guide, Release 12.2</i> 』の「IP Addressing and Services」にあ る「Configuring IP Services」を参照してください。TCP をフィルタリング するときには、TCP ポートの番号または名前だけを使用します。
		他のオプションのキーワードの意味は次のとおりです。
		 established:確立された接続と照合する場合に入力します。このキー ワードは、ack または rst フラグでの照合と同じ機能を果たします。
		 <i>flag</i>:指定された TCP ヘッダー ビットを基準にして照合します。入力 できるフラグは、ack(確認応答)、fin(終了)、psh(プッシュ)、rst (リセット)、syn(同期)、または urg(緊急)です。
手順 2c	access-list access-list-number	(任意) 拡張 UDP アクセス リストおよびアクセス条件を定義します。
	{deny permit} udp source source-wildcard	ユーザ データグラム プロトコルの場合は、udp を入力します。
	[operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name]	UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、 [<i>operator</i> [<i>port</i>]] ポート番号またはポート名は、UDP ポートの番号または名 前でなければなりません。また、UDP では、 flag および established パラ メータは無効です。
	[dscp dscp]	

	コマンド	目的
手順 2d	access-list access-list-number	(任意)拡張 ICMP アクセス リストおよびアクセス条件を定義します。
	{ deny permit } icmp <i>source</i> <i>source-wildcard destination</i>	インターネット制御メッセージ プロトコルの場合は、icmp を入力します。
	destination-wildcard [icmp-type [[icmp-type icmp-code] [icmp-message]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]	ICMP パラメータは手順 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加 されています。オプションのキーワードの意味は次のとおりです。
		 <i>icmp-type</i>: ICMP メッセージ タイプでフィルタリングする場合に入力 します。指定できる値の範囲は、0~255です。
		 <i>icmp-code</i>: ICMP パケットを ICMP メッセージ コード タイプでフィル タリングする場合に入力します。指定できる値の範囲は、0~255 で す。
		 <i>icmp-message</i>: ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力し ます。ICMP メッセージ タイプ名およびコード名のリストを確認するに は、? を使用するか、『<i>Cisco IOS IP Configuration Guide, Release 12.2</i>』 の「Configuring IP Services」を参照してください。
手順 2e	access-list access-list-number	(任意)拡張 IGMP アクセス リストおよびアクセス条件を定義します。
	{ deny permit } igmp <i>source</i> <i>source-wildcard destination</i>	インターネット グループ管理プロトコルの場合は、igmp を入力します。
	destination-wildcard [igmp-type] [precedence	IGMP パラメータは手順 2a の IP プロトコルの説明にあるパラメータとほと んど同じですが、次に示すオプションのパラメータが追加されています。
	precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]	<i>igmp-type</i> : IGMP メッセージ タイプと照合するには、0 ~ 15 の番号または メッセージ名(dvmrp、host-query、host-report、pim、 または trace)を 入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists [number name]	アクセス リストの設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リスト全体を削除するには、no access-list access-list-number グローバル コンフィギュレー ション コマンドを使用します。番号付きアクセス リストから個々の ACE は削除できません。

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを拒否し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します (eq キーワードを宛先アドレスの後に指定すると、Telnet に対応する TCP 宛先ポート 番号がチェックされます)。

Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet

- Switch(config)# access-list 102 permit tcp any any Switch(config)# end Switch# show access-lists Extended IP access list 102
- 10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet

20 permit tcp any any

ACL の作成後に(端末からの入力などによって)追加したエントリは、リストの末尾に追加されます。 番号付きアクセス リストの特定の場所にはアクセス リスト エントリを追加または削除できません。



ACL を作成するときには、アクセス リストの末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号付き拡張 ACL を端末回線(「端末回線への IPv4 ACL の適用」(P.31-37)を参照) やイン ターフェイス(「インターフェイスへの IPv4 ACL の適用」(P.31-38)を参照)に適用できます。

ACL 内の ACE の並べ替え

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時に自動的に生成されます。ip access-list resequence グローバル コンフィギュレーション コマンドを使用して、ACL のシーケンス 番号を編集したり、ACE の適用順序を変更したりできます。たとえば、ACL に新しい ACE を追加す ると、その ACE はリストの末尾に配置されます。この場合、シーケンス番号を変更することで、ACE を ACL 内の別の位置に移動できます。

ip access-list resequence コマンドの詳細については、次の URL にアクセスしてください。

http://preview.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a 60.html

名前付き標準 ACL および名前付き拡張 ACL の作成

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング(名前)を使用できます。名前付 き ACL を使用すると、ルータ上で番号付きアクセスリストの場合より多くの IPv4 アクセスリストを 設定できます。アクセスリストの識別手段として名前を使用する場合のモードとコマンド構文は、番 号を使用する場合とは多少異なります。ただし、IP アクセスリストを使用するすべてのコマンドを名 前付きアクセスリストで使用できるわけではありません。

(注)

標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号に することもできます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号 付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点が あります。

名前付き ACL を設定するときには、次の注意事項および制限事項に留意してください。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- 「標準 IPv4 ACL および拡張 IPv4 ACL の作成」(P.31-26) で説明したとおり、番号付き ACL も使 用できます。

名前を使用して標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip access-list standard name	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。
		名前には、1 ~ 99 の番号を使用できます。

コマンド	目的
deny {source [source-wildcard] host source any} または	アクセス リスト コンフィギュレーション モードで、パケット を転送するのか廃棄するのかを決定する 1 つ以上の拒否条件ま たは許可条件を 指定します。
<pre>permit {source [source-wildcard] host source any}</pre>	• host source : source および source wildcard の値 source 0.0.0.0
	• any : source および source wildcard の値 0.0.0.0 255.255.255.255
end	特権 EXEC モードに戻ります。
show access-lists [number name]	アクセス リストの設定を表示します。
copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま す。
	コマンド deny {source [source-wildcard] host source any} または permit {source [source-wildcard] host source any} end show access-lists [number name] copy running-config startup-config

名前付き標準 ACL を削除するには、no ip access-list standard name グローバル コンフィギュレー ション コマンドを使用します。

名前を使用して拡張範囲 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip access-list extended name	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。
		名前には、100 ~ 199 の番号を使用できます。
ステップ 3	{deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host	アクセス リスト コンフィギュレーション モードで、許可条件 または拒否条件を指定します。 プロトコルお上び他のキーロードの定差についてけ、「番号付
	destination any [precedence precedence] [tos tos] [established] [time_range	き拡張 ACL の作成」(P.31-29)を参照してください。
	time-range-name]	• host <i>source</i> : source および source wildcard の値 <i>source</i> 0.0.0.0
		• <i>host destination</i> : destination および destination wildcard の値 <i>destination</i> 0.0.0.0
		 any: source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show access-lists [number name]	アクセス リストの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

名前付き標準 ACL を削除するには、no ip access-list extended *name* グローバル コンフィギュレー ション コマンドを使用します。

標準 ACL または拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステート メントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケット に適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。
ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に 選択的に追加できません。ただし、no permit および no deny アクセスリスト コンフィギュレーショ ンモード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアク セス リスト *border-list* から ACE を個別に削除する例を示します。

Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any

番号付き ACL ではなく名前付き ACL を使用する理由の1つとして、名前付き ACL では行を選択して 削除できることがあります。

作成した名前付き ACL をインターフェイスに適用できます(「インターフェイスへの IPv4 ACL の適 用」(P.31-38)を参照)。

ACL での時間範囲の使用

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に 基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻 および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに 時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメン トの有効期間(指定期間内や指定曜日など)を定義できます。time-range キーワードおよび引数につ いては、「標準 IPv4 ACL および拡張 IPv4 ACL の作成」(P.31-26) および「名前付き標準 ACL およ び名前付き拡張 ACL の作成」(P.31-33) にある名前付きおよび番号付き拡張 ACL の作成に関する表 を参照してください。

時間ベースのアクセスリストを使用すると、CPU に負荷が生じます。これは、アクセスリストの新しい設定を他の機能や TCAM にロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセスリストが短期間に連続して(互いに数分以内に)有効となるような設定とならないように注意する必要があります。

(注)

時間範囲は、スイッチのシステム クロックに基づきます。したがって、信頼できるクロック ソースが 必要です。Network Time Protocol (NTP) を使用してスイッチ クロックを同期させることをお勧めし ます。詳細については、「システム日時の管理」(P.6-1) を参照してください。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	time-range time-range-name	作成する時間範囲には意味のある名前(workhours など)を割り当 て、時間範囲コンフィギュレーションモードを開始します。名前に スペースや疑問符を含めることはできません。また、文字から始め る必要があります。
ステップ 3	absolute [start time date]	適用対象の機能がいつ動作可能になるかを指定します。
	または periodic day-of-the-week hh:mm to	 時間範囲には、absolute ステートメントを1つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。
	[day-of-the-week] hh:mm または	 複数の periodic ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。
	<pre>periodic {weekdays weekend daily} hh:mm to hh:mm</pre>	設定例を参照してください。
ステップ 4	end	特権 EXEC モードに戻ります。

ACL の時間範囲パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

	コマンド	目的
ステップ 5	show time-range	時間範囲の設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
	複数の項目をそれぞれ異なる時 設定した時間範囲の制限を削除。	間に有効にする場合は、上記の手順を繰り返してください。 するには no fime-range <i>time-range-name</i> グローバル コンフィギュ
	レーション コマンドを使用しま	t.
	次に、 <i>workhours</i> (営業時間)の 認する例を示します。	D時間範囲および会社の休日(2006 年 1 月 1 日)を設定し、設定を確
	Switch (config + time-range worknows Switch (config-time-range) # periodic weekdays 8:00 to 12:00 Switch (config-time-range) # periodic weekdays 13:00 to 17:00 Switch (config-time-range) # exit Switch (config + time-range new_year_day_2006 Switch (config-time-range) # absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006 Switch (config-time-range) # end Switch # show time-range time-range entry: new_year_day_2003 (inactive) absolute start 00:00 01 January 2006 end 23:59 01 January 2006 time-range entry: workhours (inactive) periodic weekdays 8:00 to 12:00 periodic weekdays 13:00 to 17:00 時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、 アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された作 間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての	
	<pre>Switch(config)# access-list Switch(config)# access-list Switch(config)# end Switch# show access-lists Extended IP access list 188 10 deny tcp any any time- 20 permit tcp any any time- 20 permit tcp any any time %だ、名前付き ACL を使用して Switch(config)# ip access-li Switch(config-ext-nacl)# den Switch(config-ext-nacl)# den Switch(config-ext-nacl)# per Switch(config-ext-nacl)# end Switch(config-ext-nacl)# end Switch(config-ext-nacl)# end Switch(config-ext-nacl)# den Switch(config-ext-nacl)# den Switch(config-ext-nacl)# den Switch(config-ext-nacl)# end Switch# show ip access-lists Extended IP access list lpip 10 permit ip any any Extended IP access list deny 10 deny tcp any any time Extended IP access list may_ 10 permit tcp any any time</pre>	188 deny top any any time-range new_year_day_2006 188 permit top any any time-range workhours range new_year_day_2006 (inactive) ee-range workhours (inactive) C同じトラフィックを許可および拒否する例を示します。 st extended deny_access my top any any time-range new_year_day_2006 t st extended may_access mit top any any time-range workhours

ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント(注 釈)を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメ ント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コ メントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるよう に、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにある と、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、access-list access-list number remark remark グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの no 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはア クセスを許可しません。

Switch(config)# access-list 1 remark Permit only Jones workstation through Switch(config)# access-list 1 permit 171.69.2.88 Switch(config)# access-list 1 remark Do not allow Smith through Switch(config)# access-list 1 deny 171.69.3.13

名前付き IP ACL のエントリには、remark アクセス リスト コンフィギュレーション コマンドを使用 します。コメントを削除するには、このコマンドの no 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

Switch(config)# ip access-list extended telnetting Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべて に同じ制限を設定する必要があります。

ACL をインターフェイスに適用する手順については、「インターフェイスへの IPv4 ACL の適用」 (P.31-38)を参照してください。

仮想端末回線とACLに指定されたアドレス間の着信接続および発信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	line [console vty] line-number	設定する回線を指定し、インライン コンフィギュレーション モードを 開始します。
		 console:コンソール端末回線を指定します。コンソールポートは DCEです。
		• vty : リモート コンソール アクセス用の仮想端末を指定します。
		<i>line-number</i> は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は0~16です。

	コマンド	目的
ステップ 3	access-class access-list-number	(デバイスへの)特定の仮想端末回線とアクセス リストに指定されたア
	{in out}	ドレス間の着信接続および発信接続を制限します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	アクセス リストの設定を表示します。
ステップ 6	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

端末回線から ACL を削除するには、no access-class access-list-number {in | out} ライン コンフィギュ レーション コマンドを使用します。

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスに適用する方法について説明します。以下の注意事項に留意してください。

- ACL は着信レイヤ2ポートだけに適用してください。
- ACL を着信 VLAN インターフェイスまたは発信 VLAN インターフェイスのいずれかに適用する と、SNMP、Telnet、または Web トラフィックのような CPU に発信されるパケットをフィルタリ ングできます。VLAN インターフェイスに適用される IPv4 ACL は、ネットワーク内の特定のホ スト、または特定のアプリケーション (SNMP、Telnet、SSH など)に対してアクセスを制限する ことによって、スイッチ管理セキュリティを提供します。VLAN インターフェイスに接続された ACL は、VLAN 上のパケットのハードウェア スイッチングには影響しません。



E) LAN Lite イメージを実行しているスイッチでは、ACL は VLAN インターフェイスにだけ 適用でき、物理インターフェイスには適用できません。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用でき ます。
- VLAN のメンバーであるポートに ACL を適用すると、そのポートの ACL は VLAN インターフェ イスに適用された ACL よりも優先されます。ポート ACL は VLAN インターフェイス ACL を上 書きします。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュ レーション モードを開始します。
		LAN Base イメージが実行されているスイッチでは、インターフェイス に物理インターフェイスまたは VLAN インターフェイスを指定する必 要があります。LAN Lite イメージが実行されているスイッチでは、イ ンターフェイスに VLAN インターフェイスを指定する必要がありま す。

	コマンド	目的
ステップ 3	<pre>ip access-group {access-list-number</pre>	指定されたインターフェイスへのアクセスを制御します。
	$ name \} \{ in out \}$	out キーワードがサポートされるのは、VLAN インターフェイスだけ
		です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show running-config	アクセスリストの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定したアクセス グループを削除するには、no ip access-group {access-list-number | name} {in | out} インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートにアクセスリスト2を適用して、ポートに着信するパケットをフィルタリングする例を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in

次に、ポートにアクセス リスト 3 を適用して、CPU に発信されるパケットをフィルタリングする例を 示します。

Switch(config)# interface vlan 1
Switch(config-if)# ip access-group 3 in

着信 ACL の場合、スイッチはパケットの受信後に ACL とパケットを照合します。ACL がパケットを 許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチ はパケットを廃棄します。

発信 ACL の場合、スイッチは、制御されたインターフェイスとの間でパケットを送受信した後に ACL とパケットを照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。 ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されて いないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には CPU に転送してソ フトウェア処理を行う必要があるものもあります。ハードウェアで ACL の設定を保存する領域が不足 すると、パケットは転送のために CPU に送られます。ソフトウェア転送トラフィックの転送レート は、ハードウェア転送トラフィックより大幅に低くなります。

ACL により多数のパケットが CPU に送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェ アでアクセスが制御されるパケットは含まれません。スイッチド パケットに関するハードウェアの ACL の基本的な統計情報を取得するには、**show access-lists hardware counters** 特権 EXEC コマンド を使用します。

ACL のトラブルシューティング

次の ACL マネージャ メッセージが表示されて [chars] がアクセス リスト名である場合は、 ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

スイッチには、ACL のハードウェア表現を作成するのに使用可能なリソースが不足しています。この リソースには、ハードウェアメモリおよびラベル スペースが含まれますが、CPU メモリは含まれませ ん。この問題の原因は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足です。 論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での eq 以外(ne、 gt、lt、range)のテストで必要です。

次のいずれかのワークアラウンドを使用します。

- ACL 設定を変更して使用するリソースを減らします。
- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

専用のハードウェア リソースを識別するには、show platform layer4 acl map 特権 EXEC コマンドを 入力します。スイッチに使用可能なリソースがない場合は、出力に index 0 \sim index 15 が使用できない ことが示されます。

十分なリソースがない ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

たとえば、次の ACL をインターフェイスに適用し、

permit tcp source source-wildcard destination destination-wildcard range 5 60 permit tcp source source-wildcard destination destination-wildcard range 15 160 permit tcp source source-wildcard destination destination-wildcard range 115 1660 permit tcp source source-wildcard destination destination-wildcard

なおかつ次のメッセージが表示される場合は、

ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

フラグ関連の演算子は使用できません。この問題を回避するには、

 ip access-list resequence グローバル コンフィギュレーションコマンドを使用することによって、 4 つめの ACE を 1 つめの ACE の前に移動させます。

permit tcp source source-wildcard destination destination-wildcard permit tcp source source-wildcard destination destination-wildcard range 5 60 permit tcp source source-wildcard destination destination-wildcard range 15 160 permit tcp source source-wildcard destination destination-wildcard range 115 1660

または

他のACL名または番号よりも英数字順で先に表示される名前または番号にACLの名前を変更します(たとえば、ACL 79をACL 1 に変更します)。

これで、ACL 内の 1 つめの ACE をインターフェイスに適用できます。スイッチは ACE を Opselect index 内の使用可能なマッピング ビットに割り当てた後、フラグ関連の演算子を割り当てて TCAM 内の同じビットを使用します。

IPv4 ACL の設定例

ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルの詳細については、 『*Cisco IOS Security Configuration Guide, Release 12.2*』と、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「IP Addressing and Services」にある「Configuring IP Services」を参照してください。

次の例の ACL は、インターネット ホスト 172.20.128.64 へのポート アクセスを許可する標準 ACL です。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
   10 permit 172.20.128.64 wildcard bits 0.0.0.0
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 in
```

次の例の ACL は、ポート 80 (HTTP) からのポート トラフィックを拒否する拡張 ACL です。この ACL は、それ以外のすべてのトラフィックを許可します。

```
Switch(config)# access-list 106 deny tcp any any eq 80
Switch(config)# access-list 106 permit ip any any
Switch(config)# end
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

番号付き ACL

次の例の ACL は、ネットワーク 36.0.0.0 サブネット上のアドレスを受け入れ、56.0.0.0 サブネットからのすべてのパケットを拒否します。この ACL は、ポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# access-list 2 deny 56.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストが インターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、 IP ホストからは、専用メール ホストのメール (SMTP) ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先 ポートは 25 です。安全なネットワーク システムは、ポート 25 で常にメール接続を受け入れるため、 着信サービスを制御します。

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in

名前付き ACL

次に、*marketing_group* という名前の拡張 ACL を作成する例を示します。*marketing_group* ACL は、 宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可 し、その他の TCP トラフィックを拒否します。この ACL は他のすべての IP トラフィックを許可しま す。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
```

marketing group ACL は、ポートに着信するトラフィックに適用されます。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group marketing_group in
```

IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前8時~午後6時(18:00)の間、IPのHTTPトラフィックを拒否する 例を示します。この例では、土曜日および日曜日の正午~午後8時の間に限り、UDPトラフィックを 許可します。(20:00).

```
Switch(config) # time-range no-http
Switch(config) # periodic weekdays 8:00 to 18:00
!
Switch(config) # time-range udp-yes
Switch(config) # periodic weekend 12:00 to 20:00
!
Switch(config) # ip access-list extended strict
Switch(config-ext-nacl) # deny tcp any any eq www time-range no-http
Switch(config-ext-nacl) # permit udp any any time-range udp-yes
!
Switch(config-ext-nacl) # exit
Switch(config) # interface gigabitethernet0/2
Switch(config-if) # ip access-group strict in
```

コメント付きの IP ACL エントリ

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

Switch(config) # access-list 1 remark Permit only Jones workstation through Switch(config) # access-list 1 permit 171.69.2.88 Switch(config) # access-list 1 remark Do not allow Smith workstation through Switch(config) # access-list 1 deny 171.69.3.13

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しま せん。

Switch (config) # access-list 100 remark Do not allow Winter to browse the web Switch (config) # access-list 100 deny host 171.69.3.85 any eq www Switch (config) # access-list 100 remark Do not allow Smith to browse the web Switch (config) # access-list 100 deny host 171.69.3.13 any eq www

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ2インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

```
<u>(</u>注)
```

MAC ACL を使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

mac access-list extended コマンドでサポートされている非 IP プロトコルの詳細については、このリ リースのコマンド リファレンスを参照してください。

(注)

appletalk は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アク セス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

名前付き MAC 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac access-list extended name	名前を使用して拡張 MAC アクセス リストを定義します。

	コマンド	目的
ステップ 3	{deny permit} {any host source MAC address source MAC address mask} {any host destination MAC address destination MAC address mask} [type mask lsap lsap mask aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000	拡張 MAC アクセス リスト コンフィギュレーション モードで は、すべての (any) 送信元 MAC アドレス、マスク付き送信 元 MAC アドレス、または特定のホスト (host) 送信元 MAC アドレス、およびすべての (any) 宛先 MAC アドレス、マス ク付き宛先 MAC アドレス、または特定の宛先 MAC アドレス に、permit または deny を指定します。
	etype-8042 lat lavc-sca mop-console	(任意) 以下のオプションを入力することもできます。
	wines-echo vines-ip xns-idp 0-65535] [cos cos]	 <i>type mask</i>: Ethernet II または SNAP でカプセル化された パケットの任意の EtherType 番号。10 進数、16 進数、ま たは 8 進数で表記できます。一致検査の前に、任意で指定 できる <i>don't care</i> ビットのマスクが EtherType に適用され ます。
		 Isap Isap mask: IEEE 802.2 でカプセル化されたパケットのLSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で don't care ビットのマスクを指定できます。
		 aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp—非 IP プロトコル。
		 cos cos: プライオリティを設定する 0 ~ 7 の IEEE 802.1Q CoS 番号。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show access-lists [number name]	アクセス リストの設定を表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

ACL 全体を削除するには、no mac access-list extended *name* グローバル コンフィギュレーション コ マンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、他のすべてのタイプのトラフィックを 許可するアクセス リスト *mac1* を作成および表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny any any decnet-iv
    20 permit any any
```

レイヤ2インターフェイスへの MAC ACL の適用

MAC ACL を作成し、それをレイヤ2インターフェイスに適用すると、そのインターフェイスに着信 する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に 留意してください。

- 同じレイヤ2インターフェイスに適用できるのは、IPアクセスリスト1つとMACアクセスリスト1つだけです。IPアクセスリストはIPパケットだけをフィルタリングし、MACアクセスリストは非IPパケットをフィルタリングします。
- 1つのレイヤ2インターフェイスに適用できる MAC アドレス リストは1つだけです。すでに MAC ACL が設定されているレイヤ2インターフェイスに MAC アクセス リストを適用すると、 設定済みの ACL が新しい ACL に置き換えられます。

レイヤ2インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	特定のインターフェイスを指定し、インターフェイス コン フィギュレーション モードを開始します。指定するインター フェイスは物理レイヤ 2 インターフェイス (ポート ACL) で なければなりません。
ステップ 3	mac access-group {name} {in}	MAC アクセス リストを使用して、指定されたインターフェイ スへのアクセスを制御します。
		ポート ACL は、着信方向に限りサポートされます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	<pre>show mac access-group [interface interface-id]</pre>	そのインターフェイスまたはすべてのレイヤ 2 インターフェイ スに適用されている MAC アクセス リストを表示します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

指定したアクセス グループを削除するには、no mac access-group {name} インターフェイス コンフィ ギュレーション コマンドを使用します。

次に、アクセス リスト macl をポートに適用してポートに着信するパケットをフィルタリングする例を示します。

Switch(config)# interface gigabitethernet0/2
Router(config-if)# mac access-group mac1 in

(注)

mac access-group インターフェイス コンフィギュレーション コマンドは、物理レイヤ2インターフェ イスに適用された場合に限り有効となります。このコマンドは、EtherChannel ポート チャネルには使 用できません。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する 場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケッ トを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェ イスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのた めに未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

IPv4 ACL の設定の表示

スイッチ上に設定されている ACL およびインターフェイスに適用された ACL を表示できます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ2インター フェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。ま た、レイヤ2インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、 表 31-2 に記載された特権 EXEC コマンドを使用します。

表 31-2 アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [number name]	現在の1つまたはすべてのIP および MAC アドレス アクセス リストの内容、または特定のアクセス リスト(番号付きまたは名前付き)の内容を 表示します。
show ip access-lists [number name]	現在のすべての IP アクセス リスト、または特定の IP アクセス リスト (番号付きまたは名前付き)の内容を表示します。
<pre>show running-config [interface interface-id]</pre>	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容(設定されたすべての MAC および IP アクセス リスト や、どのアクセス グループがインターフェイスに適用されたかなど)を 表示します。
<pre>show mac access-group [interface interface-id]</pre>	すべてのレイヤ2インターフェイスまたは指定されたレイヤ2インター フェイスに適用されている MAC アクセス リストを表示します。





Cisco IOS IP SLA 動作の設定

(注)

Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約)を使用するには、スイッチが LAN Base イメージを実行している必要があります。

この章では、Catalyst スイッチで Cisco IOS IP Service Level Agreement (SLA; サービス レベル契約) を使用する方法について説明します。Cisco IP SLA は Cisco IOS ソフトウェアの一部であり、シスコ のお客様は連続的で信頼性の高い確実な方法でトラフィックを生成するアクティブ トラフィック モニ タリングを行って IP アプリケーションとサービスの IP サービス レベルを分析し、ネットワーク パ フォーマンスを測定することができます。Cisco IOS SLA を使用すると、サービス プロバイダーのお 客様はサービス レベル契約の検討と提供、企業のお客様はサービス レベルの検証、外部委託している サービス レベル契約の検証、およびネットワーク パフォーマンスを把握することができます。Cisco IOS IP SLA は、ネットワーク アセスメントを実行することで QoS (Quality Of Service)の検証、新 しいサービス導入の簡易化、ネットワーク トラブルシューティングの補助を可能にします。

(注)

スイッチは、IP SLA responder の機能だけをサポートしているため、IP SLA 機能をすべてサポートしているデバイスにだけ設定する必要があります。

IP SLA の詳細については、次の URL で『Cisco IOS IP SLAs Configuration Guide, Release 12.4T』を 参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

コマンド構文情報については、次の URL でコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

この章で説明する内容は、次のとおりです。

- 「Cisco IOS IP SLA の概要」(P.32-2)
- 「IP SLA 動作の設定」(P.32-5)
- 「IP SLA 動作のモニタリング」(P.32-7)

Cisco IOS IP SLA の概要

CiscoIOS IP SLA はネットワークにデータを送信し、複数のネットワーク間あるいは複数のネットワー クパス内のパフォーマンスを測定します。ネットワーク データおよび IP サービスをシミュレーション し、ネットワーク パフォーマンス情報をリアル タイムで収集します。Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバ のようなリモート IP デバイスへのトラフィックを生成し、分析します。さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用され ます。

Cisco IOS IP SLA 動作に応じて Cisco デバイスのネットワーク パフォーマンス統計情報が監視され、 CLI (コマンドライン インターフェイス) MIB および SNMP (簡易ネットワーク管理プロトコル) MIB に格納されます。IP SLA パケットには設定可能な IP レイヤおよびアプリケーション レイヤのオ プションがあります。たとえば、発信元および宛先 IP アドレス、User Datagram Protocol (UDP; ユー ザデータグラム プロトコル) /TCP ポート番号、Type of Service (ToS; サービス タイプ) バイト (Differentiated Services Code Point [DSCP; DiffServ コード ポイント] および IP プレフィクス ビット を含む)、VPN Routing/Forwarding Instance (VRF; VPN ルーティング/転送インスタンス)、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作 を設定してエンド ユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のような一意のパフォーマンス メトリックのサブセットを収集します。

- 遅延(往復および一方向)
- ジッタ (方向性あり)
- パケット損失(方向性あり)
- パケットシーケンス (パケット順序)
- パス (ホップ単位)
- 接続(方向性あり)
- サーバまたは Web サイトのダウンロード時間

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Works Internetwork Performance Monitor (IPM) やサードパーティ製パフォーマンス管理製品などの Performance Monitoring (PM; パフォーマ ンス モニタリング) アプリケーションでも使用できます。Cisco IOS IP SLA を使用するネットワーク 管理製品については、次の URL を参照してください。

http://www.cisco.com/go/ipsla

IP SLA を使用すると次のような利点があります。

- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
 - ネットワーク内のジッタ、遅延、パケット損失が測定できる。
 - 連続的で信頼性のある確実な評価が提供される。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適して いることを確認できる。
- 端末間のネットワークアベイラビリティをモニタリングして、ネットワークリソースをあらかじ め検証し接続をテストできる(たとえば、ビジネス上の重要なデータを保存する NFS サーバの ネットワークアベイラビリティをリモートサイトから確認できる)。
- 信頼性の高い評価を連続的に行ってネットワーク動作のトラブルシューティングを行うので、問題 をすぐに特定しトラブルシューティングにかかる時間を短縮できる。

• Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) パフォーマンス モニタリングとネットワークの検証を行う (MPLS をサポートするスイッチの場合)。

ここでは、IP SLA 機能について説明します。

- •「Cisco IOS IP SLA によるネットワーク パフォーマンスの測定」(P.32-3)
- 「IP SLA の応答時間の計算」(P.32-4)

Cisco IOS IP SLA によるネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の 任意のエリア間のパフォーマンスを監視することができます。2 つのネットワーク デバイス間のネット ワーク パフォーマンスは、生成トラフィックで測定します。図 32-1 に、送信元デバイスが宛先デバイ スに生成パケットを送信するときに IP SLA が開始される手順を示します。宛先デバイスがパケットを 受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メト リックを算出します。IP SLA 動作は、特定のプロトコル (UDP など)を使用してネットワークの送信 元から宛先へのネットワーク測定を行います。



図 32-1 Cisco IOS IP SLA 動作

IP SLA ネットワーク パフォーマンス測定を実施する手順は次のとおりです。

- 1. 必要であれば、IP SLA responder をイネーブルにします。
- 2. 必要な IP SLA 動作タイプを設定します。
- 3. 指定された動作タイプのオプションを設定します。
- 4. 必要であれば、しきい値条件を設定します。
- 5. 動作の実行スケジュールを指定し、しばらく動作を実行して統計情報を収集します。
- **6.** Cisco IOS CLI を使用するか NMS (network management system; ネットワーク管理システム) と SNMP を併用して、動作の結果を表示し確認します。

IP SLA 動作について詳しくは、次の URL で『*Cisco IOS IP SLAs Configuration Guide*』で動作に関す る章を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12 4t/sla 12 4t book.html



スイッチでは、ゲートキーパー 登録遅延動作測定を使用する Voice over IP (VoIP) サービス レベルを サポートしません。IP SLA アプリケーションを設定する前に、show ip sla application 特権 EXEC コ マンドを使用してソフトウェア イメージで動作タイプがサポートされていることを確認してください。

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

IP SLA Responder は宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求 パケットを予想して応答します。Responder は専用プローブなしで正確な測定を行います。Responder は、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコル を通じて提供します。Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。

(注)

IP SLA 応答側には、LAN Base イメージを実行する Catalyst 2960 スイッチまたは IE3000 スイッチ、 あるいは IP Base イメージを実行する Catalyst 3560 スイッチまたは 3750 スイッチのような Cisco IOS レイヤ 2 の応答側に設定可能なスイッチを使用できます。responder は、IP SLA 機能を全面的にサポー トする必要はありません。

図 32-1 に、IP ネットワーク内での Cisco IOS IP SLA responder の配置場所を示します。responder は、 IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。コ ントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイ ネーブルにします。この間に、responder は要求を受け付け、応答します。responder は、IP SLA パ ケットに応答したあとまたは指定の時間が経過したら ポートをディセーブルにします。セキュリティ の向上のために、コントロール メッセージでは MD5 認証が利用できます。

すべての IP SLA 動作に対して宛先デバイスの responder をイネーブルにする必要はありません。たと えば、宛先ルータが提供しているサービス (Telnet や HTTP など) は responder では必要ありません。 他社製デバイスに IP SLA responder を設定することはできません。また、Cisco IOS IP SLA はこれら のデバイス固有のサービスに対してだけ動作パケットを送信できます。

IP SLA の応答時間の計算

スイッチとルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミ リ秒かかることがあります。この遅延により応答時間が影響を受けます。テストパケットの応答が処理 待ちのキューに入っていることもあるからです。この場合、応答時間は正しいネットワーク遅延を反映 しません。IP SLA はソース デバイスとターゲット デバイス (responder が使用されている場合)の処 理遅延を最小化し、正しい Round-Trip Time (RTT; ラウンドトリップ時間)を識別します。IP SLA テ スト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA responder がイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲット デバイスでタイム スタンプを付け、処理時間は含めません。タイム スタンプはサブミリ秒単位で構成されます。

図 32-2 に、responder の動作を示します。RTT を算出するためのタイム スタンプが 4 つ付けられます。 ターゲット ルータで responder 機能がイネーブルの場合、タイム スタンプ 3 (TS3) からタイム スタン プ 2 (TS2) を引いてテスト パケットの処理にかかった時間を求め、デルタ (Δ) で表します。次に全 体の RTT からこのデルタの値を引きます。IP SLA により、この方法はソース ルータにも適用されま す。その場合、着信タイム スタンプ 4 (TS4) が割り込みレベルで付けられ、より正確な結果を得るこ とができます。





この他にも、ターゲットデバイスに2つのタイムスタンプがあれば一方向遅延、ジッタ、方向性を持 つパケット損失がトラッキングできるという利点があります。大半のネットワーク動作は非同期なの で、このような統計情報があるのは問題です。ただし一方向遅延測定を取り込むには、ソースルータ とターゲットルータの両方に Network Time Protocol (NTP)を設定し、両方のルータを同じくロック ソースに同期させる必要があります。一方向ジッタ測定にはクロック同期は不要です。

IP SLA 動作の設定

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『Cisco IOS IP SLAs Configuration Guide』を参照してください。スイッチには応答側のサポートだけが含まれているため、この内容に含まれるのは応答側の設定手順だけです。

他の動作の設定に関する詳細は、次の URL で『Cisco IOS IP SLAs Configuration Guide』を参照して ください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

- ここでは、次の情報について説明します。
- •「デフォルト設定」(P.32-5)
- 「設定時の注意事項」(P.32-5)
- 「IP SLA Responder の設定」(P.32-6)

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA コマンドについては、次の URL で『*Cisco IOS IP SLAs Command Reference, Release 12.4T*』 のコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

詳細な説明と設定手順については、次の URL で『Cisco IOS IP SLAs Configuration Guide, Release 12.4T』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

IP SLA Responder の設定

IP SLA 応答側は、LAN Base イメージを実行している Catalyst 2960 スイッチ、Cisco ME 2400 スイッ チ、または IE 3000 スイッチのような、レイヤ 2 スイッチを含む Cisco IOS ソフトウェアベース デバ イスだけで利用可能です。レイヤ 2 スイッチは IP SLA 機能をすべてサポートしているわけではありま せん。特権 EXEC モードで、ターゲット デバイス(動作ターゲット)に IP SLA responder を設定する 手順は次のとおりです。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip sla responder { tcp-connect udp-echo } ipaddress <i>ip-address</i> port <i>port-number</i>	スイッチを IP SIA responder に設定します。
		オプションのキーワードの意味は次のとおりです。
		• tcp-connect : responder の TCP 接続動作をイネーブルにします。
		 udp-echo: responderの User Datagram Protocol (UDP; ユーザ データグラム プロトコル) エコー動作またはジッタ動作をイネー ブルにします。
		• ipaddress <i>ip-address</i> : 宛先 IP アドレスを入力します。
		• port <i>port-number</i> : 宛先ポート番号を入力します。
		(注) IP アドレスとポート番号は、IP SLA 動作のソース デバイスに 設定した IP アドレスおよびポート番号と一致している必要が あります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ip sla responder	デバイスの IP SLA responder 設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP SLA responder をディセーブルにするには、**no ip sla responder** グローバル コンフィギュレーショ ン コマンドを入力します。次に、デバイスを UDP ジッタ IP SLA 動作の responder に設定する例を示 します。UDP ジッタ IP SLA 動作については次の項で説明します。

Switch(config) # ip sla responder udp-echo 172.29.139.134 5000

(注)

IP SLA responder が機能するためには、Catalyst 3750 スイッチまたは Catalyst 3560 スイッチのよう な、IP サービス イメージを実行して IP SLA をすべてサポートしている送信元デバイスを設定する必 要があります。送信元デバイスの設定情報については、マニュアルを参照してください。

IP SLA 動作のモニタリング

表 32-1 に示すユーザ EXEC コマンドまたは特権 EXEC コマンドを使用して、IP SLA 動作の設定を表示します。

表 32-1 IP SLA 動作のモニタリング

コマンド	目的
show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla responder	IP SLA responder の情報を表示します。

■ IP SLA 動作のモニタリング





QoS の設定

この章では、自動 QoS (auto-QoS) コマンドまたは標準の Quality of Service (QoS) コマンドを使用 して Catalyst 2960 スイッチ上で QoS を設定する方法について説明します。QoS を使用すると、特定 のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、 スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し ます。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信 します。

QoS を設定できるのは物理ポートだけです。分類、キューイングおよびスケジューリングのような QoS が設定できます。また、ポートにポリシー マップも適用できます。

(注)

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

この章で説明する内容は、次のとおりです。

- 「QoS の概要」(P.33-2)
- 「自動 QoS の設定」(P.33-20)

▲ 自動 QoS を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 「自動 QoS 情報の表示」(P.33-30)
- 「標準 QoS の設定」(P.33-30)
- 「標準 QoS 情報の表示」(P.33-75)

スイッチは、Modular QoS Command Line Interface (MQC; モジュラ QoS コマンドライン インター フェイス) コマンドの一部をサポートします。MQC コマンドの詳細については、次の URL にアクセ スし「Modular Quality of Service Command-Line Interface Overview」を参照してください。

 $http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html$

QoS の概要

ネットワークは通常、ベストエフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生した場合に、廃棄される可能性についても、すべてのトラフィックで同じです。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのト ラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。 ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅 をより効率的に利用できるようになります。

QoS は、Internet Engineering Task Force (IETF) の新しい規格である Differentiated Services (DiffServ) アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入る ときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP Type of Service (ToS; サービス タイプ) フィールドの 6 ビットを使用して、分類 (クラス) 情報として伝達されます。分類情報をレイヤ 2 フ レームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて 説明します (図 33-1 を参照)。

• レイヤ2フレームのプライオリティビット

レイヤ2のISL (スイッチ間リンク) フレーム ヘッダーには、下位3ビットでIEEE 802.1p Class of Service (CoS; サービスクラス) 値を伝達する1バイトのユーザフィールドがあります。レイ ヤ2ISL トランクとして設定されたポートでは、すべてのトラフィックがISL フレームに収められ ます。

レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット (ユーザ プライオリティ ビット) で CoS 値が伝達されます。レイヤ 2 IEEE 802.1Q トラン クとして設定されたポートでは、ネイティブ VLAN のトラフィックを除くすべてのトラフィック が IEEE 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ2CoS値の範囲は、0(ロープライオリティ)~7(ハイプライオリティ)です。

• レイヤ3パケットのプライオリティビット



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

レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point (DSCP) 値の いずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちら の値も使用できます。

IP precedence 値の範囲は $0 \sim 7$ です。

DSCP 値の範囲は 0 ~ 63 です。

(注)

) IPv6 QoS はこのリリースでサポートされていません。

図 33-1 フレームおよびパケットにおける QoS 分類レイヤ

カプセル化されたパケット

レイヤ2 ヘッダー	IP ヘッダー	データ
--------------	---------	-----

レイヤ2ISL フレーム

(26 バイト) (24.5 KB) (4 バイト)	ISL ヘッダー カプセル化されたフレーム 1 FCS (26 バイト) (24.5 KB) (4 バイト)
----------------------------	--

└─3 ビットを CoS に使用

レイヤ 2 802.1Q および 802.1p フレーム

プリアンブル 開始フ 区切「	レーム リ文字 DA	SA	タグ	PT	データ	FCS
			T			

└──3 ビット(ユーザ プライオリティ ビット)を CoS に使用

レイヤ3IPv4パケット

バージョン 長	ToS (1 バイト)	長さ	ID	オフセット	TTL	プロトコル	FCS	IP-SA	IP-DA	データ	46974
	\uparrow		aadana	$a \pm t_{-1}$	+ 000	D					

└─ IP precedence または DSCP

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コアスイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てる リソースの容量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバ イスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作を させることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、 ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める 制御のきめ細かさによって、簡単にも複雑にもなります。

QoS の基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し(分類)、パケットがスイッ チを通過するときに所定の QoS を指定するラベルを割り当て、設定されたリソース使用率制限にパ ケットを適合させ(ポリシングおよびマーキング)、リソース競合が発生する状況に応じて異なる処理 (キューイングおよびスケジューリング)を行う必要があります。また、スイッチから送信されたトラ フィックが特定のトラフィック プロファイルを満たすようにする必要もあります(シェーピング)。

図 33-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポ リシング、マーキング、キューイング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを 識別します。詳細については、「分類」(P.33-5)を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不 適合かを判別します。ポリサーは、トラフィックフローで消費される帯域幅を制限します。その 判別結果がマーカーに渡されます。詳細については、「ポリシングおよびマーキング」(P.33-9)を 参照してください。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、 パケットの扱い(パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウン するか、またはパケットを廃棄するか)を決定します。詳細については、「ポリシングおよびマー キング」(P.33-9)を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを2つの入力キューのどちらに格納するかを選択します。キューイングは、輻輳回避メカニズムであるWeighted Tail-Drop(WTD)アルゴリズムによって拡張されます。しきい値を超過している場合、パケットは廃棄されます。詳細については、「キューイングおよびスケジューリングの概要」(P.33-13)を参照してください。
- スケジューリングでは、設定されている Shaped Round Robin (SRR)の重みに基づいて、キューを処理します。入力キューの1つがプライオリティキューです。共有が設定されている場合、 SRR はプライオリティキューを処理してから他のキューを処理します。詳細については、「SRR のシェーピングおよび共有」(P.33-14)を参照してください。

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベル および対応する DSCP または CoS 値を評価します。複数の入力ポートが1 つの出力ポートに同時 にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区 別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している 場合、パケットは廃棄されます。詳細については、「キューイングおよびスケジューリングの概要」 (P.33-13) を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの1つ(キュー1)は、他のキューの処理前に空になるまで 処理される緊急キューにできます。

図 33-2 QoS の基本モデル



分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS が スイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトで は、QoS はグローバルにディセーブルになっているため、分類は実行されません。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングお よびスケジューリング アクションを決定します。QoS ラベルは信頼設定およびパケット タイプに従っ てマッピングされます(図 33-3 (P.33-7)を参照)。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。非 IP トラフィックには、次の分類オプションを使用できます(図 33-3を参照)。

- 着信フレームの CoS 値を信頼します (ポートが CoS を信頼するように設定します)。次に、設定可能な CoS/DSCP マップを使用して、パケットの DSCP 値を生成します。レイヤ2の ISL フレーム ヘッダーは、1 バイトのユーザ フィールドの下位 3 ビットで CoS 値を伝達します。レイヤ2 IEEE 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0 (ロー プライオリティ) ~7 (ハイ プライオリティ)です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが 着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。 スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成し ます。
- 設定されたレイヤ2のMAC(メディアアクセス制御)Access Control List (ACL; アクセスコントロールリスト)に基づいて分類を実行します。レイヤ2のMACACLは、MAC送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットにはDSCPおよびCoS値として0が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACLが設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられるDSCPまたはCoS値が指定されます。

IP トラフィックには、次の分類オプションを使用できます(図 33-3を参照)。

 着信パケットの DSCP 値を信頼し (DSCP を信頼するようにポートを設定し)、同じ DSCP 値をパ ケットに割り当てます。IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義 しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ~ 63 です。

2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを 使用して、DSCP を別の値に変更できます。

- 着信パケットの IP precedence 値を信頼し(IP precedence を信頼するようにポートを設定し)、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP バージョン4 仕様では、1 バイトの ToS フィールドの上位3 ビットが IP precedence として定義されています。IP precedence 値の範囲は0(ロープライオリティ)~7(ハイプライオリティ)です。
- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
- 設定された IP 標準 ACL または IP 拡張 ACL (IP ヘッダーの各フィールドを調べる)に基づいて、 分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が 割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されて いる場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」(P.33-12)を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態による分類の設定」(P.33-35)を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段 階に送られます。



QoS ACL に基づく分類

(注)

スイッチで、LAN Lite イメージが実行されている場合、ACL を設定することはできますが、インター フェイスまたは VLAN に結合することはできません。

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グ ループ (クラス) を定義できます。QoS のコンテキストでは、Access Control Entry (ACE; アクセス コントロール エントリ)の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なり ます。

- 許可アクションとの一致が検出されると(最初の一致の原則)、指定の QoS 関連アクションが実行 されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの 一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。



アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルト で存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに 注意してください。

ACL でトラフィック クラスを定義したあとで、そのトラフィック クラスにポリシーを結合できます。 ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、 特定の集約としてクラスを分類する(DSCP を割り当てるなど) コマンドまたはクラスのレート制限を 実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートで ポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、access-list グローバル コンフィギュレーショ ン コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、mac access-list extended グローバル コンフィギュレーション コマンドを使用します。設定情報について は、「QoS ポリシーの設定」(P.33-43)を参照してください。

クラス マップおよびポリシー マップに基づく分類

(注)

ポリシーマップを使用するには、スイッチが LAN Base イメージを実行している必要があります。

クラス マップは、特定のトラフィック フロー(またはクラス)に名前を付けて、他のすべてのトラ フィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定 のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グ ループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができま す。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用で きます。パケットをクラス マップ条件と照合したあとで、ポリシー マップを使用してさらに分類しま す。 ポリシー マップでは、作用対象のトラフィック クラスを指定します。トラフィック クラスの CoS、 DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適合な 場合の対処法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、 ポートにポリシー マップを結合しなければなりません。

クラス マップを作成するには、class-map グローバル コンフィギュレーション コマンドまたは class ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する 場合には、class-map コマンドを使用する必要があります。class-map コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、match クラス マップ コンフィ ギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

ポリシー マップは、policy-map グローバル コンフィギュレーション コマンドを使用して作成し、名 前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始さ れます。このモードでは、class、trust、または set ポリシー マップ コンフィギュレーション コマンド およびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック ク ラスに対して実行するアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクション を定義する police および police aggregate ポリシー マップ クラス コンフィギュレーション コマンドを 含めることもできます。

ポリシー マップをイネーブルにするには、service-policy インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

詳細については、「ポリシングおよびマーキング」(P.33-9)を参照してください。設定情報については、「QoS ポリシーの設定」(P.33-43)を参照してください。

ポリシングおよびマーキング

(注)

ポリシングおよびマーキングを使用するには、スイッチが LAN Base イメージを実行している必要があります。

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てたあとで、ポリシング およびマーキング プロセスを開始できます(図 33-4 を参照)。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパ ケットは、「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、 パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パ ケットを変更しないで通過させるアクション、パケットを廃棄するアクション、またはパケットに割り 当てられた DSCP 値を変更(マークダウン)してパケットの通過を許可するアクションなどがありま す。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベ ルが設定されます。ポリシング済み DSCP マップの詳細については、「マッピング テーブル」 (P.33-12)を参照してください。マークダウンされたパケットは、元の QoS ラベルと同じキューを使 用して、フロー内のパケットの順番が崩れないようにします。

(注)

すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を 受けます(ポリサーが設定されている場合)。その結果、ブリッジングされたパケットは、ポリシング またはマーキングが行われたときに廃棄されたり、DSCP または CoS フィールドが変更されたりする ことがあります。

ポリシングは物理ポートだけに設定できます。物理ポートのポリシング設定の詳細については、「物理 ポートのポリシング」(P.33-10)を参照してください。 ポリシー マップおよびポリシング アクションを設定したあとで、service-policy インターフェイス コ ンフィギュレーション コマンドを使用して、入力ポートにポリシーを統合します。詳細については、 「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」 (P.33-49) および「集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング」 (P.33-54) を参照してください。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

- Individual: QoS はポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々 に適用します。このタイプのポリサーは、police ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- Aggregate: QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに 累積的に適用します。このタイプのポリサーは、police aggregate ポリシー マップ クラス コン フィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することに より設定します。ポリサーの帯域幅限度を指定するには、mls qos aggregate-policer グローバル コンフィギュレーション コマンドを使用します。このようにして、集約ポリサーはポリシー マッ プ内にある複数のトラフィック クラスで共有されます。

ポリシングは、トークン バケット アルゴリズムを使用します。各フレームがスイッチに着信すると、 バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指 定されたレート(ビット/秒)で送信されます。バケットにトークンが追加されるたびに、スイッチ は、バケット内に十分なスペースがあるかを確認します。十分なスペースがなければ、パケットは不適 合とマーキングされ、指定されたポリサー アクション(廃棄またはマークダウン)が実行されます。

バケットが満たされる速度は、バケット深度(burst-byte)、トークンが削除されるレート(rate-bps)、 および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に 上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場 合、バケットはオーバーフローせず、トラフィックフローに何のアクションも実行されません。ただ し、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレーム に対してポリシング アクションが実行されます。

バケット深度(バケットがオーバーフローするまでに許容される最大バースト)を設定するには、 police ポリシーマップ クラス コンフィギュレーション コマンドまたは mls qos aggregate-policer グ ローバル コンフィギュレーション コマンドの burst-byte オプションを使用します。トークンがバケッ トから削除されるレート(平均レート)を設定するには、police ポリシーマップ クラス コンフィギュ レーション コマンドまたは mls qos aggregate-policer グローバル コンフィギュレーション コマンドの rate-bps オプションを使用します。 図 33-4 に、ポリシングおよびマーキングのプロセスを示します。





マッピング テーブル

(注)

マッピング テーブルを使用するには、スイッチが LAN Base イメージを実行している必要があります。

QoS を処理している間、すべてのトラフィック(非 IP トラフィックを含む)のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、 CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するに は、mls qos map cos-dscp および mls qos map ip-prec-dscp グローバル コンフィギュレーション コマンドを使用します。

DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。こ のマップを設定するには、mls qos map dscp-mutation グローバル コンフィギュレーション コマ ンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます(パケットが不適合で、マークダウン値がポリサーによって指定されている場合)。この設定可能なマップは、ポリシング済み DSCP マップといいます。このマップを設定するには、mls qos map policed-dscp グローバル コンフィギュレーション コマンドを使用します。
- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出 カキューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいてお り、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用し てキューを選択します。入力または出力のキューに加えて、QOS ラベルは WTD しきい値も識別 します。これらのマップを設定するには、mls qos srr-queue {input | output } dscp-map および mls qos srr-queue {input | output } cos-map グローバル コンフィギュレーション コマンドを使用 します。

CoS/DSCP、DSCP/CoS、および **IP** precedence/DSCP マップのデフォルト値は、使用しているネット ワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマッ プです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。 DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。その他のすべてのマップは スイッチ全体に適用されます。

設定情報については、「DSCP マップの設定」(P.33-56)を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「入力キューでのキューイングおよび スケジューリング」(P.33-15)を参照してください。DSCP および CoS 出力キューしきい値マップの 詳細については、「出力キューでのキューイングおよびスケジューリング」(P.33-17)を参照してくだ さい。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立てます(図 33-5 を参照)。

図 33-5 入力および出力キューの位置



すべてのポートの入力帯域幅の合計が内部リングの帯域幅を超えることがあるため、入力キューはパ ケットの分類、ポリシング、およびマーキングのあと、パケットがスイッチファブリックに転送され る前の位置に配置されています。複数の入力ポートから1つの出力ポートに同時にパケットが送信され て、輻輳が発生することがあるため、出力キューは内部リングのあとに配置されています。

WTD



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

入力および出力キューは両方とも、WTD と呼ばれるテールドロップ輻輳回避メカニズムの拡張バー ジョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとに廃棄優先順位を設定し たりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを 使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると(宛先 キューの空きスペースがフレーム サイズより小さくなると)、フレームは廃棄されます。

各キューには3つのしきい値があります。QOS ラベルは、3つのしきい値のうちのどれがフレームの 影響を受けるかを決定します。3つのしきい値のうち、2つは設定可能(明示的)で、1つは設定不可 能(暗示的)です。

図 33-6 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。廃棄割合は次のように設定されています。40%(400 フレーム)、60%(600 フレーム)、および 100%(1000 フレーム) です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は 最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当 てられます(キューフル ステート)。CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ~ 3 は 40% し きい値に割り当てられます。 600 個のフレームが格納されているキューに、新しいフレームが着信したとします。このフレームの CoS 値は4 および5 で、60% のしきい値が適用されます。このフレームがキューに追加されると、し きい値を超過するため、フレームは廃棄されます。



 $\begin{array}{c} \underline{\text{CoS } 6 \sim 7} \\ \underline{\text{CoS } 4 \sim 5} \\ \underline{\text{CoS } 0 \sim 3} \\ \end{array} \begin{array}{c} 60\% \\ 40\% \end{array} \begin{array}{c} 600 \\ 400 \\ 0 \end{array}$

詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」 (P.33-62)、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」 (P.33-68)、および「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.33-70)を参照 してください。

36692

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されま す。入力キューでは、SRR によってパケットが internal リングに送信されます。出力キューでは、 SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有が デフォルト モードであり、これ以外のモードはサポートされていません。

シェーピングモードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。 シェーピングされたトラフィックの場合は、リンクがアイドルの場合も、割り当てを超える帯域幅は使 用されません。シェーピングを使用すると、時間あたりのトラフィックフローがより均一になり、 バーストトラフィックの最高時と最低時を削減します。シェーピングの場合は、各重みの絶対値を使 用して、キューに使用可能な帯域幅が計算されます。

共有モードでは、各キューは設定された重みに従って帯域幅を共有します。帯域幅に対してはこのレベ ルが保証されますが、このレベルに限定されるわけではありません。たとえば、特定のキューが空であ り、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共 有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関 係ありません。シェーピングおよび共有は、インターフェイスごとに設定されます。各インターフェイ スは、一意に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」(P.33-65)、「出力キューでの SRR シェーピング 重みの設定」(P.33-71)、および「出力キューでの SRR 共有重みの設定」(P.33-72)を参照してくださ い。

入力キューでのキューイングおよびスケジューリング

図 33-7 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

```
図 33-7 入力ポートのキューイングおよびスケジューリング フローチャート
```



(注)

共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってのみ処理される、設定可能な入力キューを 2 つサポートして います。表 33-1 にこれらのキューの説明を示します。

表 33-1 入力キューのタイプ

キュー タイプ 1	准治:
	122.46
標準	標準プライオリティと見なされるユーザ トラフィック。各フローを区別するために、3 つの異なるしきい値 を設定できます mls gos srr-queue input threshold mls gos srr-queue input dscp-man お上びmls gos
	2 RAC (e 2 7 ° mis dos si i-ducue input un esnoru, mis dos si i-ducue input usep-map, 40 2 ° mis dos
	srr-queue input cos-map グローバル コンフィギュレーション コマンドを使用できます。
緊急	Differentiated Services (DF) 緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラ
	フィック。このトラフィックに必要な帯域幅は mls qos srr-queue input priority-queue グローバル コン
	フィギュレーション コマンドを使用して、合計トラフィックの割合として設定できます。緊急キューには帯
	域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが2つ使用されます。これらのキューは、ネットワークを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。mls qos srr-queue input dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8 }、ま たは mls qos srr-queue input cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8 } グローバル コンフィギュレーション コマンドを使用します。DSCP 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、show mls qos maps 特権 EXEC コマンドを使用しま す。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサポートします。各キュー には 3 つのドロップしきい値があります。そのうちの 2 つは設定可能(*明示的*) な WTD しきい値で、 もう 1 つはキューフル ステートに設定済みの設定不可能(*暗示的*) なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合(しきい値 ID 1 および ID 2 用)を割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* グローバル コンフィ ギュレーション コマンド を使用します。各しきい値は、キューに割り当てられたバッファの合計値に 対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更でき ません。WTD の仕組みの詳細については、「WTD」(P.33-13) を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する(スペース量を割り当てる)には、mls qos srr-queue input buffers percentage1 percentage2 グローバル コンフィギュレーション コマンドを使用 します。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットが廃棄される前に バッファに格納して送信できるデータ量が制御されます。帯域幅を割合として割り当てるには、mls qos srr-queue input bandwidth weight1 weight2 グローバル コンフィギュレーション コマンドを使用 します。重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、mls qos srr-queue input priority-queue queue-id bandwidth weight グローバル コンフィギュレーション コマンドを使用しま す。プライオリティ キューは internal リングの負荷に関わらず帯域幅の一部が保証されているため、 確実な配信を必要とするトラフィック(音声など)に使用する必要があります。

SRR は mls qos srr-queue input priority-queue *queue-id* bandwidth *weight* グローバル コンフィギュ レーション コマンドの bandwidth キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は mls qos srr-queue input bandwidth *weight1 weight2* グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キュー と共有し、キューを処理します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定の キューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライ オリティが低いパケットが廃棄されるようにキューのしきい値を調整したりして、トラフィックのプラ イオリティを設定できます。設定情報については、「入力キューの特性の設定」(P.33-62)を参照して ください。
出力キューでのキューイングおよびスケジューリング

図 33-8 に、出力ポートのキューイングおよびスケジューリングフローチャートを示します。

緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の3つのキューが処理されます。



図 33-8 出力ポートのキューイングおよびスケジューリング フローチャート

各ポートは、そのうち1つ(キュー1)を出力緊急キューにできる、4つの出力キューをサポートしています。これらのキューは、キューセットごとに設定されます。出力ポートから脱退するすべてのトラフィックは、パケットに割り当てられた QoS ラベルに基づいて、これらの4つのキューのいずれかを通過し、しきい値の影響を受けます。

図 33-9 に出力キュー バッファを示します。バッファ スペースは共通プールと専用プールからなりま す。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保しま す。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューの バッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかが制 御されます。スイッチは、目的のキューが確保された量(限度内)を超えるバッファを消費していない かどうか、最大バッファ(限度超)をすべて消費しているかどうか、および共通プールが空である(空 きバッファなし)か、または空でない(空きバッファあり)かを検出します。キューが限度を超えてい ない場合、スイッチは専用プールまたは共通プール(空でない場合)からバッファ スペースを割り当 てます。共通プールに空きバッファがない場合、またはキューが限度を超えている場合は、フレームが 廃棄されます。



図 33-9 出力キューのバッファ割り当て

バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り 当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンド を使用します。各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定する には、**mls qos queue-set output** *qset-id* **buffers** *allocation1* ... *allocation4* グローバル コンフィギュ レーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。 残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティトラフィックを確実にバッファに格納できます。た とえば、バッファスペースが400の場合、バッファスペースの70%をキュー1に割り当てて、10% をキュー2~4に割り当てることができます。キュー1には280のバッファが割り当てられ、キュー2 ~4にはそれぞれ40バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。たとえば、 キュー用として 100 バッファがある場合、50%(50 バッファ)を確保できます。残りの 50 バッファは 共通プールに戻されます。また、最大しきい値を設定することにより、一杯になったキューが確保量を 超えるバッファを取得できるようにすることもできます。共通プールが空でない場合、必要なバッファ を共通プールから割り当てることができます。

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力 キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングしま す。**mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8* }、または **mls** qos srr-queue output cos-map queue *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8* } グローバル コンフィギュレーション コマンドを使用します。DSCP 出力 キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特 権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサポートします。各キュー には 3 つのドロップしきい値があります。そのうちの 2 つは設定可能(*明示的*)な WTD しきい値で、 もう 1 つはキューフル ステートに設定済みの設定不可能(*暗示的*)なしきい値です。しきい値 ID 1 お よび ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値は、 キューフル ステートに設定済みで、変更できません。キューセットにポートをマッピングするには、 **queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。WTD しきい値 の割合を変更するには、キューセット設定を変更します。WTD の仕組みの詳細については、「WTD」 (P.33-13)を参照してください。

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。ポートに共有重みまた はシェーピング重みを割り当てるには、srr-queue bandwidth share weight1 weight2 weight3 weight4 または srr-queue bandwidth shape weight1 weight2 weight3 weight4 インターフェイス コンフィギュ レーション コマンドを使用します。シェーピングと共有の違いについては、「SRR のシェーピングおよ び共有」(P.33-14) を参照してください。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットが廃棄される前にバッファに 格納して送信できるデータ量が制御されます。重みの比率は、SRR スケジューラが各キューからパ ケットを送信する頻度の比率です。

緊急キューがイネーブルでないかぎり、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域 幅重みは無視されて比率計算に使用されません。緊急キューはプライオリティ キューであり、処理さ れて空になってから、他のキューが処理されます。緊急キューをイネーブルにするには、 priority-queue out インターフェイス コンフィギュレーション コマンドを使用します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定の キューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライ オリティが低いパケットが廃棄されるようにキューのしきい値を調整したりして、トラフィックのプラ イオリティを設定できます。設定情報については、「出力キューの特性の設定」(P.33-67)を参照して ください。



ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、 次のようにパケットが変更されることがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます(これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合)。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、このあとの段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されないで、 DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポー トが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されない で、CoS/DSCP マップに従って DSCP が変更されることがあります。

入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。ポリ シー マップの設定アクションによっても、DSCP が書き換えられます。

自動 QoS の設定

<u>へ</u> (注)

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

自動 QoS 機能を使用して、既存の QoS 機能の配置を容易にできます。自動 QoS では、ネットワーク 設計について前提条件を設定し、その結果スイッチは、デフォルトの QoS 動作を使用せずに、各トラ フィック フローについて優先度を指定して入力および出力キューを適切に使用できるようになります (デフォルトで自動 QoS はディセーブルになっています。したがって、スイッチはパケットの内容やサ イズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送 信します)。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラ フィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

自動 QoS コマンドを使用して Cisco IP Phone、および Cisco SoftPhone アプリケーションを実行する デバイスに接続するポートを指定します。また、アップリンクを介して信頼のおけるトラフィックを受 信するポートを指定します。自動 QoS は以下の機能を実行します。

- Cisco IP Phone の有無の検出
- QoS 分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- 「生成される自動 QoS 設定」(P.33-21)
- 「コンフィギュレーションにおける自動 QoS の影響」(P.33-26)
- 「自動 QoS 設定時の注意事項」(P.33-26)
- 「VoIP 用自動 QoS のイネーブル化」(P.33-27)
- 「自動 QoS 設定例」(P.33-28)

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。

自動 QoS がイネーブルの場合、入力パケット ラベルを使用してトラフィックを分類し、パケット ラベルを割り当て、入力および出力キューを設定します(表 33-2 を参照)。

表 33-2 トラフィック タイプ、パケット ラベル、キュー

	VolP ¹ データ トラフィック	VoIP 制御 トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他のトラフィック
DSCP	46	24, 26	48	56	34	_
CoS	5	3	6	7	4	_
CoS/入力 キューマップ	2, 3, 4, 5, 6, 7 $(\pm 2 - 2)$ 0, 1 $(\pm 2 - 1)$					0、1 (キュー1)
CoS /出力 キュー マップ	$5 (\pm 2 - 1) 3, \ 6, \ 7 (\pm 2 - 2) \qquad 4 (\pm 2 - 3)$			$ \begin{array}{cccc} 2 & 0, 1 \\ (\pm 2 - 3) & (\pm 2 - 4) \end{array} $		

1. VoIP = Voice over IP

表 33-3 に、入力キューに対して生成される自動 QoS 設定を示します。

表 33-3 入力キューの自動 QoS 設定

			キュー重み	キュー(バッファ)
入力キュー	キュー番号	CoS/キュー マップ	(帯域幅)	サイズ
SRR 共有	1	0, 1	81%	67%
プライオリティ	2	2, 3, 4, 5, 6, 7	19%	33%

表 33-4 に、出力キューに対して生成される自動 QoS 設定を示します。

表 33-4 出力キューの自動 QoS 設定

		CoS/	キュー重み	ギガビット対応ポートの	10/100 イーサネット ポートの
出力キュー	キュー番号	キュー マップ	(帯域幅)	キュー(バッファ)サイズ	キュー(バッファ)サイズ
プライオリティ	1	5	最大 100%	16%	10%
SRR 共有	2	3, 6, 7	10%	6%	10%
SRR 共有	3	2, 4	60%	17%	26%
SRR 共有	4	0, 1	20%	61%	54%

自動 QoS 機能を最初のポートでイネーブルにすると、以下の動作が自動的に発生します。

- QoSは、グローバルにイネーブル(mls qos グローバル コンフィギュレーション コマンド)になり、他のグローバル コンフィギュレーション コマンドが追加されます。
- auto qos voip cisco-phone インターフェイス コンフィギュレーション コマンドを Cisco IP Phone が接続されたネットワーク エッジにあるポートに入力すると、スイッチは信頼境界機能をイネー ブルにします。スイッチは、Cisco Discovery Protocol (CDP) を使用して Cisco IP Phone の有無 を検出します。Cisco IP Phone が検出されたら、ポートの入力分類がパケットで受信される QoS ラベルを信頼するように設定されます。またスイッチは、ポリシングを使用して、パケットがイン プロファイルかアウト オブ プロファイルかを判別し、パケットに対するアクションを指定します。 パケットに 24、26、または 46 の DSCP 値がない場合、またはパケットが適合外の場合、スイッチ は DSCP 値を 0 に変更します。Cisco IP Phone がなければ、パケットで入力分類が QoS ラベルを 信用しないように設定されます。スイッチは、表 33-3 および表 33-4 の設定に従ってポート上の入 力および出力キューを設定します。スイッチで信頼境界機能がイネーブルになる前に、ポリシング がポリシー マップ分類と一致するトラフィックに適用されます。
- auto qos voip cisco-softphone インターフェイス コンフィギュレーション コマンドを、Cisco SoftPhone を稼動するデバイスに接続されたネットワークのエッジのポートに入力すると、スイッ チはポリシングを使用して、パケットがプロファイルの内部または外部にいるかを判断し、パケッ ト上のアクションを指定します。パケットに 24、26、または 46 の DSCP 値がない場合、またはパ ケットが適合外の場合、スイッチは DSCP 値を 0 に変更します。スイッチは、表 33-3 および 表 33-4 の設定に従ってポート上の入力および出力キューを設定します。
- ネットワーク内部に接続されたポート上で auto qos voip trust インターフェイス コンフィギュ レーション コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値が信頼 されます(前提条件は、トラフィックがすでに他のエッジ デバイスによって分類されていること です)。スイッチは、表 33-3 および表 33-4 の設定に従ってポート上の入力および出力キューを設 定します。

信頼境界機能の詳細については、「ポート セキュリティを確保するための信頼境界機能の設定」 (P.33-39)を参照してください。

auto qos voip cisco-phone、auto qos voip cisco-softphone、または auto qos voip trust インターフェ イス コンフィギュレーション コマンドを使用して自動 QoS をイネーブルにする場合、スイッチはトラ フィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、表 33-5 にリストさ れているコマンドをポートに適用します。

	自動的に生成されるコマンド
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ(着信パケットの CoS 値の DSCP 値へのマッピング) を設定します。	Switch(config)# mls qos Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	<pre>Switch(config)# no mls qos srr-queue input cos-map Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 3 0 Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 1 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 1 2 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7 Switch(config)# mls qos srr-queue input cos-map queue 2 threshold 3 3 5</pre>

表 33-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config) # no mls qos srr-queue output cos-map Switch(config) # mls qos srr-queue output cos-map queue 1 threshold 3 5 Switch(config) # mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7 Switch(config) # mls qos srr-queue output cos-map queue 3 threshold 3 2 4 Switch(config) # mls qos srr-queue output cos-map queue 4 threshold 2 1 Switch(config) # mls qos srr-queue output cos-map queue 4 threshold 2 1
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config) # no mls qos srr-queue input dscp-map Switch(config) # mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15 Switch(config) # mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7 Switch(config) # mls qos srr-queue input dscp-map queue 1 threshold 3 32 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config) # mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config) # no mls qos srr-queue output dscp-map Switch(config) # mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47 Switch(config) # mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31 Switch(config) # mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 Switch(config) # mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63 Switch(config) # mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23 Switch(config) # mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39 Switch(config) # mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch(config) # mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch(config) # mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15 Switch(config) # mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7

表 33-5 生成される自動 QoS 設定 (続き)

	自動的に生成されるコマンド
スイッチが自動的に入力キューを設定します。キュー2がプ ライオリティ キューでキュー1 が共有モードです。また、ス イッチは、入力キューの帯域幅とバッファ サイズも設定しま す。	<pre>Switch(config) # no mls qos srr-queue input priority-queue 1 Switch(config) # no mls qos srr-queue input priority-queue 2 Switch(config) # mls qos srr-queue input bandwidth 90 10 Switch(config) # mls qos srr-queue input threshold 1 8 16 Switch(config) # mls qos srr-queue input threshold 2 34 66 Switch(config) # mls qos srr-queue input buffers 67 33</pre>
スイッチが自動的に出力キューのバッファ サイズを設定しま す。ポートにマッピングされた出力キューの帯域幅と SRR モード (シェーピングまたは共有) を設定します。	Switch (config) # mls qos queue-set output 1 threshold 1 138 138 92 138 Switch (config) # mls qos queue-set output 1 threshold 2 138 138 92 400 Switch (config) # mls qos queue-set output 1 threshold 3 36 77 100 318 Switch (config) # mls qos queue-set output 1 threshold 4 20 50 67 400 Switch (config) # mls qos queue-set output 2 threshold 1 149 149 100 149 Switch (config) # mls qos queue-set output 2 threshold 2 118 118 100 235 Switch (config) # mls qos queue-set output 2 threshold 3 41 68 100 272 Switch (config) # mls qos queue-set output 2 threshold 4 42 72 100 242 Switch (config) # mls qos queue-set output 1 buffers 10 10 26 54 Switch (config) # mls qos queue-set output 2 buffers 16 6 17 61 Switch (config-if) # priority-que out Switch (config-if) # srr-queue bandwidth share 10 10 60 20
auto qos voip trust コマンドを入力すると、スイッチは mls qos trust cos コマンドを使用して、非ルーテッド ポート上で 自動的に入力分類をパケット内で受信する、信頼する CoS 値 へ設定します。	Switch(config-if)# mls qos trust cos Switch(config-if)# mls qos trust dscp
auto qos voip cisco-phone コマンドを入力すると、スイッチ が自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。	Switch(config-if)# mls qos trust device cisco-phone

表 33-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド
auto qos voip cisco-softphone コマンドを入力すると、ス イッチが自動的にクラス マップおよびポリシー マップを作成 します。	Switch(config) # mls qos map policed-dscp 24 26 46 to 0 Switch(config) # class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap) # match ip dscp ef Switch(config) # class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap) # match ip dscp cs3 af31 Switch(config) # policy-map AutoQoS-Police-SoftPhone Switch(config-pmap) # class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c) # set dscp ef Switch(config-pmap-c) # police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap-c) # set dscp cs3 Switch(config-pmap-c) # set dscp cs3 Switch(config-pmap-c) # police 32000 8000 exceed-action policed-dscp-transmit
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ(別名 <i>AutoQoS-Police-SoftPhone</i>) を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルで ある入力インターフェイスに適用します。	Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
auto qos voip cisco-phone コマンドを入力すると、スイッチ が自動的にクラス マップおよびポリシー マップを作成しま す。	<pre>witch(config)# mls qos map policed-dscp 24 26 46 to 0 Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust Switch(config-cmap)# match ip dscp ef Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust Switch(config-cmap)# match ip dscp cs3 af31 Switch(config)# policy-map AutoQoS-Police-CiscoPhone Switch(config)# policy-map AutoQoS-Police-CiscoPhone Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust Switch(config-pmap-c)# set dscp ef Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust Switch(config-pmap-c)# set dscp cs3 Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit</pre>
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ(別名 <i>AutoQoS-Police-CiscoPhone</i>) を、Cisco Phone 機能を備えた自動 QoS がイネーブルである 入力インターフェイスに適用します。	Switch(config-if)# service-policy input AutoQoS-Police-CiscoPhone

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになると、auto qos voip インターフェイス コンフィギュレーション コマンド および生成された設定が実行コンフィギュレーションに追加されます。

スイッチは、自動 QoS が生成したコマンドを、CLI から入力したように適用します。既存のユーザ設 定により、生成コマンドのアプリケーションに障害が発生したり、生成コマンドによってユーザ設定が 上書きされたりする可能性があります。これらの動作は警告なしに発生します。すべての生成コマンド が正常に適用された場合、上書きされていないユーザ入力設定が実行コンフィギュレーションに残りま す。上書きされたユーザ入力設定は、現在の設定をメモリに保存することなく、スイッチをリロードす ることで取得できます。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが 復元されます。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- 自動 QoS は、非ルーテッド ポートおよびルーテッド ポートで Cisco IP Phone に VoIP のスイッチ を設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼動するデバイスの VoIP 用にスイッチを設定します。
- Cisco SoftPhone を稼動するデバイスが非ルーテッドポートまたはルーテッドポートに接続されている場合、スイッチはポート単位で Cisco SoftPhone アプリケーション1つのみをサポートします。
- Cisco IOS Release 12.2(40)SE、Auto-Qos VoIP では出力インターフェイスに対して priority-queue インターフェイス コンフィギュレーション コマンドが使用されます。ポリシー マップおよび信頼できるデバイスを Cisco IP Phone の同一インターフェイス上に設定することも可 能です。
- スイッチ ポートが Cisco IOS Release 12.2(37)SE かそれよりも前のリリースで auto qos voip cisco-phone インターフェイス コンフィギュレーション コマンドを使用して設定された場合、 auto-QoS によって Cisco IOS Release 12.2(40)SE に新しく生成されたコマンドは、ポートに適用 されません。このようなコマンドを自動的に適用するには、設定を削除してからポートに再度適用 する必要があります。
- 自動 QoS のデフォルト設定を利用する場合、他の QoS コマンドを実行する前に自動 QoS をイ ネーブルにする必要があります。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了し たあとにのみ調整することを推奨します。詳細については、「コンフィギュレーションにおける自 動 QoS の影響」(P.33-26)を参照してください。
- 自動 QoS をイネーブルにしたら、名前に AutoQoS が含まれているポリシー マップまたは集約ポリ サーを変更しないでください。ポリシー マップまたは集約ポリサーを変更する必要がある場合、 これらをコピーしてから、コピーしたポリシー マップまたは集約ポリサーを変更してください。 生成したポリシー マップではなくこの新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除し、新しいポリシー マップをインターフェイスに適用します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランクポートでイネーブルにできます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。
- ルーテッドポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- 接続したデバイスは、Cisco Call Manager バージョン 4 以降を使用する必要があります。

VoIP 用自動 QoS のイネーブル化

QoS ドメイン内で VoIP 用の自動 QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行 します。

	コマンド	目的			
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。			
ステップ 2	interface interface-id	Cisco IP Phone に接続されたポート、Cisco SoftPhone 機能を実 行するデバイスに接続されたポート、またはネットワーク内部の 信頼性のある他のスイッチやルータに接続されたアップリンク ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。			
ステップ 3	auto qos voip {cisco-phone	自動 QoS をイネーブルにします。			
	cisco-softphone trust}	 キーワードの意味は次のとおりです。 cisco-phone: ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話が検出された場合のみ信頼されます。 			
		 cisco-softphone:ポートが Cisco SoftPhone 機能を実行する デバイスに接続されています。 			
		 trust:アップリンク ポートが信頼性のあるスイッチまたは ルータに接続されていて、入力パケットの VoIP トラフィッ ク分類が信頼されています。 			
ステップ 4	end	特権 EXEC モードに戻ります。			
ステップ 5	show auto qos interface interface-id	設定を確認します。			
		このコマンドは、自動 QoS がイネーブルであるインターフェイ ス上の自動 QoS コマンドを表示します。自動 QoS 設定および ユーザの変更を表示するには、show running-config 特権 EXEC コマンドを使用します。			

自動 QoS のイネーブルまたはディセーブル時に自動的に生成された QoS コマンドを表示するには、自 動 QoS をイネーブルにする*前*に、debug auto qos 特権 EXEC コマンドを入力します。詳細について は、このリリースに対応するコマンド リファレンスにある debug autoqos コマンドの項を参照してく ださい。

ポートで自動 QoS をディセーブルにするには、no auto qos voip インターフェイス コンフィギュレー ション コマンドを使用します。このポート用に自動 QoS が生成したインターフェイス コンフィギュ レーション コマンドのみが削除されます。これが自動 QoS をイネーブルにしている最後のポートの場 合に、no auto qos voip コマンドを入力すると、自動 QoS 生成グローバル コンフィギュレーション コ マンドが残っていても、(グローバル コンフィギュレーションによって他のポートのトラフィックを中 断しないように) 自動 QoS はディセーブルであると見なされます。

自動 QoS 生成グローバル コンフィギュレーション コマンドをディセーブルにするには、no mls qos グ ローバル コンフィギュレーション コマンドを使用します。QoS がディセーブルになると、パケット (パケットの CoS 値、DSCP 値、および IP precedence 値) は変更されないため、trusted (信頼性のあ る) ポート、または untrusted (信頼性のない) ポートの概念はありません。トラフィックはパスス ルー モードでスイッチングされます (書き換えられずにスイッチングされ、ポリシングを伴わないベ ストエフォート型として分類されます)。 次に、ポートに接続されたスイッチまたはルータが信頼性のあるデバイスである場合に、自動 QoS を イネーブルにして着信パケットで受信された QoS ラベルを信頼する例を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust

自動 QoS 設定例

ここでは、自動 QoS をネットワークに実装する方法について説明します(図 33-10 を参照)。QoS パフォーマンスを最適にするには、ネットワーク内部のデバイスすべてで自動 QoS をイネーブルにします。



図 33-10 ネットワークでの自動 QoS の設定例

図 33-10 に、VoIP トラフィックを他のすべてのトラフィックに優先するネットワークを示します。 QoS ドメインの端にあるワイヤリング クローゼットのスイッチで、自動 QoS がイネーブルとなってい ます。



自動 QoS コマンドを入力する前に標準 QoS コマンドを設定しないでください。QoS 設定を微調整できますが、自動 QoS が完了したあとにのみ調整することを推奨します。

QoS ドメインのエッジにあるスイッチで VoIP トラフィックを他のトラフィックより優先させるように 設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	debug auto qos	自動 QoS のデバッグをイネーブルにします。デバッグをイネーブルにする と、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	cdp enable	CDP をグローバルにイネーブルにします。デフォルトではイネーブルに設 定されています。
ステップ 4	interface interface-id	Cisco IP Phone に接続するスイッチ ポートを指定し、インターフェイス コ ンフィギュレーション モードを開始します。
ステップ 5	auto qos voip cisco-phone	ポート上で自動 QoS をイネーブルにし、そのポートが Cisco IP Phone に接 続されるように指定します。
		着信パケットの QoS ラベルは、Cisco IP Phone が検出された場合のみ信頼 されます。
ステップ 6	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7		Cisco IP Phone に接続されているポートの数だけ、ステップ 4 ~ 6 を繰り 返します。
ステップ 8	interface interface-id	信頼性のあるスイッチまたはルータに接続していると認識されるスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始 します。図 33-10を参照してください。
ステップ 9	auto qos voip trust	ポート上で自動 QoS をイネーブルにし、そのポートが信頼性のあるルータ またはスイッチに接続されるように指定します。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show auto qos	設定を確認します。
		このコマンドは、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定およびユーザの変更を表示する には、show running-config 特権 EXEC コマンドを使用します。
		自動 QoS によって影響される QoS 設定の詳細については、「自動 QoS 情報の表示」(p.28-30)を参照してください。
ステップ 12	copy running-config startup-config	auto qos voip インターフェイス コンフィギュレーション コマンドおよび 生成された自動 QoS 設定をコンフィギュレーション ファイル内に保存しま す。

自動 QoS 情報の表示

自動 QoS 設定を表示するには、show auto qos [interface [*interface-id*]] 特権 EXEC コマンドを使用し ます。ユーザによる設定変更を表示するには、show running-config 特権 EXEC コマンドを使用しま す。show auto qos コマンド出力と show running-config コマンド出力を比較してユーザ定義の QoS 設定を比較できます。

自動 QoS によって影響を受ける QoS 設定を表示するには、以下のいずれかのコマンドを使用します。

- show mls qos
- show mls qos maps cos-dscp
- show mls qos interface [interface-id] [buffers | queueing]
- show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]
- show mls qos input-queue
- show running-config

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

標準 QoS の設定

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

ここでは、次の設定情報について説明します。

- 「標準 QoS のデフォルト設定」(P.33-31)
- 「標準 QoS 設定時の注意事項」(P.33-33)
- •「QoS のグローバルなイネーブル化」(P.33-35)(必須)
- 「ポートの信頼状態による分類の設定」(P.33-35)(必須)
- •「QoS ポリシーの設定」(P.33-43)(必須)
- 「DSCP マップの設定」(P.33-56)(任意、DSCP/DSCP 変換マップまたはポリシング済み DSCP マップを使用する必要がない場合)
- 「入力キューの特性の設定」(P.33-62)(任意)
- 「出力キューの特性の設定」(P.33-67)(任意)

標準 QoS のデフォルト設定

QoS はディセーブルに設定されています。パケット(パケットの CoS 値、DSCP 値、および IP precedence 値) は変更されないため、trusted(信頼性のある)ポート、または untrusted(信頼性のない)ポートの概念はありません。トラフィックはパススルー モードでスイッチングされます(書き換えられずにスイッチングされ、ポリシングを伴わないベストエフォート型として分類されます)。

mls qos グローバル コンフィギュレーション コマンドを使用して QoS をイネーブルにし、その他のす べての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型 として分類されます (DSCP および CoS 値は 0 に設定されます)。ポリシー マップは設定されません。 デフォルトでは、すべてのポートの信頼状態は untrusted です。入力および出力キューのデフォルト設 定については、「入力キューのデフォルト設定」(P.33-31) および「出力キューのデフォルト設定」 (P.33-32) を参照してください。

入力キューのデフォルト設定

表 33-6 に、QoS がイネーブルの場合の入力キューのデフォルト設定を示します。

表 33-6 入力キューのデフォルト設定

機能	キュー1	キュー2
バッファ割り当て	90%	10%
帯域幅割り当て	4	4
プライオリティ キューの帯域幅 ²	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみパケットを送信します。

2. キュー2はプライオリティキューです。共有が設定されている場合、SRR はプライオリティキューを処理してから、他のキューを処理します。

表 33-7 に、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示します。

表 33-7 デフォルトの CoS 入力キューしきい値マップ

CoS 值	キュー ID- しきい値 ID
0–4	1–1
5	2–1
6, 7	1–1

表 33-8 に、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示します。

表 33-8 デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID- しきい値 ID
0–39	1–1
40–47	2–1
48–63	1–1

出力キューのデフォルト設定

表 33-9 に、QoS がイネーブルの場合、各キューセットの出力キューのデフォルト設定を示します。すべてのポートはキューセット1 にマッピングされます。ポートの帯域幅限度は100% に設定され、レートは制限されません。

表 33-9 出	キューのデフォルト設定
----------	-------------

機能	キュー1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
専用しきい値	50%	50%	50%	50%
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み (絶対) ¹	25	0	0	0
SRR 共有重み ²	25	25	25	25

1. シェーピング重みが0の場合、このキューはシェーピングモードで動作します。

2. 帯域幅の4分の1が各キューに割り当てられます。

表 33-10 に、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 33-10 デフォルトの CoS 出力キューしきい値マップ

CoS 值	キュー ID- しきい値 ID
0, 1	2-1
2, 3	3-1
4	4-1
5	1–1
6, 7	4-1

表 33-11 に、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 33-11 デフォルトの DSCP 出力キューしきい値マップ

DSCP 値	キュー ID- しきい値 ID
0–15	2-1
16–31	3-1
32–39	4-1
40–47	1–1
48-63	4-1

マッピング テーブルのデフォルト設定

デフォルトの CoS/DSCP マップは、表 33-12 (P.33-56) のとおりです。

デフォルトの IP precedence/DSCP マップは、表 33-13 (P.33-57) のとおりです。

デフォルトの DSCP/CoS マップは、表 33-14 (P.33-59) のとおりです。

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップ です。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする(マー クダウンしない)空のマップです。

標準 QoS 設定時の注意事項

QoS の設定を始める前に、次の事項を確認してください。

- 「QoS ACL の注意事項」(P.33-33)
- 「ポリシングの注意事項」(P.33-34)
- 「一般的な QoS の注意事項」(P.33-34)

QoS ACL の注意事項

ACL で QoS を設定する際の注意事項は次のとおりです。

- QoS ACL 分類を使用する場合は、sdm prefer qos グローバル コンフィギュレーション コマンドを 入力して Switch Database Management (SDM) 機能を QoS テンプレートに設定します。SDM は システム リソースを設定し、ACE の最大数をサポートします。SDM テンプレートの詳細につい ては、第7章「SDM テンプレートの設定」を参照してください。
- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラスマップごとに使用できる ACL は 1 つだけ、使用できる match クラスマップ コン フィギュレーション コマンドは 1 つだけです。ACL には、フィールドとパケットの内容を照合す る ACE を複数指定できます。
- ポリシーマップの信頼ステートメントには、ACL 行毎に複数の TCAM エントリが必要です。入 カサービス ポリシーマップに ACL の信頼ステートメントが含まれている場合、利用可能な QoS TCAM に収めるにはアクセスリストが大きすぎる可能性があり、ポリシーマップをポートに適用 する際にエラーが発生する場合もあります。可能な限り、QoS ACL の行数を最小限に抑えてくだ さい。

ポリシングの注意事項

ポリシングの注意事項を次に示します。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 のポリサー(255 のユーザ設定可能ポリサーとシステムの内部使用のために予約された1つのポリサー)をサポートしています。ポート単位でサポートされている、ユーザ設定可能なポリサーの最大数は63 です。ポリサーは必要に応じてソフトウェアに割り当てられ、ハードウェアおよび ASIC 境界の制約を受けます。ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは1つのパケットに適用できるポリサーは1つだけです。設定できるのは、平均レートパラメータおよび認定バーストパラメータだけです。
- ポリシングレートは、1 MB/s 差分のみで設定できます。ポリシングレートを1 Mb/s 未満に設定 すると、スイッチのプロンプトは正確な値を要求します。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに 結合されたポリシーマップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランクポートの場合、ポートを介して受信した*すべての* VLAN のト ラフィックは、そのポートに結合されたポリシーマップに基づいて分類、ポリシング、および マーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理 ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。 また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- QoS を設定できるのは物理ポートだけです。VLAN のレベルでは QoS はサポートされていません。
- スイッチで受信された制御トラフィック (スパニング ツリー Bridge Protocol Data Unit [BPDU; ブ リッジ プロトコル データ ユニット] やルーティング アップデート パケットなど) には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小の ときに設定を変更するようにしてください。

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。

QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos	QoS をグローバルにイネーブルにします。
		デフォルト設定における QoS の動作については、「標準 QoS のデフォ ルト設定」(P.33-31)、「入力キューでのキューイングおよびスケジュー リング」(P.33-15)、および「出力キューでのキューイングおよびスケ ジューリング」(P.33-17)を参照してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

QoS をディセーブルにするには、no mls qos グローバル コンフィギュレーション コマンドを使用します。

ポートの信頼状態による分類の設定

ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネット ワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」(P.33-43)に記載されている作業を 1 つまたは複数実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」(P.33-35)
- 「インターフェイスの CoS 値の設定」(P.33-38)
- •「ポートセキュリティを確保するための信頼境界機能の設定」(P.33-39)
- 「DSCP 透過モードのイネーブル化」(P.33-40)
- 「別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定」(P.33-41)

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のス イッチ ポートをいずれか 1 つの信頼状態に設定できます。図 33-11 に、ネットワーク トポロジの例を 示します。



ポートが受信したトラフィックの分類を信頼するようにポートを設定するには、特権 EXEC モードで 次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	信頼するポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	mls qos trust [cos dscp ip-precedence]	ポートの信頼状態を設定します。
		デフォルトでは、ポートは trusted ではありません。キーワード を指定しない場合、デフォルトは dscp です。
		キーワードの意味は次のとおりです。
		 cos: パケットの CoS 値を使用して入力パケットを分類します。タグなしパケットの場合は、ポートのデフォルトの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。
		 dscp:パケットの DSCP 値を使用して入力パケットを分類 します。非 IP パケットでは、パケットがタグ付きの場合、 パケットの CoS 値が使用されます。パケットがタグなしの 場合は、デフォルトのポート CoS が使用されます。スイッ チは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
		 ip-precedence:パケットの IP precedence 値を使用して入力 パケットを分類します。非 IP パケットでは、パケットがタ グ付きの場合、パケットの CoS 値が使用されます。パケッ トがタグなしの場合は、デフォルトのポート CoS が使用さ れます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

untrusted ステートにポートを戻す場合は、no mls qos trust インターフェイス コンフィギュレーショ ン コマンドを使用します。

デフォルトの CoS 値を変更する方法については、「インターフェイスの CoS 値の設定」(P.33-38)を参照してください。CoS/DSCP マップを設定する方法については、「CoS/DSCP マップの設定」(P.33-56)を参照してください。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、mls qos cos インター フェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

デフォルトのポート CoS 値を定義する場合、またはポート上のすべての着信パケットにデフォルトの CoS 値を割り当てる場合には、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 3	mls qos cos { <i>default-cos</i> override}	デフォルトのポート CoS 値を設定します。
		 <i>default-cos</i>には、ポートに割り当てるデフォルトの CoS 値を指定 します。パケットがタグなしの場合、デフォルトの CoS 値がパ ケットの CoS 値になります。CoS 値に指定できる範囲は0~7で す。デフォルトは0です。
		 着信パケットにすでに設定されている信頼状態を変更し、すべての 着信パケットにデフォルトのポート CoS 値を適用する場合は、 override キーワードを使用します。デフォルトでは、CoS の上書 きはディセーブルに設定されています。
		特定のポートに届くすべての着信パケットに、他のポートからのパ ケットより高い、または低いプライオリティを与える場合には、 override キーワードを使用します。ポートがすでに DSCP、CoS、 または IP precedence を信頼するように設定されている場合でも、 設定済みの信頼状態がこのコマンドによって上書き変更され、すべ ての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値 が割り当てられます。着信パケットがタグ付きの場合、入力ポート で、ポートのデフォルト CoS を使用してパケットの CoS 値が変更 されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、no mls qos cos {*default-cos* | override} インターフェイス コンフィ ギュレーション コマンドを使用します。

ポート セキュリティを確保するための信頼境界機能の設定

ー般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して(図 33-11 (P.33-36)を参照)、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、 音声パケット CoS レベルをハイ プライオリティ (CoS = 5) にマーキングし、データ パケットをロー プライオリティ (CoS = 0) にマーキングすることで、共有データ リンクを通して音声品質を保証して います。電話からスイッチに送信されたトラフィックは通常 IEEE 802.1Q ヘッダーを使用するタグで マーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチへ送信されるトラフィックは、音声トラ フィックがネットワーク内の他のタイプのトラフィックに対して適切にプライオリティ付けがされてい ることを保証するように信頼されています。mls qos trust cos インターフェイス コンフィギュレー ション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するよう に、電話が接続されているスイッチ ポートを設定します。mls qos trust dscp インターフェイス コン フィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの DSCP ラベル を信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイ プライオリ ティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、(信 頼性のある CoS 設定により) PC が生成した CoS ラベルがスイッチで信頼されてしまいます。それに 対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone (Cisco IP Phone 7910、7935、7940、および 7960)の存在を検出します。電話が検出されない場合、信頼境界機能がハ イ プライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定をディセーブルにしま す。信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場 合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることも できる場合があります。switchport priority extend cos インターフェイス コンフィギュレーション コ マンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイ ネーブルに設定されています。
ステップ 3	interface interface-id	Cisco IP Phone に接続するポートを指定し、インターフェイス コン フィギュレーション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	cdp enable	ポート上で CDP をイネーブルに設定します。デフォルトでは、CDP が イネーブルに設定されています。
ステップ 5	mls qos trust cos	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するように スイッチ ポートを設定します。
		または
	mls qos trust dscp	Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するよう にルーテッド ポートを設定します。
		デフォルトでは、ポートは trusted ではありません。

	コマンド	目的
ステップ 6	mls qos trust device cisco-phone	Cisco IP Phone が信頼性のあるデバイスであることを指定します。
		信頼境界機能と自動 QoS (auto qos voip インターフェイス コンフィ ギュレーション コマンド)を同時にイネーブルにはできません。両者 は相互に排他的です。
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show mls qos interface	設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

信頼境界機能をディセーブルにするには、no mls qos trust device インターフェイス コンフィギュレー ション コマンドを使用します。

DSCP 透過モードのイネーブル化

スイッチは透過的な DSCP 機能をサポートします。この機能は発信パケットの DSCP フィールドのみ に作用します。透過的な DSCP 機能のデフォルト設定はディセーブルです。スイッチは着信パケット の DSCP フィールドを変更します。発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシ ングとマーキング、および DSCP/DSCP 変換マップを含め、QoS 設定によって異なります。

no mls qos rewrite ip dscp コマンドを用いて透過的な DSCP 機能をイネーブルにした場合、スイッチ は着信パケットの DSCP フィールドを変更しません。そのため、発信パケットの DSCP フィールドの 内容はパケットの着信時と同じです。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプ ライオリティを提示する CoS 値を生成します。また、スイッチは内部の DSCP 値を使用して、出力 キューおよびしきい値も選択します。

特権 EXEC モードを開始して、透過的な DSCP 機能をスイッチでイネーブルにするには、次の手順を 実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos	QoS をグローバルにイネーブルにします。
ステップ 3	no mls qos rewrite ip dscp	透過的な DSCP 機能をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変 更させる設定にするには、mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを使 用します。

no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS お よび DSCP 値は変更されません(デフォルトの QoS 設定)。 no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイ ネーブルにしてから、mls qos trust [cos | dscp] インターフェイス コンフィギュレーション コマンドを 入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機 能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定でき ます(図 33-12 を参照)。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分 類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内で の定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 33-12 別の QoS ドメインとの境界ポートの DSCP 信頼状態



ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。両方の QoS ドメインに一貫した方法でマッピングするには、両方の ドメイン内のポート上で次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map dscp-mutation <i>dscp-mutation-name in-dscp</i> to <i>out-dscp</i>	DSCP/DSCP 変換マップを変更します。
		デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。
		 dscp-mutation-name には、変換マップ名を入力します。新し い名前を指定することにより、複数のマップを作成できます。
		 <i>in-dscp</i>には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、toキーワードを入力します。
		• <i>out-dscp</i> には、DSCP 値を 1 つ入力します。
		DSCP の範囲は 0 ~ 63 です。
ステップ 3	interface interface-id	信頼するポートを指定し、インターフェイス コンフィギュレー ション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルト では、ポートは trusted ではありません。
ステップ 5	mls qos dscp-mutation	指定された DSCP trusted 入力ポートにマップを適用します。
	dscp-mutation-name	<i>dscp-mutation-name</i> には、ステップ 2 で作成した変換マップ名を 指定します。
		1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mls qos maps dscp-mutation	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ポートを trusted 以外のステートに戻すには、no mls qos trust インターフェイス コンフィギュレー ション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、no mls qos map dscp-mutation *dscp-mutation-name* グローバル コンフィギュレーション コマンドを使用します。

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ~ 13 が DSCP 値 30 にマッピ ングされるように DSCP/DSCP 変換マップ (*gi0/2-mutation*) を変更する例を示します。

Switch(config)# mls qos map dscp-mutation gi0/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi0/2-mutation
Switch(config-if)# end

QoS ポリシーの設定

QoS ポリシーを設定するには、通常、トラフィックをクラス別に分類し、各トラフィック クラスに適用するポリシーを設定し、ポリシーをポートに結合する必要があります。

基本情報については、「分類」(P.33-5)および「ポリシングおよびマーキング」(P.33-9)を参照して ください。設定時の注意事項については、「標準 QoS 設定時の注意事項」(P.33-33)を参照してくださ い。

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。ネットワーク 設定に応じて、次の作業を1つまたは複数実行する必要があります。

- 「ACL によるトラフィックの分類」(P.33-43)
- 「クラス マップによるトラフィックの分類」(P.33-47)
- 「ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」 (P.33-49)
- 「集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング」(P.33-54)

ACL によるトラフィックの分類

IP 標準 ACL または IP 拡張 ACL を使用することによって、IP トラフィックを分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用することによって分類できます。

IP トラフィック用に IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number {deny permit} source [source-wildcard]	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。
		 access-list-number には、アクセス リスト番号を入力します。 有効範囲は 1 ~ 99 および 1300 ~ 1999 です。
		 permit キーワードを使用すると、条件が一致した場合に特定のトラフィックタイプを許可します。deny キーワードを使用すると、条件が一致した場合に特定のトラフィックタイプを拒否します。
		 source には、パケットの送信元となるネットワークまたはホストを指定します。any キーワードは 0.0.0.0 255.255.255.255 の 省略形として使用できます。
		 (任意) source-wildcard には、source に適用されるワイルド カード ビットをドット付き 10 進表記で入力します。無視する ビット位置には1を入れます。
		(注) アクセス リストを作成するときは、アクセス リストの末尾 に暗黙の拒否ステートメントがデフォルトで存在し、それ 以前のステートメントで一致が見つからなかったすべての パケットに適用されることに注意してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、no access-list access-list-number グローバル コンフィギュレーショ ン コマンドを使用します。

次に、指定された3つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワークアドレスのホスト部分にワイルドカードビットが適用されます。アクセスリストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.255
! (Note: all other access implicitly denied)

IP トラフィック用に IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number { deny permit } protocol source source-wildcard destination destination-wildcard	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。
		 access-list-number には、アクセスリスト番号を入力します。 有効範囲は 100 ~ 199 および 2000 ~ 2699 です。
		 permit キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。deny キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。
		 protocol には、IP プロトコルの名前または番号を入力します。 疑問符(?)を使用すると、使用できるプロトコル キーワードのリストが表示されます。
		 source には、パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、source 0.0.0.0 source-wildcard 255.255.255.255 の短縮形として any キーワードを使用したり、source 0.0.0.0 を表す host キーワードを使用します。
		 source-wildcard では、無視するビット位置に1を入力することによって、ワイルドカードビットを指定します。ワイルドカードを指定するには、ドット付き10進表記を使用したり、source 0.0.0.0 source-wildcard 255.255.255.255 の短縮形として any キーワードを使用したり、source 0.0.0.0 を表す host キーワードを使用します。
		 destination には、パケットの宛先となるネットワークまたは ホストを指定します。destination および destination-wildcard には、source および source-wildcard での説明と同じオプショ ンを使用できます。
		(注) アクセス リストを作成するときは、アクセス リストの末尾 に暗黙の拒否ステートメントがデフォルトで存在し、それ 以前のステートメントで一致が見つからなかったすべての パケットに適用されることに注意してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists	設定を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、no access-list access-list-number グローバル コンフィギュレーショ ン コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

Switch(config)# access-list 100 permit ip any any dscp 32

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック (precedence 値は 5) を許可する ACL を作成する例を示します。

Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック (DSCP 値は 32) を許可する ACL を作成する例を示します。

Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32 非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行しま す。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mac access-list extended name	リスト名を指定し、レイヤ 2 MAC ACL を作成します。
		このコマンドを入力すると、拡張 MAC ACL コンフィギュレー ション モードに切り替わります。
ステップ 3	{permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	条件が一致した場合に許可または拒否するトラフィック タイプ を指定します。必要な回数だけコマンドを入力します。
		 src-MAC-addrには、パケットの送信元となるホストの MACアドレスを指定します。MACアドレスを指定するに は、16 進表記(H.H.H)を使用したり、source 0.0.0、 source-wildcard ffff.ffff の短縮形として any キーワード を使用したり、source 0.0.0 を表す host キーワードを使用し ます。
		 mask では、無視するビット位置に1を入力することによって、ワイルドカードビットを指定します。
		 <i>dst-MAC-addr</i>には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記(H.H.H)を使用したり、source 0.0.0、 source-wildcard ffff.ffff.ffffの短縮形として any キーワード を使用したり、source 0.0.0 を表す host キーワードを使用し ます。
		 (任意) <i>type mask</i> には、Ethernet II または SNAP でカプセ ル化されたパケットの Ethertype 番号を指定して、パケット のプロトコルを識別します。<i>type</i> の範囲は 0 ~ 65535 です。 通常は 16 進数で指定します。<i>mask</i> には、一致をテストする 前に Ethertype に適用される <i>無視 (don't care)</i> ビットを入力 します。
		(注) アクセス リストを作成するときは、アクセス リストの末 尾に暗黙の拒否ステートメントがデフォルトで存在し、 それ以前のステートメントで一致が見つからなかったす べてのパケットに適用されることに注意してください。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show access-lists [access-list-number access-list-name]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、no mac access-list extended access-list-name グローバル コンフィ ギュレーション コマンドを入力します。

次に、2 つの許可 (permit) ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示しま す。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレス が 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めのステートメントでは、 MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホスト への、Ethertype が XNS-IDP のトラフィックのみが許可されます。

Switch(config) # mac access-list extended maclist1
Switch(config-ext-macl) # permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl) # permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)

クラス マップによるトラフィックの分類

個々のトラフィックフロー(またはクラス)を他のすべてのトラフィックから分離して名前を付ける には、class-map グローバル コンフィギュレーション コマンドを使用します。クラス マップでは、さ らに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。match ステー トメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを1 つ入力することによって定義 します。

(注)

class ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの 作成時にクラス マップを作成することもできます。詳細については、「ポリシー マップによる物理ポー トのトラフィックの分類、ポリシング、およびマーキング」(P.33-49)を参照してください。

クラスマップを作成し、トラフィックを分類するための一致条件を定義するには、特権 EXEC モード で次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	access-list access-list-number {deny permit} source [source-wildcard] または	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラ フィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマ ンドを繰り返します。
	access-list access-list-number {deny permit} protocol source	詳細については、「ACL によるトラフィックの分類」(P.33-43)を 参照してください。
	[source-wildcard] destination [destination-wildcard]	(注) アクセス リストを作成するときは、アクセス リストの末尾 に暗黙の拒否ステートメントがデフォルトで存在し、それ
		以前のステートメントで一致が見つからなかったすべての パケットに適用されることに注意してください。
	mac access-list extended name	
	{ permit deny } { host <i>src-MAC-addr</i> <i>mask</i> any host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i> } [<i>type mask</i>]	

	コマンド	目的
ステップ 3	class-map [match-all match-any] class-map-name	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
		デフォルトでは、クラスマップは定義されていません。
		 (任意) このクラス マップ配下のすべての一致ステートメント の論理 AND を実行するには、match-all キーワードを使用し ます。この場合は、クラス マップ内のすべての一致条件と一 致する必要があります。
		 (任意) このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。
		• <i>class-map-name</i> には、クラス マップ名を指定します。
		match-all または match-any のどちらのキーワードも指定しない 場合、デフォルトは match-all です。
		(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワード の機能は変わりません。
ステップ 4	<pre>match {access-group acl-index-or-name</pre>	トラフィックを分類するための一致条件を定義します。
		デフォルトでは、一致条件は定義されていません。
	<i>T T T T T T T T T T</i>	クラス マップごとにサポートされる一致条件は1つだけです。また、クラス マップごとにサポートされる ACL は1つだけです。
		 access-group acl-index-or-name には、ステップ2で作成した ACL の番号または名前を指定します。
		 ip dscp dscp-list には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定でき る範囲は 0 ~ 63 です。
		 ip precedence <i>ip-precedence-list</i> には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで 区切ります。指定できる範囲は 0 ~ 7です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show class-map	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュ レーション コマンドを使用します。既存のクラス マップを削除するには、no class-map [match-all | match-any] class-map-name グローバル コンフィギュレーション コマンドを使用します。一致条件を 削除するには、no match {access-group acl-index-or-name | ip dscp | ip precedence} クラス マップ コ ンフィギュレーション コマンドを使用します。

次に、*class1*というクラスマップの設定例を示します。*class1*にはアクセスリスト103という一致条件が1つ設定されています。このクラスマップによって、任意のホストから任意の宛先へのトラフィック(DSCP値は10)が許可されます。

Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end

Switch#

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、*class2* という名前のクラス マップを作成する例を示します。

Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

作用対象となるトラフィック クラスを指定するポリシー マップを、物理ポート上に設定できます。ト ラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィッ ク クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラ フィック クラスにトラフィック帯域幅限度を指定するアクション(ポリサー)や、トラフィックが不 適合な場合の対処法を指定するアクション(マーキング)などを指定できます。

ポリシーマップには、次の特性もあります。

- 1つのポリシーマップに、それぞれ異なる一致条件とポリサーを指定した複数のクラスステートメントを指定できます。
- 1 つのポートから受信されたトラフィックタイプごとに、別々のポリシーマップクラスを設定できます。
- ポリシーマップの信頼状態およびポートの信頼状態は互いに排他的であり、最後に設定された方 が有効となります。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシーマップは、1つだけです。
- mls qos map ip-prec-dscp dscp1...dscp8 グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定さ れている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、set ip precedence new-precedence ポリシー マップ クラス コンフィギュレーション コマンドを使用して パケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マッ プによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、set dscp new-dscp ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- set ip dscp コマンドを入力または使用すると、スイッチは設定内で、このコマンドを set dscp に変更します。
- set ip precedence または set precedence ポリシーマップ クラス コンフィギュレーション コマンド を使用すると、パケット IP Precedence 値を変更できます。この設定は、スイッチ コンフィギュ レーションで set ip precedence として表示されます。
- ポリシーマップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。ポリシーマップは、ポート信頼状態の前に適用されます。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	class-map [match-all match-any] class-map-name	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
		デフォルトでは、クラス マップは定義されていません。
		 (任意) このクラス マップ配下のすべての一致ステートメント の論理 AND を実行するには、match-all キーワードを使用し ます。この場合は、クラス マップ内のすべての一致条件と一 致する必要があります。
		 (任意) このクラス マップ配下のすべての一致ステートメント の論理 OR を実行するには、match-any キーワードを使用し ます。この場合は、1 つまたは複数の一致条件と一致する必要 があります。
		• <i>class-map-name</i> には、クラス マップ名を指定します。
		match-all または match-any のどちらのキーワードも指定しない 場合、デフォルトは match-all です。
		(注) クラスマップごとにサポートされる match コマンドは1つ だけなので、match-all でも match-any でもキーワードの 機能は変わりません。
ステップ 3	policy-map policy-map-name	ポリシー マップ名を入力することによってポリシー マップを作成 し、ポリシー マップ コンフィギュレーション モードを開始しま す。
		デフォルトでは、ポリシー マップは定義されていません。
		ポリシー マップのデフォルトの動作では、パケットが IP パケット の場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に 設定されます。ポリシングは実行されません。
ステップ 4	class class-map-name	トラフィックの分類を定義し、ポリシー マップ クラス コンフィ ギュレーション モードを開始します。
		デフォルトでは、ポリシー マップ クラス マップは定義されていま せん。
		すでに class-map グローバル コンフィギュレーション コマンドを 使用してトラフィック クラスが定義されている場合は、このコマ ンドで class-map-name にその名前を指定します。

特権 EXEC モードを開始して、ポリシー マップを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 5	trust [cos dscp ip-precedence]	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼状態を設定します。
		 (注) このコマンドと set コマンドは、同じポリシー マップ内で 相互に排他的になります。trust コマンドを入力する場合 は、ステップ6へ進んでください。
		デフォルトでは、ポートは trusted ではありません。このコマンド を入力するときにキーワードを指定しない場合、デフォルトは dscp になります。
		キーワードの意味は次のとおりです。
		 cos: QoS は受信した CoS 値やデフォルトのポート CoS 値、 および CoS/DSCP マップを使用して、DSCP 値を抽出します。
		 dscp: QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値はCoS/DSCP マップから抽出されます。
		 ip-precedence: QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。
		詳細については、「CoS/DSCP マップの設定」(P.33-56)を参照し てください。
ステップ 6	<pre>set {dscp new-dscp ip precedence new-precedence}</pre>	パケットに新しい値を設定することによって、IP トラフィックを 分類します。
		 dscp new-dscp には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。
		 ip precedence new-precedence には、分類されたトラフィック に割り当てる新しい IP precedence 値を入力します。指定でき る範囲は0~7です。

	コマンド	目的
ステップ 7	<pre>police rate-bps burst-byte [exceed-action {drop policed-dscp-transmit}]</pre>	分類したトラフィックにポリサーを定義します。
		デフォルトでは、ポリサーは定義されていません。サポートされて いるポリサー数については、「標準 QoS 設定時の注意事項」 (P.33-33)を参照してください。
		 rate-bps には、平均トラフィック レートをビット/秒(bps) で指定します。指定できる範囲は 1000000 ~ 1000000000 で す。ポリシング レートは、1 MB/s 差分のみで設定できます。 ポリシング レートを 1 MB/s 未満に設定すると、スイッチのプ ロンプトは正確な値を要求します。
		 burst-byteには、標準バーストサイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000です。
		 (任意)レートを超過した場合に実行するアクションを指定します。パケットを廃棄する場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して)DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.33-58)を参照してください。
ステップ 8	exit	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	interface interface-id	ポリシー マップを適用するポートを指定し、インターフェイス コ ンフィギュレーション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 11	service-policy input policy-map-name	ポリシーマップ名を指定し、入力ポートに適用します。
		サポートされるポリシー マップは、入力ポートごとに 1 つだけで す。
ステップ 12	end	特権 EXEC モードに戻ります。
ステップ 13	<pre>show policy-map [policy-map-name [class class-map-name]]</pre>	設定を確認します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュ レーション コマンドを使用します。既存のクラス マップを削除するには、no class class-map-name ポ リシー マップ コンフィギュレーション コマンドを使用します。untrusted ステートに戻すには、no trust ポリシーマップ コンフィギュレーション コマンドを使用します。割り当てられた DSCP または IP precedence 値を削除するには、no set {dscp new-dscp | ip precedence new-precedence} ポリシー マップ コンフィギュレーション コマンドを使用します。既存のポリサーを削除するには、no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}] ポリシー マップ コンフィギュレー ション コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、no service-policy input policy-map-name インターフェイス コンフィギュレーション コマンドを使用しま す。
次に、ポリシー マップを作成し、入力ポートに結合する例を示します。この設定では、IP 標準 ACL で ネットワーク 10.1.0.0 からのトラフィックを許可します。この分類にトラフィックが一致した場合、 着信パケットの DSCP 値が信頼されます。一致したトラフィックが平均トラフィック レート(48000 bps)、および標準バースト サイズ(8000 バイト)を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP はマークダウンされて、送信されます。

Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap-c)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input flow1t

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を 示します。最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、 MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めの許可ス テートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config) # mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac) # exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config) # policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap) # class macclass2 maclist2
Switch(config-pmap-c) # set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if) # mls qos trust cos
Switch(config-if) # service-policy input macpolicy1
```

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシー マップ内の複数のトラフィック クラスで共有されるポリ サーを作成できます。ただし、集約ポリサーを複数の異なるポリシー マップまたはポートにわたって 使用することはできません。

集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的				
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。				
ステップ 2	mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte	同じポリシー マップ内の複数のトラフィック クラスに適用でき るポリサー パラメータを定義します。				
	exceed-action {drop policed-dscp-transmit}	デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意 事項」(P.33-33)を参照してください。				
		 aggregate-policer-name には、集約ポリサーの名前を指定 します。 				
		 rate-bps には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 1000000 ~ 1000000000 です。ポリシング レートは、1 MB/s 差分のみで設定できま す。ポリシング レートを 1 MB/s 未満に設定すると、ス イッチのプロンプトは正確な値を要求します。 				
		 burst-byte には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 				
		 レートを超過した場合に実行するアクションを指定します。 パケットを廃棄する場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.33-58)を参照してください。 				
ステップ 3	class-map [match-all match-any] class-map-name	必要に応じて、トラフィックを分類するクラスマップを作成します。詳細については、「クラスマップによるトラフィックの 分類」(P.33-47)を参照してください。				
ステップ 4	policy-map policy-map-name	ポリシー マップ名を入力することによってポリシー マップを作 成し、ポリシー マップ コンフィギュレーション モードを開始し ます。				
		詳細については、「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」(P.33-49)を参照してください。				
ステップ 5	class class-map-name	トラフィックの分類を定義し、ポリシー マップ クラス コンフィ ギュレーション モードを開始します。				
		詳細については、「ポリシー マップによる物理ポートのトラ フィックの分類、ポリシング、およびマーキング」(P.33-49) を参照してください。				

	コマンド	目的
ステップ 6	police aggregate aggregate-policer-name	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。
		<i>aggregate-policer-name</i> には、ステップ 2 で指定した名前を入 力します。
ステップ 7	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	interface interface-id	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
		指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 9	service-policy input policy-map-name	ポリシーマップ名を指定し、入力ポートに適用します。
		サポートされるポリシー マップは、入力ポートごとに1つだけ です。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show mls qos aggregate-policer [aggregate-policer-name]	設定を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された集約ポリサーをポリシー マップから削除するには、no police aggregate aggregate-policer-name ポリシー マップ コンフィギュレーション モードを使用します。集約ポリサー およびそのパラメータを削除するには、no mls qos aggregate-policer aggregate-policer-name グロー バル コンフィギュレーション コマンドを使用します。

次に、集約ポリサーを作成して、ポリシーマップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。 ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。 ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネット ワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。 トラフィックが平均レート (48000 bps)、および標準バースト サイズ (8000 バイト)を超過している 場合は、(ポリシング済み DSCP マップに基づいて) DSCP がマークダウンされて、送信されます。ポ

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config) # mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap) # match access-group 2
Switch(config-cmap)# exit
Switch(config) # policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap) # exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

DSCP マップの設定

ここでは、次の設定情報について説明します。

- 「CoS/DSCP マップの設定」(P.33-56)(任意)
- 「IP precedence/DSCP マップの設定」(P.33-57)(任意)
- 「ポリシング済み DSCP マップの設定」(P.33-58)(任意、マップのヌル設定が不適切な場合以外)
- 「DSCP/CoS マップの設定」(P.33-59)(任意)
- 「DSCP/DSCP 変換マップの設定」(P.33-60)(任意、マップのヌル設定が不適切な場合以外)

DSCP/DSCP 変換マップを除くすべてのマップはグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表 すために内部使用する DSCP 値にマッピングします。

表 33-12 に、デフォルトの CoS/DSCP マップを示します。

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 33-12 デフォルトの CoS/DSCP マップ

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。 CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
configure terminal	グローバル コンフィギュレーション モードを開始します。
mls qos map cos-dscp dscp1dscp8	CoS/DSCP マップを変更します。
	<i>dscp1dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力 します。各 DSCP 値はスペースで区切ります。
	DSCP の範囲は 0 ~ 63 です。
end	特権 EXEC モードに戻ります。
show mls qos maps cos-dscp	設定を確認します。
copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
	コマンド configure terminal mls qos map cos-dscp dscp1dscp8 end show mls qos maps cos-dscp copy running-config startup-config

デフォルトのマップに戻すには、no mls qos cos-dscp グローバル コンフィギュレーション コマンドを 使用します。

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp
```

IP precedence/DSCP マップの設定

着信パケットの IP precedence 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングするには、IP precedence/DSCP マップを使用します。

表 33-13 に、デフォルトの IP precedence/DSCP マップを示します。

IP precedence 値	DSCP 値	
0	0	
1	8	
2	16	
3	24	
4	32	
5	40	
6	48	
7	56	

表 33-13 デフォルトの IP precedence/DSCP マップ

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map ip-prec-dscp	IP precedence/DSCP マップを変更します。
	dscp1dscp8	<i>dscp1dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。
		DSCP の範囲は 0 ~ 63 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos maps ip-prec-dscp	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、no mls qos ip-prec-dscp グローバル コンフィギュレーション コマン ドを使用します。 次に、IP precedence/DSCP マップを変更して表示する例を示します。

Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45 Switch(config)# end Switch# show mls qos maps ip-prec-dscp

ポリシング済み DSCP マップの設定

ポリシングおよびマーキング アクションによって得られる新しい値に DSCP 値をマークダウンするに は、ポリシング済み DSCP マップを使用します。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空の マップです。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順 は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map policed-dscp dscp-list to	ポリシング済み DSCP マップを変更します。
	mark-down-dscp	 <i>dscp-list</i>には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、toキーワードを入力します。
		 <i>mark-down-dscp</i>には、対応するポリシング済み(マークダウン される) DSCP 値を入力します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos maps policed-dscp	設定を確認します。
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、no mls qos policed-dscp グローバル コンフィギュレーション コマン ドを使用します。

次に、DSCP 50 ~ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

Switch (config) # mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0 Switch(config) # end Switch# show mls qos maps policed-dscp Policed-dscp map: d1: d20 1 2 3 4 5 6 7 8 9 0: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 1 : 20 21 22 23 24 25 26 27 28 29 2 : 30 31 32 33 34 35 36 37 38 39 3 : 40 41 42 43 44 45 46 47 48 49 4 : 5: 00 00 00 00 00 00 00 00 58 59 6 : 60 61 62 63

<u>》</u> (注)

このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、 マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

4 つの出力キューのうち1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップ を使用します。

表 33-14 に、デフォルトの DSCP/CoS マップを示します。

DSCP 値	CoS 値
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40-47	5
48–55	6
56-63	7

表 33-14 デフォルトの DSCP/CoS マップ

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

DSCP/CoS マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos map dscp-cos dscp-list to cos	DSCP/CoS マップを変更します。
		 <i>dscp-list</i>には、最大8つのDSCP値をスペースで区切って入力します。さらに、toキーワードを入力します。
		• cos には、DSCP 値と対応する CoS 値を入力します。
		DSCPの範囲は $0 \sim 63$ 、CoSの範囲は $0 \sim 7$ です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos maps dscp-to-cos	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、no mls qos dscp-cos グローバル コンフィギュレーション コマンドを 使用します。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示 する例を示します。

Switch(config) # mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0 Switch(config) # end

Switch#	sh	ow mls	s qo	os r	naps	s ds	scp-	cos	3		
Dscp-cos	s m	ap:									
d1	:	d2 0	1	2	3	4	5	6	7	8	9
0	:	00	00	00	00	00	00	00	00	00	01
1	:	01	01	01	01	01	01	00	02	02	02
2	:	02	02	02	02	00	03	03	03	03	03
3	:	03	03	00	04	04	04	04	04	04	04
4	:	00	05	05	05	05	05	05	05	00	06
5	:	00	06	06	06	06	06	07	07	07	07
6	:	07	07	07	07						

(注)

上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行 は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値 を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。 DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポート適用します(入力変換)。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を使用し てパケットを処理します。スイッチは新しい DSCP 値を使用して、ポートからパケットを送信します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。デフォルトの DSCP/DSCP 変換 マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	mls qos map dscp-mutation	DSCP/DSCP 変換マップを変更します。		
	dscp-mutation-name in-dscp to out-dscp	 dscp-mutation-name には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 		
		 <i>in-dscp</i>には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、toキーワードを入力します。 		
		• <i>out-dscp</i> には、DSCP 値を 1 つ入力します。		
		DSCPの範囲は0~63です。		
ステップ 3	interface interface-id	マップを適用するポートを指定し、インターフェイス コンフィ ギュレーション モードを開始します。		
		指定できるインターフェイスとして、物理ポートも含まれます。		
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルト では、ポートは trusted ではありません。		
ステップ 5	mls qos dscp-mutation	指定された DSCP trusted 入力ポートにマップを適用します。		
	dscp-mutation-name	<i>dscp-mutation-name</i> には、ステップ 2 で指定した変換マップ名を 入力します。		
ステップ 6	end	特権 EXEC モードに戻ります。		

	コマンド	目的
ステップ 7	show mls qos maps dscp-mutation	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、no mls qos dscp-mutation *dscp-mutation-name* グローバル コンフィ ギュレーション コマンドを使用します。

次に、DSCP/DSCP 変換マップを定義する例を示します。明示的に設定されていないすべてのエントリ は変更されません(空のマップで指定された値のままです)。

```
Switch(config) # mls gos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch (config) # mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config) # mls gos map dscp-mutation mutation1 20 21 22 to 20
Switch (config) # mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config-if) # mls qos trust dscp
Switch(config-if) # mls qos dscp-mutation mutation1
Switch(config-if) # end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
  mutation1:
     d1: d20 1 2 3 4 5 6 7 8 9
     0:
            00 00 00 00 00 00 00 00 10 10
     1 :
            10 10 10 10 14 15 16 17 18 19
            20 20 20 23 24 25 26 27 28 29
     2 :
            30 30 30 30 30 35 36 37 38 39
      3 :
      4 :
            40 41 42 43 44 45 46 47 48 49
            50 51 52 53 54 55 56 57 58 59
      5 :
      6 :
            60 61 62 63
```

(注)

上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の 最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。た とえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。 ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- 各キューに(DSCP 値または CoS 値によって)割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファスペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック(音声など)の有無

ここでは、次の設定情報について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.33-62)(任意)
- 「入力キュー間のバッファスペースの割り当て」(P.33-64)(任意)
- 「入力キュー間の帯域幅の割り当て」(P.33-65)(任意)
- 「入力プライオリティキューの設定」(P.33-66)(任意)

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定の キューに格納し、より低いプライオリティを持つパケットが廃棄されるようにキューのしきい値を調整 します。

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input dscp-map queue queue-id threshold threshold-id	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。
	dscp1dscp8	デフォルトでは、DSCP 値 0 ~ 39 および 48 ~ 63 はキュー 1 およびしき い値 1 にマッピングされます。DSCP 値 40 ~ 47 はキュー 2 およびしきい
	または	値1にマッピングされます。
	mls qos srr-queue input cos-map queue queue-id threshold threshold-id cos1cos8	デフォルトでは、CoS 値 0 ~ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。
		 queue-id に指定できる範囲は、1~2です。
		 threshold-id の範囲は、1~3です。3の廃棄の割合は定義済みであり、キューフルステートに設定されます。
		 <i>dscp1dscp8</i>には、最大8つの値をスペースで区切って入力します。 指定できる範囲は0~63です。
		 cos1cos8には、最大8つの値をスペースで区切って入力します。指定できる範囲は0~7です。

	コマンド	目的
ステップ 3	mls qos srr-queue input threshold <i>queue-id threshold-percentage1</i> <i>threshold-percentage2</i>	入力キューに 2 つの WTD しきい値の割合(しきい値 1 および 2 用)を割 り当てます。デフォルトでは、両方のしきい値が 100% に設定されていま す。
		 queue-id に指定できる範囲は、1~2です。
		 threshold-percentage1 threshold-percentage2 の範囲は、1~100 で す。各値はスペースで区切ります。
		各しきい値は、キューに割り当てられたキュー記述子の総数の割合です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos maps	設定を確認します。
		DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 お よびしきい値 1 (02-01) のようになります。
		CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応 するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およ びしきい値 2 (2-2) のようになります。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの CoS 入力キューしきい値マップまたはデフォルトの DSCP 入力キューしきい値マップに 戻すには、no mls qos srr-queue input cos-map、または no mls qos srr-queue input dscp-map グロー バル コンフィギュレーション コマンドを使用します。デフォルトの WTD しきい値の割合に戻すには、 no mls qos srr-queue input threshold *queue-id* グローバル コンフィギュレーション コマンドを使用し ます。

次に、DSCP 値 $0 \sim 6 \varepsilon$ 、入力キュー 1 およびしきい値 1 (ドロップしきい値が 50%) にマッピングする例を示します。DSCP 値 $20 \sim 26$ は、入力キュー 1 およびしきい値 2 (ドロップしきい値が 70%) にマッピングされます。

Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6 Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26 Switch(config)# mls qos srr-queue input threshold 1 50 70

この例では、50% の WTD しきい値が DSCP 値 $(0 \sim 6)$ に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値 $(20 \sim 26)$ よりも先に廃棄されます。

入力キュー間のバッファ スペースの割り当て

2つのキュー間で入力バッファを分割する比率を定義します(スペース量を割り当てます)。バッファ 割り当てと帯域幅割り当てにより、パケットが廃棄される前にバッファに格納できるデータ量が制御さ れます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は 任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input buffers	入力キュー間にバッファを割り当てます。
	percentage1 percentage2	デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% が キュー 2 に割り当てられます。
		<i>percentage1 percentage2</i> の範囲は、0~100です。各値はスペースで 区切ります。
		キューが着信バースト トラフィックをすべて処理できるように、 バッファを割り当てる必要があります。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos interface buffer	設定を確認します。
	または	
	show mls qos input-queue	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no mls qos srr-queue input buffers グローバル コンフィギュレーショ ン コマンドを使用します。

次に、バッファ スペースの 60% を入力キュー 1 に、40% を入力キュー 2 に割り当てる例を示します。 Switch(config)# mls qos srr-queue input buffers 60 40

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、 SRR スケジューラが各キューからパケットを送信する頻度の比率です。帯域幅割り当てとバッファ割 り当てにより、パケットが廃棄される前にバッファに格納できるデータ量を制御できます。入力キュー で SRR が動作するのは、共有モードの場合のみです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input bandwidth weight1 weight2	入力キューに共有ラウンドロビン重みを割り当てます。
		weight1 およびweight2 のデフォルト設定は4 です(帯域幅の 1/2 が 2 つのキューで等しく共有されます)。
		<i>weight1</i> および <i>weight2</i> の範囲は、1 ~ 100 です。各値はスペースで 区切ります。
		SRR は mls qos srr-queue input priority-queue queue-id bandwidth weight グローバル コンフィギュレーション コマンドの bandwidth キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は mls qos srr-queue input bandwidth weight1 weight2 グローバル コンフィギュレーション コマ ンドによって設定された重みに従い、残りの帯域幅を両方の入力 キューと共有し、キューを処理します。詳細については、「入力プラ イオリティ キューの設定」(P.33-66) を参照してください。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos interface queueing	設定を確認します。
	または	
	show mls qos input-queue	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no mls qos srr-queue input bandwidth グローバル コンフィギュレー ション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティキューはディセーブルです。 キュー1に割り当てられた共有帯域幅の比率は25/(25 + 75)、キュー2の比率は75/(25 + 75)です。

Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75

入力プライオリティ キューの設定

プライオリティキューは、迅速な処理が必要なトラフィック(遅延およびジッタを最小に抑える必要のある音声トラフィックなど)にのみ使用します。

プライオリティキューは、オーバーサブスクライブリングに激しいネットワークトラフィックが発生している状況で(バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、 キューがいっぱいになって、フレームが廃棄されている場合)、遅延およびジッタを軽減するように帯 域幅の一部が保証されています。

SRR は mls qos srr-queue input priority-queue queue-id bandwidth weight グローバル コンフィギュ レーション コマンドの bandwidth キーワードで指定された設定済みの重みに従って、プライオリティ キューを処理します。次に、SRR は mls qos srr-queue input bandwidth weight1 weight2 グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キュー と共有し、キューを処理します。

プライオリティキューを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue input priority-queue queue-id bandwidth weight	キューをプライオリティ キューとして割り当て、内部リングが輻輳 している場合にリングの帯域幅を保証します。
		デフォルトのプライオリティ キューはキュー 2 です。このキューに は帯域幅の 10% が割り当てられています。
		 queue-id に指定できる範囲は、1~2です。
		 bandwidth weightには、内部リングの帯域幅に対する割合を割り当てます。指定できる範囲は0~40です。値が大きい場合はリング全体に影響が及び、パフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos interface queueing	設定を確認します。
	または	
	show mls qos input-queue	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、no mls qos srr-queue input priority-queue *queue-id* グローバル コンフィ ギュレーション コマンドを使用します。プライオリティ キューイングをディセーブルにするには、帯 域幅の重みを 0 に設定します。たとえば、mls qos srr-queue input priority-queue *queue-id* bandwidth 0 を入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー1は、帯域幅の10%が割り当てられているプライオリティキューです。キュー1および2に割り当てられている帯域幅比率は4/(4+4)です。 SRRは、10%の帯域幅が設定されたキュー1(プライオリティキュー)を最初に処理します。次に、 SRRは残りの90%の帯域幅をキュー1と2にそれぞれ45%ずつ割り当てて、各キューで等しく共有します。

Switch(config) # mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config) # mls qos srr-queue input bandwidth 4 4

出力キューの特性の設定

ネットワークおよび QoS ソリューションの複雑さに応じて、次に示す作業をすべて実行しなければならない場合があります。次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット(ポートごとの4つの出力キュー)に適用されるドロップしきい値の割合、およびトラフィックタイプに必要なメモリの確保量および最大メモリ
- キューセットに割り当てる固定バッファスペースの量
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術(シェーピング、共有、または両方)

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」(P.33-67)
- 「出力キューセットに対するバッファスペースの割り当ておよび WTD しきい値の設定」(P.33-68) (任意)
- 「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.33-70)(任意)
- 「出力キューでの SRR シェーピング重みの設定」(P.33-71)(任意)
- 「出力キューでの SRR 共有重みの設定」(P.33-72)(任意)
- 「出力緊急キューの設定」(P.33-73)(任意)
- 「出力インターフェイスの帯域幅の制限」(P.33-74)(任意)

設定時の注意事項

緊急キューをイネーブルにする、または SRR の重みに基づいて出力キューを処理する場合は、次の注 意事項に従ってください。

- 出力緊急キューがイネーブルの場合、キュー1に対応する SRR シェーピング重みおよび共有重み は上書きされます。
- 出力緊急キューがディセーブルで、SRR シェーピング重みおよび共有重みが設定されている場合、 シェーピングモードはキュー1の共有モードを無効にし、SRR はこのキューをシェーピングモー ドで処理します。
- 出力緊急キューがディセーブルで、SRR シェーピング重みが設定されていない場合、SRR はこの キューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファのアベイラビリティの保証、WTD の設定、およびキューセットの最大割り当ての設定を行う には、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* グローバル コンフィギュレーション コマンド を使用します。

各しきい値はキューに割り当てられたバッファの割合です。このパーセント値を指定するには、mls qos queue-set output *qset-id* buffers *allocation1* ... *allocation4* グローバル コンフィギュレーション コ マンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なる廃棄割合をサ ポートします。

(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

メモリ割り当てを設定し、キューセットのを廃棄するには、特権 EXEC モードで次の手順を実行しま す。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos queue-set output <i>qset-id</i> buffers allocation1 allocation4	キューセットにバッファを割り当てます。 デフォルトでは、すべての割り当て値は4つのキューに均等にマッピ ングされます(25、25、25、25)。各キューにはバッファスペースの 1/4 が割り当てられます。
		 <i>qset-id</i>には、キューセットの ID を入力します。指定できる範囲は1~2です。各ポートはキューセットに属し、キューセットでは、ポートごとに4つの出力キューの特性がすべて定義されます。
		 allocation1 allocation4 には、キューセット内のキューごとに 1 つずつ、合計4 つのパーセントを指定します。allocation1、 allocation3、allocation4 の場合、使用可能な範囲は0~99で す。allocation2 の場合、使用可能な範囲は1~100です(CPU バッファを含む)。
		トラフィックの重要性に従ってバッファを割り当てます。たとえば、 プライオリティが最も高いトラフィックを格納するキューに、大きな 割合のバッファを割り当てます。

	コマンド	目的
ステップ 3	mls qos queue-set output <i>qset-id</i> threshold <i>queue-id drop-threshold1</i> <i>drop-threshold2 reserved-threshold</i> <i>maximum-threshold</i>	WTD を設定し、バッファのアベイラビリティを保証し、キューセット(ポートごとに 4 つの出力キュー)の最大メモリ割り当てを設定します。
		デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定さ れています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべての キューの最大は 400% に設定されています。
		 <i>qset-id</i>には、ステップ2で指定したキューセットの ID を入力します。指定できる範囲は1~2です。
		 queue-id には、コマンドの実行対象となるキューセット内の特定のキューを入力します。指定できる範囲は1~4です。
		 <i>drop-threshold1 drop-threshold2</i>には、キューの割り当てメモリの割合として表される2つのWTDを指定します。指定できる範囲は1~3200%です。
		 reserved-threshold には、割り当てメモリの割合として表される キューに保証(確保)されるメモリ サイズを入力します。指定で きる範囲は1~100%です。
		 maximum-threshold を指定すると、いっぱいになったキューが確保量を超えるバッファを取得できるようになります。この値は、共通プールが空でない場合に、パケットが廃棄されるまでキューが使用できるメモリの最大値です。指定できる範囲は1~3200%です。
ステップ 4	interface interface-id	発信トラフィックのポートを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
ステップ 5	queue-set qset-id	キューセットにポートをマッピングします。
		<i>qset-id</i> には、ステップ 2 で指定したキューセットの ID を入力しま す。指定できる範囲は 1 ~ 2 です。デフォルトは 1 です。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show mls qos interface [interface-id] buffers	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no mls qos queue-set output *qset-id* buffers グローバル コンフィギュ レーション コマンドを使用します。デフォルトの WTD の割合に戻すには、no mls qos queue-set output *qset-id* threshold [*queue-id*] グローバル コンフィギュレーション コマンドを使用します。

次に、ポートをキューセット2にマッピングする例を示します。出力キュー1にはバッファスペースの40%、出力キュー2、3、および4には20%が割り当てられます。キュー2の廃棄は割り当てメモリの40および60%に設定され、割り当てメモリの100%が保証(確保)され、パケットが廃棄されるまでこのキューが使用できる最大メモリが200%に設定されます。

Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet0/1
lSwitch(config-if)# queue-set 2

出力キューおよび ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定の キューに格納し、より低いプライオリティを持つパケットが廃棄されるようにキューのを調整します。

(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

DSCP または CoS 値を出力キューおよび ID にマッピングするには、特権 EXEC モードで次の手順を 実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscpl_dscp8	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。
	または mls qos srr-queue output cos-map queue queue.id threshold threshold.id	デフォルトでは、DSCP 値 0 ~ 15 はキュー 2 およびしきい値 1 に、 DSCP 値 16 ~ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ~ 39 および 48 ~ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ~ 47 はキュー 1 およびしきい値 1 にマッピングされます。
	cos1cos8	デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、 CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、お よび 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 および しきい値 1 にマッピングされます。
		 queue-id に指定できる範囲は、1~4です。
		 <i>threshold-id</i>の範囲は、1~3です。3の廃棄の割合は定義済みであり、キューフルステートに設定されます。
		 <i>dscp1dscp8</i>には、最大8つの値をスペースで区切って入力します。指定できる範囲は0~63です。
		 cos1cos8 には、最大8つの値をスペースで区切って入力します。指定できる範囲は0~7です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show mls qos maps	設定を確認します。
		DSCP 出力キューしきい値マップは、表形式で表示されます。dl 列 は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。dl および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、 キュー 2 およびしきい値 1 (02-01) のようになります。
		CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番めの行 に対応するキュー ID およびしきい値 ID が示されます。たとえば、 キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに 戻すには、no mls qos srr-queue output dscp-map または no mls qos srr-queue output cos-map グ ローバル コンフィギュレーション コマンドを使用します。

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

Switch(config) # mls qos srr-queue output dscp-map queue 1 threshold 2 10 11

出力キューでの SRR シェーピング重みの設定

各キューに割り当てられる使用可能な帯域幅の量を指定できます。重みの比率は、SRR スケジューラ が各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックを平滑化したり、出力をより滑らかにしたりするには、シェーピングを使用します。シェーピング重みの詳細については、「SRR のシェーピングおよび共有」(P.33-14)を参照してください。共有重みの詳細については、「出力キューでの SRR 共有重みの設定」(P.33-72)を参照してください。

ポートにマッピングされた4つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピング をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	発信トラフィックのポートを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
ステップ 3	srr-queue bandwidth shape weight1	出力キューに SRR 重みを割り当てます。
	weight2 weight3 weight4	デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。
		weight1 weight2 weight3 weight4 には、シェーピングされるポートの 割合を制御する重みを入力します。このキューのシェーピング帯域幅 は、インバース比率(1 /weight)によって制御されます。各値はス ペースで区切ります。指定できる範囲は $0 \sim 65535$ です。
		重み0を設定した場合は、対応するキューが共有モードで動作しま す。srr-queue bandwidth shape コマンドで指定された重みは無視さ れます。srr-queue bandwidth share インターフェイス コンフィギュ レーション コマンドで各キューに指定された重みが有効になります。 シェーピングおよび共有の両方に対して同じキューセットのキューを 設定した場合は、必ず番号が最も小さいキューにシェーピングを設定 してください。
		シェーピング モードは共有モードより優先されます。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface interface-id queueing	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no srr-queue bandwidth shape インターフェイス コンフィギュレー ション コマンドを使用します。 次に、キュー1に帯域幅のシェーピングを設定する例を示します。キュー2、3、および4の重み比率 は0に設定されているため、これらのキューは共有モードで動作します。キュー1の帯域幅の重みは 1/8(12.5%)です。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0

出力キューでの SRR 共有重みの設定

共有モードでは、各キューは設定された重みに従って帯域幅を共有します。帯域幅に対してはこのレベ ルが保証されますが、このレベルに限定されるわけではありません。たとえば、特定のキューが空であ り、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。 共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は 関係ありません。

(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

ポートにマッピングされた4つの出力キューに共有重みを割り当てて、帯域幅の共有をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	発信トラフィックのポートを指定し、インターフェイス コンフィ ギュレーション モードを開始します。
ステップ 3	srr-queue bandwidth share weight1	出力キューに SRR 重みを割り当てます。
	weight2 weight3 weight4	デフォルトでは、4 つの重みがすべて 25 です(各キューに帯域幅の 1/4 が割り当てられています)。
		weight1 weight2 weight3 weight4 には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は $1 \sim 255$ です。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show mls qos interface interface-id queueing	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no srr-queue bandwidth share インターフェイス コンフィギュレー ション コマンドを使用します。

次に、出力ポートで稼動している SRR スケジューラの重み比率を設定する例を示します。4 つの キューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー1、2、3、および 4 に対して 1/(1+2+3+4)、2/(1+2+3+4)、3/(1+2+3+4)、および 4/(1+2+3+4) になります (それぞれ、10、20、30、および 40%)。つまり、キュー4の帯域幅はキュー1の4倍、キュー2の2 倍、キュー3の約1.3倍です。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のすべてのパケットより高く設定できます。SRR は、このキューが空になるまで処理してから他のキューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	mls qos	スイッチ上で QoS をイネーブルにします。
ステップ 3	interface interface-id	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	priority-queue out	デフォルトでディセーブルに設定されている出力緊急キューをイネー ブルにします。
		このコマンドを設定すると、SRR に参加するキューは1つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、 <i>srr-queue bandwidth shape</i> または srr-queue bandwidth share コマンドの weight1 が無視されます(比率計算に使用されません)。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

出力緊急キューをディセーブルにするには、no priority-queue out インターフェイス コンフィギュ レーション コマンドを使用します。

次に、SRR 重みが設定されている場合に出力緊急キューをイネーブルにする例を示します。出力緊急 キューは、設定済みの SRR 重みよりも優先されます。

Switch(config) # interface gigabitethernet0/1
Switch(config-if) # srr-queue bandwidth shape 25 0 0 0
Switch(config-if) # srr-queue bandwidth share 30 20 25 25
Switch(config-if) # priority-queue out
Switch(config-if) # end

出力インターフェイスの帯域幅の制限

出力ポートの帯域幅は制限できます。たとえば、カスタマーが高速リンクの一部しか費用を負担しない 場合は、帯域幅をその量に制限できます。

(注)

ほとんどの場合は、出力キューのデフォルト設定が最適です。デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびこれらの設定がご使用の QoS ソリューションを満たしていない場合のみです。

出力ポートの帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	レートを制限するポートを指定し、インターフェイス コンフィギュ レーション モードを開始します。
ステップ 3	srr-queue bandwidth limit weight1	ポートの上限となるポート速度の割合を指定します。指定できる範囲 は 10 ~ 90 です。
		デフォルトでは、ポートのレートは制限されず、100% に設定されて います。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	<pre>show mls qos interface [interface-id] queueing</pre>	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、no srr-queue bandwidth limit インターフェイス コンフィギュレー ション コマンドを使用します。

次に、ポートの帯域幅を80%に制限する例を示します。

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth limit 80

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。回線レートは接続速度の 80% (800 Mbps) に低下します。ハードウェアは回線レートを増分値 6 で調整するので、これらは厳密な値ではありません。

標準 QoS 情報の表示

標準 QoS 情報を表示するには、表 33-15 の特権 EXEC コマンドを1 つまたは複数使用します。

表 33-15 標準 QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [class-map-name]	トラフィックを分類するための一致条件を定義した QoS クラス マップを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos aggregate-policer [aggregate-policer-name]	集約ポリサーの設定を表示します。
show mls qos input-queue	入力キューの QoS 設定を表示します。
show mls qos interface [<i>interface-id</i>] [buffers policers queueing statistics]	バッファ割り当て、ポリサーが設定されるポート、キューイン グ方式、入出力統計情報など、ポート レベルの QoS 情報が表 示されます。
show mls qos maps [cos-dscp cos-input-q cos-output-q dscp-cos dscp-input-q dscp-mutation dscp-mutation-name dscp-output-q ip-prec-dscp policed-dscp]	QoS マッピング情報を表示します。
show mls qos queue-set [qset-id]	出力キューの QoS 設定を表示します。
<pre>show policy-map [policy-map-name [class class-map-name]]</pre>	着信トラフィックの分類条件を定義した QoS ポリシー マップ を表示します。
	 (注) 着信トラフィックの分類情報を表示する場合は、show policy-map interface 特権 EXEC コマンドを使用しな いでください。control-plane および interface キー ワードはサポートされていません。表示される統計情報 は無視してください。
show running-config include rewrite	透過的な DSCP 設定を表示します。

■ 標準 QoS 情報の表示





IPv6ホスト機能の設定

(注)

IPv6 ホスト機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

2960 この章では、Catalyst スイッチに、IPv6 ホスト機能を設定する方法について説明します。

IPv6 Multicast Listener Discovery (MLD) スヌーピングの設定の詳細については、第 35 章「IPv6 MLD スヌーピングの設定」を参照してください。

デュアル スタック環境(IPv4 と IPv6 の両方をサポートする)をイネーブルにするには、Switch Database Management (SDM; スイッチング データベース管理) テンプレートをデュアル IPv4 および IPv6 テンプレートに設定する必要があります。「デュアル IPv4/IPv6 プロトコル スタック」(P.34-5) を参照してください。



この章で説明するコマンドの構文および使用方法の詳細については、手順に記載された Cisco IOS のマ ニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「IPv6 の概要」(P.34-2)
- 「IPv6 の設定」(P.34-7)
- 「IPv6 の表示」(P.34-13)

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality Of Service (QoS; サービス品質)、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 ア ドレス スペースでは、プライベート アドレスの必要性、およびネットワーク エッジ上の境界ルータで の Network Address Translation (NAT; ネットワーク アドレス変換)処理の必要性が軽減されます。

シスコシステムズの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

この章の IPv6 および他の機能の詳細については、

- 次のURLにある『Cisco IOS IPv6 Configuration Library』を参照してください。 http://www.cisco.com/en/US/docs/ios/12 2t/ipv6/ipv6 vgf.html
- Cisco IOS ソフトウェア マニュアルを検索するには、検索フィールドを使用します。たとえば、ス タティック ルートに関する情報を取得する場合は、検索フィールドに「*Implementing Static Routes for IPv6*」と入力してスタティック ルートに関する資料を取得します。
 http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Prod ucts Configuration Guide Chapter.html

ここでは、スイッチへの IPv6 の実装について説明します。内容は次のとおりです。

- 「IPv6 アドレス」 (P.34-2)
- 「サポート対象の IPv6 ホスト機能」(P.34-3)

IPv6 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスだけです。スイッチはサイトローカルなユ ニキャスト アドレス、エニキャスト アドレス、またはマルチキャスト アドレスをサポートしません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド (n:n:n:n:n:n:n:n:n:n:n) の形式) で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略 した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン(::)を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この 短縮形を使用できるのは、各アドレス内で1回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス フォーマット、アドレス タイプ、および **IPv6** パケット ヘッダーの詳細については、 Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Implementing Addressing and Basic Connectivity」の章では、次のセクションの内容は Catalyst 2960 スイッチに適用されます。

- 「IPv6 Address Formats」
- 「IPv6 Address Output Display」
- 「Simplified IPv6 Packet Header」

サポート対象の IPv6 ホスト機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

- 「128 ビット幅のユニキャスト アドレス」(P.34-3)
- 「IPv6 用 DNS」 (P.34-4)
- **[ICMPv6]** (P.34-4)
- 「近接ディスカバリ」(P.34-4)
- 「IPv6 のステートレス自動設定および重複アドレス検出」(P.34-4)
- 「IPv6 アプリケーション」 (P.34-4)
- 「デュアル IPv4/IPv6 プロトコル スタック」(P.34-5)
- 「IPv6 による SNMP および Syslog」(P.34-6)
- 「IPv6 による HTTP (S)」 (P.34-7)

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサ ポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単 位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジング します。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャス ト アドレスをサポートします。サイトに対してローカルなユニキャスト アドレスはサポートされてい ません。

集約可能なグローバルユニキャストアドレスは、集約可能グローバルユニキャストプレフィクスの付いた IPv6アドレスです。このアドレス構造を使用すると、ルーティングプレフィクスを厳格に集約することができ、グローバルルーティングテーブル内のルーティングテーブルエントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネットサービスプロバイダーに至る集約リンク上で使用されます。

これらのアドレスはグローバル ルーティング プレフィクス、サブネット ID、およびインターフェ イス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ 値 001 (2000::/3) で開始するアドレス範囲が使用されます。プレフィクスが 2000::/3 (001) ~ E000::/3 (111) のアドレスには、Extended Unique Identifier (EUI) 64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

リンクに対してローカルなユニキャストアドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンクに対してローカルなプレフィクス FE80::/10(1111111010)およびインターフェイス ID を使用します。Neighbor Discovery Protocol (NDP; 近接ディスカバリプロトコル)およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。ローカルリンク上のノードは、リンクに対してローカルなアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com から『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addressing and Basic Connectivity」章の、「IPv6 Unicast Addresses」を参照してください。

IPv6 用 DNS

IPv6 は、Domain Name System (DNS; ドメイン ネーム システム) のレコード タイプを、DNS 名前/ アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイ プは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

ICMPv6

IPv6 の Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) は、 ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、そ の他の診断機能を報告します。IPv6 では、近接ディスカバリ プロトコルおよびパス MTU ディスカバ リに ICMP パケットも使用されます。

近接ディスカバリ

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼動するプロトコル、および NDP をサポートし ない IPv6 ステーション対応のスタティック ネイバ エントリをサポートします。IPv6 NDP は ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク(ローカル リンク)上のネイバのリンクレイヤ アドレスを判別し、ネイバに到達できるかどうかを確認し、近接 ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マス ク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされま せん。

近接ディスカバリスロットリングにより、IPv6パケットをルーティングするためにネクストホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバである場合は、そのようなパケットが追加されると、スイッチはそのパケットを廃棄します。この廃棄により、CPU に余分な 負荷がかからないようになります。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、traceroute、Telnet、Trivial File Transfer Protocol (TFTP)、および FTP (ファイル転送プロトコル)
- IPv6 トランスポートによる Secure Shell (SSH; セキュア シェル)
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ

• IPv6 アドレスの Cisco Discovery Protocol (CDP) サポート

これらのアプリケーションの詳細については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

デュアル IPv4/IPv6 プロトコル スタック

IPv4 および IPv6 プロトコルの両方で Ternary Content Addressable Memory (TCAM)の使用を割り当 てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

図 34-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。





デュアル IPv4/IPv6 スイッチング データベース管理(SDM)テンプレートを使用すると、(IPv4 と IPv6 の両方をサポートする)デュアル スタック環境をイネーブルにできます。デュアル IPv4/IPv6 SDM テンプレートについての詳細は、「第7章「SDM テンプレートの設定」」を参照してください。

IPv4/IPv6 テンプレートを使用することにより、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッ セージが表示されます。
- IPv4 専用環境で、スイッチは Ipv4 QoS および ACL をハードウェアで適用します。IPv6 パケット はサポートされません。
- デュアル IPv4/IPv6 環境で、スイッチは IPv4 QoS および ACL をハードウェアで適用します。
- IPv6 QoS および ACL はサポートされていません。
- デュアル スタック テンプレートを使用すると各リソースの TCAM 容量が少なくなるので、IPv6 を使用しない場合はデュアル スタック テンプレートを使用しないでください。

IPv4/IPv6 プロトコル スタックについての詳細は、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義 します。スタティック ルートが有効なのは、外部ネットワークへのパスが1 つしかない小規模ネット ワークの場合は、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する 場合です。

スタティック ルートの詳細については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 による SNMP および Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランス ポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサ ポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバーとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定の User Datagram Protocol (UDP; ユーザ データグラム プロトコル) SNMP ソ ケットを開く
- SR IPV6 TRANSPORT と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 に関連する SNMP については、Cisco.com から『Cisco IOS IPv6 Configuration Library 』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP(S)

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバ は IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレ スを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソ ケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク レイヤ相互作用を処理するためのソケットが必要です。

HTTP 接続が確立するためには、基本ネットワーク接続(ping) がクライアントとサーバ ホストとの 間に存在する必要があります。

詳細については、Cisco.com から『Cisco IOS IPv6 Configuration Library』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

IPv6 の設定

ここでは、次の IPv6 転送の設定情報について説明します。

- 「IPv6のデフォルト設定」(P.34-7)
- 「IPv6 アドレス指定の設定および IPv6 ホストのイネーブル化」(P.34-8)
- 「IPv6 ICMP レート制限の設定」(P.34-10)
- 「IPv6 のスタティック ルートの設定」(P.34-11)

IPv6 のデフォルト設定

表 34-1 に IPv6 のデフォルト設定を示します。

表 34-1 IPv6 のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルト
IPv6 アドレス	未設定

IPv6 アドレス指定の設定および IPv6 ホストのイネーブル化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ 上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- ipv6 address インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコ ロン区切りの 16 進形式で指定したアドレスで指定した ipv6-address 変数および ipv6-prefix 変数を 入力する必要があります。prefix-length 変数(スラッシュ(/) で始まる)は、プレフィクス(ア ドレスのネットワーク部分)を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクに対 してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的 に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グルー プに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャストアドレスの送信要求ノードマルチキャストグ ループ FF02:0:0:0:1:ff00::/104(このアドレスは近接ディスカバリプロセスで使用される)
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

IPv6 の設定の詳細については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

IPv6 アドレスをレイヤ 3 インターフェイスに割り当てて、IPv6forwarding をイネーブルにするには、 特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	sdm prefer dual-ipv4-and-ipv6 default	• IPv4 および IPv6 をサポートする SDM テンプレートを 選択します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	reload	OS(オペレーティング システム)をリロードします。
ステップ 5	configure terminal	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	interface interface-id	インターフェイス コンフィギュレーション モードを開始し、 設定するインターフェイスを指定します。

	コマンド	目的
ステップ 7	ipv6 address ipv6-prefix/prefix length eui-64 または ipv6 address ipv6-address link-local または ipv6 enable	IPv6 アドレスの下位 64 ビットの Extended Unique Identifier (EUI) を使用して、グローバル IPv6 アドレスを指定しま す。ネットワーク プレフィクスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算さ れます。これにより、インターフェイス上で IPv6 処理がイ ネーブルになります。 インターフェイスで IPv6 がイネーブルな場合に自動設定さ れる、リンクに対してローカルなアドレスでなく、インター フェイス上の特定の、リンクに対してローカルなアドレスを 使用するように指定します。このコマンドにより、インター
		インターフェイスに IPv6 リンクに対してローカルなアドレ スを自動設定し、インターフェイスでの IPv6 処理をイネー ブルにします。リンクに対してローカルなアドレスを使用で きるのは、同じリンク上のノードと通信する場合だけです。
ステップ 8	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	end	特権 EXEC モードに戻ります。
ステップ 10	show ipv6 interface interface-id	設定を確認します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

インターフェイスから IPv6 アドレスを削除するには、no ipv6 address *ipv6-prefix/prefix length* eui-64 or no ipv6 address *ipv6-address* link-local インターフェイス コンフィギュレーション コマンドを使用 します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、no ipv6 address インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレス で明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、no ipv6 enable インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグロー バルにディセーブルにするには、no ipv6 unicast-routing グローバル コンフィギュレーション コマン ドを使用します。

次に、IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよび グローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。両方のアドレスの下位 64 ビットでは、EUI-64 インターフェイス ID が使用されます。show ipv6 interface EXEC コマンドの出 力は、インターフェイスのリンクに対してローカルなプレフィクス FE80::/64 にインターフェイス ID (20B:46FF:FE2F:D940) を付加する方法を示しています。

```
Switch(config) # sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if) # end
Switch# show ipv6 interface gigabitethernet0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
 2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
 Joined group address(es):
   FF02::1
   FF02::2
   FF02::1:FF2F:D940
 MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv6のDRPの設定についての詳細は、Cisco.comから『Cisco IOS IPv6 Configuration Library』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、 デフォルト バケット サイズ (バケットに格納される最大トークン数) は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 icmp error-interval interval [bucketsize]	IPv6 ICMP エラー メッセージの間隔およびバケット サイズ を設定します。
		 <i>interval</i>:バケットに追加されるトークンの間隔(ミリ 秒)。指定できる範囲は0~2147483647 ミリ秒です。
		 <i>bucketsize</i>:(任意)バケットに格納される最大トークン数。指定できる範囲は1~200です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	<pre>show ipv6 interface [interface-id]</pre>	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

デフォルト設定に戻すには、no ipv6 icmp error-interval グローバル コンフィギュレーション コマン ドを使用します。

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例 を示します。

Switch(config) **#ipv6 icmp error-interval 50 20**

IPv6 のスタティック ルートの設定

IPv6 スタティックルートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ipv6 route ipv6-prefix/prefix length {ipv6-address interface-id [ipv6-address]} [administrative distance]	スタティック IPv6 ルートを設定します。	
	 <i>ipv6-prefix</i>:スタティックルートの宛先となる IPv6 ネット ワーク。スタティックホストルートを設定する場合は、ホ スト名も設定できます。 	
	 /prefix length : IPv6 プレフィクスの長さ。プレフィクス (アドレスのネットワーク部分)を構成するアドレスの上位 連続ビット数を示す 10 進値です。10 進値の前にスラッシュ を付加する必要があります。 	
	 <i>ipv6-address</i>:指定したネットワークに到達するために使用 可能なネクストホップの IPv6 アドレス。ネクストホップの IPv6 アドレスを直接接続する必要はありません。再帰処理 が実行されて、直接接続されたネクストホップの IPv6 アド レスが検出されます。このアドレスは、16 ビット値をコロ ンで区切った 16 進数で指定する必要があります。 	
		 interface-id: Point-To-Point (ポイントツーポイント) イン ターフェイスおよびブロードキャスト インターフェイスか らのダイレクト スタティック ルートを指定します。ポイン トツーポイント インターフェイスの場合、ネクスト ホップ の IPv6 アドレスを指定する必要はありません。ブロード キャスト インターフェイスの場合は、常にネクスト ホップ の IPv6 アドレスを指定するか、または指定したプレフィク スをリンクに割り当てて、リンクに対してローカルなアドレ スをネクスト ホップとして指定する必要があります。パ ケットの送信先となるネクスト ホップの IPv6 アドレスを指 定することもできます。
	 (注) リンクに対してローカルなアドレスをネクストホップとして使用する場合は、interface-id を指定する必要があります(リンクに対してローカルなネクストホップを隣接ルータに設定する必要もあります)。 	
		 administrative distance: (任意) 管理ディスタンス。指定できる範囲は1~254 です。デフォルト値は1で、この場合、接続されたルートを除くその他のどのルートタイプよりも、スタティックルートが優先します。フローティングスタティックルートを設定する場合は、ダイナミックルーティングプロトコルよりも大きな管理ディスタンスを使用します。
ステップ 3	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	show ipv6 static [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>] [interface <i>interface-id</i>] [recursive] [detail]	 IPv6 ルーティング テーブルの内容を表示して、設定を確認します。 interface interface-id:(任意)出力インターフェイスとして 指定されたインターフェイスを含むスタティック ルートの
	または show ipv6 route static [updated]	みを表示します。 recursive:(任意)再帰スタティックルートのみを表示します。recursive キーワードは interface キーワードと相互に 排他的です。ただし、コマンド構文に IPv6 プレフィクスが 指定されているかどうかに関係なく、使用することができます。
		 detail:(任意)次に示す追加情報を表示します。 有効な再帰ルートの場合、出力パス セットおよび最大 分解深度 無効なルートの場合、ルートが無効な理由
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

設定されたスタティック ルートを削除するには、**no ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] グローバル コンフィギュレーション コマンドを 使用します。

次に、管理ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する 例を示します。

Switch(config) # ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。
IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照して ください。

表 34-2 に、スイッチ上で IPv6 を監視するための特権 EXEC コマンドを示します。

表 34-2 IPv6 の監視用コマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 interface interface-id	IPv6 インターフェイスのステータスおよび設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバ キャッシュ エントリを表示します。
show ipv6 prefix-list	IPv6 プレフィクス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 34-3 に、IPv4 および IPv6 のアドレス タイプに関する情報を表示するための特権 EXEC コマンドを 示します。

表 34-3 IPv4 および IPv6 のアドレス タイプの表示用コマンド

コマンド	目的
show ip http server history	アクセスした IP アドレス、接続が終了したときの時間を含む、最近 20 回の HTTP サーバへの接続を表示します。
show ip http server connection	アクセスしているローカルおよびリモート IP アドレスを含む、HTTP サーバへの現在の接続を表示します。
show ip http client connection	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
show ip http client history	サーバに対して HTTP クライアントが行った最後の 20 回の要求のリスト を表示します。

次に、show ipv6 interface 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
```

```
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
<output truncated>
```

次に、show ipv6 protocols 特権 EXEC コマンドの出力例を示します。

Switch# show ipv6 protocols

```
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
Interfaces:
Vlan6
FastEthernet0/4
FastEthernet0/11
FastEthernet0/12
Redistribution:
None
```

次に、show ipv6 static 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1
```

次に、show ipv6 neighbor 特権 EXEC コマンドの出力例を示します。

Switch# show ipv6 neighbors				
IPv6 Address	Age	Link-layer Addr	State	Interface
3FFE:C000:0:7::777	-	0007.0007.0007	REACH	Vl7
3FFE:C101:113:1::33	-	0000.0000.0033	REACH	Fa1/0/13

次に、show ipv6 route 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L FF00::/8 [0/0]
via Null0, receive
```

次に、show ipv6 traffic 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 traffic
IPv6 statistics:
 Rcvd: 1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
 Sent: 36861 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
        0 RPF drops, 0 RPF suppressed drops
 Mcast: 1 received, 36861 sent
ICMP statistics:
 Rcvd: 1 input, 0 checksum errors, 0 too short
       0 unknown info type, 0 unknown error type
       unreach: O routing, O admin, O neighbor, O address, O port
       parameter: 0 error, 0 header, 0 option
```

```
0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: O routing, O admin, O neighbor, O address, O port
parameter: O error, O header, O option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        O group query, O group report, O group reduce
        O router solicit, 9944 router advert, O redirects
        84 neighbor solicit, 84 neighbor advert
UDP statistics:
 Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output
TCP statistics:
 Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

■ IPv6 の表示





IPv6 MLD スヌーピングの設定

(注)

この IPv6 MLD スヌーピングを使用するには、スイッチが LAN Base イメージを実行している必要があります。



Catalyst2960 スイッチ上で、Multicast Listener Discovery(MLD)スヌーピングを使用すれば、ス イッチド ネットワーク内のクライアントおよびルータへ IP Version 6(IPv6)マルチキャスト データ を効率的に配信することができます。IPv6 を使用するには、デュアル IPv4 および IPv6 Switching Database Management(SDM; スイッチング データベース管理)テンプレートが設定されている必要 があります。テンプレートの選択は、sdm prefer dual-ipv4-and-ipv6 default グローバル コンフィ ギュレーション コマンドを入力しておこないます。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、「第7章「SDM テンプレートの設定」」を参照してください。
- スイッチの IPv6 については、「第 34 章「IPv6 ホスト機能の設定」」を参照してください。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

この章で説明する内容は、次のとおりです。

- 「MLD スヌーピングの概要」(P.35-2)
- 「IPv6 MLD スヌーピングの設定」(P.35-5)
- 「MLD スヌーピング情報の表示」(P.35-13)

MLD スヌーピングの概要

IP バージョン4 (IPv4) では、レイヤ2スイッチは Internet Group Management Protocol (IGMP; イ ンターネット グループ管理プロトコル) スヌーピングを使用して、ダイナミックにレイヤ2インター フェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。その ため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイス にだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピング を使用すると、IPv6 マルチキャスト データは VLAN (仮想 LAN) 内のすべてのポートにフラッディ ングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、 IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、直接接続されたリンク上のマルチ キャスト リスナー(IPv6 マルチキャストパケットを受信するノード)の存在、および隣接ノードを対 象とするマルチキャストパケットを検出します。MLD は IGMP から派生しています。MLD バージョ ン1(MLDv1)は IGMPv2 と、MLD バージョン2(MLDv2)は IGMPv3 とそれぞれ同等です。 MLD は ICMP バージョン 6(ICMPv6)のサブプロトコルです。MLD メッセージは ICMPv6 メッ セージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の2つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング: MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 Basic Snooping (MBSS): MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、 IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。



スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 Enhanced Snooping (MESS) をサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できま す。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト MAC アドレス テー ブルはソフトウェアで構築され、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェ アおよびハードウェアで構築されます。そのあと、スイッチはハードウェアで IPv6 マルチキャストア ドレスに基づくブリッジングを実行します。

次に、IPv6 MLD スヌーピングの一部のパラメータについて説明します。

- 「MLD メッセージ」 (P.35-3)
- 「MLD クエリー」 (P.35-3)
- 「マルチキャスト クライアント エージングの堅牢性」(P.35-4)
- 「マルチキャストルータ検出」(P.35-4)
- 「MLD レポート」 (P.35-4)
- 「MLD Done メッセージおよび即時脱退」(P.35-5)
- 「TCN 処理」(P.35-5)

MLD メッセージ

MLDv1は、次の3種類のメッセージをサポートします。

- Listener Query: IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query (MASQ)のいずれかになります。
- Multicast Listener Report: IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ: IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レ ポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの 場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージ は、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グ ループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに 応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタ ティックな IPv6 マルチキャスト MAC アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングさ れ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエ リーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチ キャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、 VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアド レス エージングを維持します。

(注)

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が使用 されている場合は、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるように、Catalyst 6500 スイッチの拡張 VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイ ネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ (IGMP Leave メッセー ジと同等)を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネー ブルでなければ、スイッチは メッセージを受信したポートに MASQ を送信して、ポートに接続する他 のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバシップの削除を設定できます。1 つのアドレスに 対するメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレ スに対するレポートがない場合のみです。デフォルト値は2です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより 行われます。
- 複数のルータが同じレイヤ2インターフェイス上にある場合、MLDスヌーピングではポート上の 単一のマルチキャストルータ(直前にルータ制御パケットを送信したルータ)を追跡します。
- マルチキャストルータポートのダイナミックなエージングは、デフォルトタイマーの5分に基づきます。ポート上で制御パケットが5分間受信されない場合、マルチキャストルータはルータのポートリストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブル の場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネー ブルかどうかに関わらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出されたあとは、不明の IPv6 マルチキャスト デー タは、検出されたルータ ポートに対してのみ転送されます(それまでは、すべての IPv6 マルチ キャスト データは入力 VLAN にフラッディングされます)。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されま せん。IPv6 マルチキャスト ルータが検出され、MLDv1 レポート が受信されると、IPv6 マルチキャ スト グループ アドレスおよび IPv6 マルチキャスト MAC アドレスが VLAN の MLD データベースに 入力されます。そのあと、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィック が、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入 力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制(リスナー メッセージ抑制) は自動的 にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レ ポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信さ れません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべて の MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、ス イッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後の メンバー ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポート で応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ(IGMP Leave メッセージと同 等)を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は(IGMP スヌーピングと同様に)、ポートに単一のホストが接続 されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバーである場合、グ ループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に(1 つのポート上にグループのクライアントが複数ある場合)、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、ipv6 mld snooping last-listener-query count により設定されます。デフォル ト値は 2 です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの 最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、 MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応 答時間は、ipv6 mld snooping last-listener-query-interval により設定されます。削除されたポートが マルチキャスト アドレスの最後のメンバーである場合は、マルチキャスト アドレスも削除され、ス イッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit を使用して、Topology Change Notification (TCN; トポロジ変更 通知)送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーに よりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、 選択されたポートにのみマルチキャスト データの送信を開始します。この値は、ipv6 mld snooping tcn flood query count を使用して設定します。デフォルトでは、2 つのクエリーが送信されます。ス イッチが VLAN 内の Spanning-Tree Protocol (STP; スパニング ツリー プロトコル) ルートになる場 合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元 アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場 合と同じです。

IPv6 MLD スヌーピングの設定

次に、IPv6 MLD スヌーピングの設定方法について説明します。

- 「MLD スヌーピングのデフォルト設定」(P.35-6)
- 「MLD スヌーピング設定時の注意事項」(P.35-6)
- 「MLD スヌーピングのイネーブル化またはディセーブル化」(P.35-7)
- 「スタティックなマルチキャスト グループの設定」(P.35-8)
- 「マルチキャスト ルータ ポートの設定」(P.35-9)
- 「MLD 即時脱退のイネーブル化」(P.35-10)
- 「MLD スヌーピング クエリーの設定」(P.35-10)
- 「MLD リスナー メッセージ抑制のディセーブル化」(P.35-12)

MLD スヌーピングのデフォルト設定

表 35-1 に、MLD スヌーピングのデフォルト設定を示します。

表 35-1 MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング(グローバル)	ディセーブル
MLD スヌーピング(VLAN 単位)	イネーブル VLAN MLD スヌーピングが実行されるためには、 MLD スヌーピングがグローバルにイネーブルである必要があり ます。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル:2、VLAN 単位:0
	(注) VLAN 値はグローバル設定を上書きします。VLAN 値 が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル:2、VLAN 単位:0
	(注) VLAN 値はグローバル設定を上書きします。VLAN 値 が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー	グローバル:1000 (1 秒)、VLAN:0
インターバル	(注) VLAN 値はグローバル設定を上書きします。VLAN 値 が 0 の場合、VLAN はグローバルのインターバルを使用 します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2
MLD リスナー抑制	イネーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、ipv6 mld snooping を使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が 使用されている場合は、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるように、 Catalyst 6500 スイッチの拡張 VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要があり ます。標準範囲 VLAN (1 ~ 1005)の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を 同時にイネーブルにできます。
- スイッチに保持可能なアドレスエントリの最大数は1000です。

MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定 はグローバル設定を上書きします。すなわち、MLD スヌーピングはデフォルト ステート(イネーブ ル)の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、 MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルにな ります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディ セーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順 を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping	スイッチで MLD スヌーピングをグローバルにイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 5	reload	OS (オペレーティング システム)をリロードします。

スイッチで MLD スヌーピングをグローバルにディセーブルにするには、no ipv6 mld snooping を使用 します。

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

(注)

IPv6 マルチキャスト ルータが Catalyst 6500 スイッチで、拡張 VLAN (1006 ~ 4094 の範囲) が使用 されている場合は、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるように、Catalyst 6500 スイッチの拡張 VLAN 上で IPv6 MLD スヌーピングをイネーブルにする必要があります。標準範囲 VLAN (1 ~ 1005) の場合は、Catalyst 6500 スイッチの VLAN 上で IPv6 MLD スヌーピングをイ ネーブルにする必要はありません。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	ipv6 mld snooping	スイッチで MLD スヌーピングをグローバルにイネーブルにします。	
ステップ 3	ipv6 mld snooping vlan vlan-id	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。	
		(注) VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。	
ステップ 4	end	特権 EXEC モードに戻ります。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

VLAN インターフェイスで MLD スヌーピングをディセーブルにするには、指定された VLAN 番号に 対して no ipv6 mld snooping vlan *vlan-id* を使用します。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ2ポートは、通常マルチキャスト グループにダイナミックに加入しますが、 VLAN に IPv6 マルチキャスト アドレスおよび メンバー ポートをスタティックに設定することもでき ます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping vlan vlan-id static ipv6_multicast_address interface interface-id	マルチキャスト グループのメンバーとしてレイヤ2ポートに マルチキャスト グループをスタティックに設定します。
		 vlan-id は、マルチキャスト グループの VLAN ID です。 VLAN ID の範囲は1~1001 および 1006~4094 です。
		 <i>ipv6_multicast_address</i>は、128ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された 形式でなければなりません。
		 <i>interface-id</i>は、メンバーポートです。物理インターフェイスまたはポートチャネル(1~48)に設定できます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping multicast-address user または show ipv6 mld snooping multicast-address vlan <i>vlan-id</i> user	スタティックなメンバー ポートおよび IPv6 アドレスを確認 します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存しま す。

マルチキャスト グループからレイヤ 2 ポートを削除するには、**no ipv6 mld snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* を使用します。グループからすべてのメンバー ポートが削除 された場合、このグループは削除されます。

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet0/1
Switch(config)# end

マルチキャスト ルータ ポートの設定

MLD スヌーピングでは、MLD クエリーおよび PIMv6 クエリーを介してルータ ポートについて学習し ますが、CLI (コマンドライン インターフェイス)を使用しても VLAN にマルチキャスト ルータ ポー トを追加できます。マルチキャスト ルータ ポートを追加する(マルチキャスト ルータにスタティック 接続を追加する)には、スイッチで ipv6 mld snooping vlan mrouter グローバル コンフィギュレー ション コマンドを使用します。

<u>~~</u> (注)

マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

コマンド 目的 ステップ 1 configure terminal グローバル コンフィギュレーション モードを開始します。 ステップ 2 ipv6 mld snooping vlan vlan-id mrouter マルチキャスト ルータの VLAN ID、およびマルチキャスト interface interface-id ルータにインターフェイスを指定します。 VLAN ID の範囲は1~1001および1006~4094です。 • インターフェイスは物理インターフェイスにすることも ポート チャネルにすることもできます。指定できるポー トチャネルの範囲は1~48です。 ステップ 3 end 特権 EXEC モードに戻ります。 ステップ 4 show ipv6 mld snooping mrouter [vlan VLAN インターフェイスで IPv6 MLD スヌーピングがイ vlan-id ネーブルになっていることを確認します。 ステップ 5 copy running-config startup-config (任意) コンフィギュレーション ファイルに設定を保存しま す。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

VLAN からマルチキャスト ルータ ポートを削除するには、**no ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* を使用します。

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# exit

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出すると ただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping vlan vlan-id	VLAN インターフェイス上で即時脱退がイネーブルになっている ことを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN で MLD 即時脱退をディセーブルにするには、no ipv6 mld snooping vlan *vlan-id* immediate-leave を使用します。

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit

MLD スヌーピング クエリーの設定

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポー トで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。 ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を 待機する時間を任意で設定できます。

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 mld snooping robustness-variable <i>value</i>	(任意) スイッチが一般クエリーに応答しないリスナー (ポート) を削除する前に、送信されるクエリー数を設定します。指定できる 範囲は1~3です。デフォルトは2です。
ステップ 3	ipv6 mld snooping vlan vlan-id robustness-variable value	(任意) VLAN 単位で堅牢性変数を設定します。これにより、 MLD レポート応答がない場合にマルチキャスト アドレスがエージ ング アウトされるまでに、MLD スヌーピングが送信する一般クエ リー数が決定されます。指定できる範囲は1~3です。デフォルト は0です。0に設定すると、使用される数はグローバルな堅牢性変 数の値になります。

	コマンド	目的
ステップ 4	ipv6 mld snooping last-listener-query-count <i>count</i>	(任意) MLD クライアントがエージング アウトされる前にスイッ チが送信する MASQ 数を設定します。指定できる範囲は1~7で す。デフォルトは2です。クエリーは1秒後に送信されます。
ステップ 5	ipv6 mld snooping vlan vlan-id last-listener-query-count count	(任意) VLAN 単位で最後のリスナー クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は1~7です。デフォルトは0です。0に設定すると、グローバルなカウント値が使用されます。クエリーは1秒後に送信されます。
ステップ 6	ipv6 mld snooping last-listener-query-interval interval	(任意) スイッチが MASQ を送信したあと、マルチキャスト グ ループからポートを削除するまで待機する最大応答時間を設定しま す。指定できる範囲は、100 ~ 32,768 ミリ秒です。デフォルト値 は 1000 (1 秒) です。
ステップ 7	ipv6 mld snooping vlan <i>vlan-id</i> last-listener-query-interval <i>interval</i>	(任意) VLAN 単位で最後のリスナー クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ~ 32,768 ミリ秒です。デフォルトは0です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	ipv6 mld snooping ten query solicit	(任意) TCN 送信請求をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラ フィックすべてをフラッディングしてから、マルチキャスト デー タをマルチキャスト データの受信を要求するポートに対してのみ 送信します。デフォルトでは、TCN はディセーブルに設定されて います。
ステップ 9	ipv6 mld snooping tcn flood query count <i>count</i>	(任意) TCN がイネーブルの場合、送信される TCN クエリー数を 指定します。指定できる範囲は 1 ~ 10 で、デフォルトは 2 です。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show ipv6 mld snooping querier [vlan vlan-id]	(任意) スイッチまたは VLAN の MLD スヌーピング クエリア情報 を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、MLD スヌーピングのグローバルな堅牢性変数を3に設定する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit

次に、MLD スヌーピングの最後のリスナー クエリー インターバル(最大応答時間)を 2000 (2 秒) に設定する例を示します。

Switch# configure terminal Switch(config)# ipv6 mld snooping last-listener-query-interval 2000 Switch(config)# exit

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no ipv6 mld snooping listener-message-suppression	MLD メッセージ抑制をディセーブルにします。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show ipv6 mld snooping	IPv6 MLD スヌーピング レポート抑制がディセーブルで あることを確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD メッセージ抑制を再びイネーブルにするには、ipv6 mld snooping listener-message-suppression を使用します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インター フェイスの MLD スヌーピング情報を表示できます。MLD スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

MLD スヌーピング情報を表示するには表 35-2 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 35-2 MLD スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [vlan vlan-id]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピ ング設定情報を表示します。
	(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入 力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ipv6 mld snooping mrouter [vlan vlan-id]	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブ ルにすると、スイッチはマルチキャスト ルータの接続先であるイン ターフェイスを自動的に学習します。これらのインターフェイスは動 的に学習されます。
	(任意) 個々の VLAN に関する情報を表示するには、 vlan <i>vlan-id</i> を入 力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ipv6 mld snooping querier [vlan <i>vlan-id</i>]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレス および着信ポートに関する情報を表示します。
	(任意) vlan <i>vlan-id</i> を入力して、単一の VLAN 情報を表示します。指 定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<pre>show ipv6 mld snooping multicast-address [vlan vlan-id] [count dynamic user]</pre>	スイッチまたは VLAN のすべてあるいは特定の IPv6 マルチキャスト アドレス情報を表示します。
	• count を入力して、スイッチまたは VLAN のグループ数を表示します。
	• dynamic を入力して、スイッチまたは VLAN の MLD スヌーピン グ学習済みグループ情報を表示します。
	• user を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。
show ipv6 mld snooping multicast-address vlan <i>vlan-id</i> [<i>ipv6-multicast-address</i>]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピ ングを表示します。

■ MLD スヌーピング情報の表示



CHAPTER **36**

EtherChannel およびリンクステート トラッ キングの設定

(注)

リンクステート トラッキングを使用するには、スイッチが LAN Base イメージを実行している必要が あります。

この章では、Catalyst 2960 スイッチに、EtherChannels を設定する方法について説明します。 EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供し ます。EtherChannel を使用すると、ワイヤリング クローゼットおよびデータ センタ間の帯域幅を拡張 できます。EtherChannel はネットワーク上でボトルネックの発生が見込まれるところに、任意に配置 できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的 に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他 のリンクにトラフィックをリダイレクトします。この章では、リンクステート トラッキングを設定す る方法についても説明します。

(注)

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

- 「EtherChannel の概要」(P.36-1)
- 「EtherChannel の設定」(P.36-9)
- 「EtherChannel、PAgP、および LACP ステータスの表示」(P.36-18)
- 「リンクステート トラッキングの概要」(P.36-18)
- 「リンクステート トラッキングの設定」(P.36-22)

EtherChannel の概要

- 「EtherChannel の概要」(P.36-2)
- 「ポートチャネル インターフェイス」(P.36-3)
- 「ポート集約プロトコル」(P.36-4)
- 「LACP」 (P.36-6)
- 「EtherChannel \mathcal{O} On \mathcal{E} ード」 (P.36-7)
- 「ロードバランシングおよび転送方式」(P.36-7)

EtherChannel の概要

EtherChannel は、単一の論理リンクにバンドルされた個々のファスト イーサネットまたはギガビット イーサネット リンクで構成されます(図 36-1 を参照)。

図 36-1 一般的な EtherChannel 構成



EtherChannel は、スイッチ間またはスイッチとホスト間に、最大 800Mbps(ファスト EtherChannel) または 8 Gbps(ギガビット EtherChannel)の全二重帯域幅を提供します。各 EtherChannel は、互換 性のある設定のイーサネット ポートを 8 つまで使用して構成できます。

各 EtherChannel 内のすべてのポートは、レイヤ 2 ポートとして設定する必要があります。 EtherChannel の数は 6 に制限されています。

詳細については、「EtherChannel 設定時の注意事項」(P.36-10)を参照してください。

EtherChannel は、Port Aggregation Protocol (PAgP; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、または On のいずれかのモードに設定できます。EtherChannel の両端は同 じモードで設定します。

- EtherChannel の一方の端を PAgP または LACP モードに設定すると、システムはもう一方の端と ネゴシエーションし、アクティブにするポートを決定します。互換性のないポートは独立ステート になり、他の単一リンクのようにデータトラフィックを伝送し続けます。ポート設定は変更され ませんが、ポートは EtherChannel に参加しません。
- EtherChannel を on モードに設定すると、ネゴシエーションは実行されません。スイッチは EtherChannel 内で互換性のあるすべてのポートを強制的にアクティブにします。EtherChannel の もう一方の端(他のスイッチ上)も、同じように on モードに設定する必要があります。それ以外 を設定した場合、パケットの損失が発生します。

EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィッ クが EtherChannel 内の残りのリンクに切り替えられます。スイッチでトラップがイネーブルになって いる場合、スイッチ、EtherChannel、および失敗したリンクを区別したトラップが送信されます。 EtherChannel の1つのリンク上の着信ブロードキャストおよびマルチキャスト パケットは、 EtherChannel の他のリンクに戻らないようにブロックされます。

ポートチャネル インターフェイス

レイヤ2 EtherChannel を作成すると、ポートチャネル論理インターフェイスが必要となります。 EtherChannel は次の方法で作成できます。

- channel-group インターフェイス コンフィギュレーション コマンドを使用します。チャネル グ ループに最初の物理ポートが追加されると、ポートチャネル論理インターフェイスが自動的に作成 されます。channel-group コマンドにより、物理ポート(10/100/1000 ポート)と論理ポートがバ インドされます(図 36-2 を参照)。
- interface port-channel port-channel-number グローバル コンフィギュレーション コマンドを使用 して、手動でポートチャネル論理インターフェイスを作成します。次に、channel-group channel-group-number インターフェイス コンフィギュレーション コマンドを使用して、物理ポー トに論理インターフェイスをバインドします。channel-group-number は port-channel-number と 同じ値に設定することも、違う値を使用することもできます。新しい値を使用すると、 channel-group コマンドによって新しいポートチャネルが動的に作成されます。

各 EtherChannel には1~6 番のポートチャネル論理インターフェイスがあります。ポートチャネルイ ンターフェイス番号は、channel-group インターフェイス コンフィギュレーション コマンドで指定さ れた番号に対応しています。



物理ポート、論理ポートチャネル、およびチャネル グループの関係

EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネ ルインターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用した設 定変更は、設定を適用したポートだけに作用します。EtherChannel のすべてのポートのパラメータを 変更するには、コンフィギュレーション コマンド (スパニング ツリー コマンド、またはレイヤ 2 EtherChannel をトランクとして設定するコマンドなど)をポートチャネル インターフェイスに適用し ます。

ポート集約プロトコル

Port Aggregation Protocol (PAgP) はシスコ独自のプロトコルで、シスコ製スイッチおよび PAgP をサ ポートするベンダーによってライセンス供与されたスイッチでのみ稼動します。PAgP を使用すると、 イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できま す。

スイッチは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各 ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク(チャネルまたは集 約ポート)に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、 ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同 じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成したあとで、PAgP は 単一スイッチ ポートとして、スパニング ツリーにそのグループを追加します。

PAgP モード

表 36-1 に、channel-group インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel PAgP モードを示します。

表 36-1 EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する
	PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはあり
	ません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パ
	ケットを送信することによって、相手ポートとのネゴシエーションを開始します。

スイッチ ポートは、auto モードまたは desirable モードに設定された相手ポートとだけ PAgP パケットを交換します。on モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーション により、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの 条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

PAgP モードが異なっていても、モード間で互換性があるかぎり、ポートは EtherChannel を形成できます。次に例を示します。

- desirable モードのポートは、desirable モードまたは auto モードの別のポートとともに EtherChannel を形成できます。
- auto モードのポートは、desirable モードの別のポートとともに EtherChannel を形成できます。

どのポートも PAgP ネゴシエーションを開始しないため、auto モードのポートは、auto モードの別の ポートとは EtherChannel を形成できません。 PAgP 対応のデバイスにスイッチを接続する場合、non-silent キーワードを使用すると、非サイレント 動作としてスイッチ ポートを設定できます。auto モードまたは desirable モードとともに non-silent を指定しなかった場合は、サイレント モードが指定されていると見なされます。

サイレント モードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにス イッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サー バ、またはパケット アナライザなどです。この場合、サイレント パートナーに接続された物理ポート 上で PAgP を稼動させると、このスイッチ ポートが動作しなくなります。ただし、サイレントを設定 すると、PAgP が動作してチャネル グループにポートを結合し、このポートが伝送に使用されます。

PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出

仮想スイッチは、Virtual Switch Link (VSL; 仮想スイッチ リンク) により接続された複数の Catalyst 6500 コア スイッチであり、それらのスイッチ間で制御情報とデータ トラフィックを伝送します。ス イッチのうちの1つはアクティブ モードです。その他のスイッチはスタンバイ モードです。冗長性を 確保するために、Catalyst 2960 スイッチのようなリモート スイッチは、Remote Satellite Link (RSL) により仮想スイッチに接続されます。

(注)

LAN Base イメージを実行している Catalyst 2960 スイッチだけが、リモート スイッチになれます。

2 つのスイッチ間の VSL に障害が発生すると、一方のスイッチは他方のスイッチのステータスを認識 しません。両方のスイッチがアクティブモードになり、ネットワークを、重複したコンフィギュレー ション (IP アドレスおよびブリッジ ID の重複を含む)を伴うデュアルアクティブの状態にする可能性 があります。ネットワークがダウンする場合もあります。

デュアルアクティブの状態を防止するために、コア スイッチは PAgP Protocol Data Uunit (PDU; プロ トコル データ ユニット)を RSL を介してリモート スイッチに送信します。PAgP PDU はアクティブ スイッチを識別し、リモート スイッチは、コア スイッチが同期化するように PDU をコア スイッチに 転送します。アクティブ スイッチに障害が発生した場合、またはアクティブ スイッチがリセットされ た場合は、スタンバイ スイッチがアクティブスイッチの役割を引き継ぎます。VSL がダウンした場合 は、1 つのコア スイッチが他のコア スイッチのステータスを認識して状態を変更しません。

PAgP と他の機能との相互作用

Dynamic Trunking Protocol (DTP) および Cisco Discovery Protocol (CDP) は、EtherChannel の物 理ポートを使用してパケットを送受信します。トランク ポートは、番号が最も小さい VLAN 上で PAgP Protocol Data Unit (PDU; プロトコルデータ ユニット)を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを 提供します。このポートがバンドルから削除されると、バンドル内の他のポートの1つが EtherChannel に MAC アドレスを提供します。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルに なっている、稼動状態のポート上だけです。

LACP

LACP は IEEE 802.3ad で定義されており、シスコ製スイッチが IEEE 802.3ad プロトコルに適合した スイッチ間のイーサネット チャネルを管理できるようにします。LACP を使用すると、イーサネット ポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および 各ポートの機能を学習します。次に、設定が類似しているポートを単一の倫理リンク(チャネルまたは 集約ポート)に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、 ハードウェア、管理、およびポート パラメータ制約です。たとえば、LACP は速度、デュプレックス モード、ネイティブ VLAN、VLAN 範囲、トランキング ステータス、およびトランキング タイプが同 じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成したあとで、LACP は 単一スイッチ ポートとして、スパニング ツリーにそのグループを追加します。

LACP モード

表 36-2 に、channel-group インターフェイス コンフィギュレーション コマンドでユーザが設定できる EtherChannel LACP モードを示します。

表 36-2 EtherChannel LACP モード

モード	説明
アクティ	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パ
ブ	ケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する
	LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはあ
	りません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび passive LACP モードでは、どちらの場合も、ポートは相手ポートとのネゴシエー ションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号 などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

LACP モードが異なっていても、モード間で互換性があるかぎり、ポートは EtherChannel を形成できます。次に例を示します。

- active モードのポートは、active モードまたは passive モードの別のポートとともに EtherChannel を形成できます。
- どのポートも LACP ネゴシエーションを開始しないため、passive モードのポートは、passive モードの別のポートとは EtherChannel を形成できません。

LACP と他の機能との相互作用

DTP および **CDP** は、EtherChannel の物理ポートを介してパケットを送受信します。トランク ポート は、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャネル内で最初に起動するポートが EtherChannel に MAC アドレスを 提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルに なっている稼動状態のポートとの間だけです。

EtherChannel \mathcal{O} On $\mathcal{T} - \mathcal{F}$

EtherChannel の on モードは、EtherChannel の手動設定に使用します。on モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの on モードが役立ちます。on モードでは、リンクの両端のス イッチが on モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの on モードで設定されたポートは、速度やデュプレックスのようなポート特性 に互換性を持たせる必要があります。on モードで設定されていたとしても、互換性のないポートは suspended ステートになります。

注意

on モードでの作業は慎重に行ってください。このモードは手動による設定が必要です。 EtherChannelの両端のポートには同じ内容を設定する必要があります。グループの設定を誤ると、 パケット損失またはスパニング ツリー ループが発生する可能性があります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル 内の1つのリンクを選択する数値に縮小することによって、チャネル内のリンク間でトラフィックの ロードバランシングを行います。EtherChannel のロードバランシングには、MAC アドレスまたは IP アドレス、送信元アドレスや宛先アドレスのどちらか一方、またはその両方のアドレスを使用できま す。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ロード バランシングおよび転送方式を設定するには、port-channel load-balance グローバル コンフィギュ レーション コマンドを使用します。

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、ロードバランシングを行う ために、送信元ホストが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、送信元ホ ストが同じパケットは同じチャネル ポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットに指定されて いる宛先ホストの MAC アドレスに基づいてチャネル ポート間で分配されます。したがって、宛先が 同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転 送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および 宛先の両方の MAC アドレスに基づいてチャネル ポート間で分配されます。この転送方式は、負荷分 散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のス イッチに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な 場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャネル ポートを使用できます。

送信元 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロードバランシングを行 うために、IP アドレスが異なるパケットはそれぞれ異なるチャネル ポートを使用しますが、IP アドレ スが同じパケットは同じチャネル ポートを使用します。

宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャネルポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャネルポートで送信されます。

送信元/宛先 IP アドレスベース転送の場合、パケットは EtherChannel に送信されて、着信パケットの 送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方 式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたものです。 特定のスイッチに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適切で あるかが不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス Bに、IP アドレ ス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それ ぞれ異なるチャネル ポートを使用できます。

ロードバランシング方式ごとに利点が異なります。ロードバランシング方式は、ネットワーク内のス イッチの位置、および負荷分散が必要なトラフィックの種類に基づいて選択する必要があります。 図 36-3 では、4 つのワークステーションからデータを集約しているスイッチからの EtherChannel が ルータと通信しています。ルータは単一 MAC アドレス デバイスであるため、スイッチ EtherChannel で送信元ベース転送をおこなうことにより、スイッチがルータの使用可能なすべての帯域幅を使用する ことが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数の ワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっている ためです。

設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単 一 MAC アドレスのみを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンク が常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロードバランシン グの効率がよくなる場合があります。



EtherChannel の設定

ここでは、次の設定情報について説明します。

- 「EtherChannel のデフォルト設定」(P.36-9)
- 「EtherChannel 設定時の注意事項」(P.36-10)
- 「レイヤ 2 EtherChannel の設定」(P.36-11)(必須)
- 「EtherChannel ロードバランシングの設定」(P.36-13)(任意)
- 「PAgP 学習方式およびプライオリティの設定」(P.36-14)(任意)
- 「LACP ホット スタンバイ ポートの設定」(P.36-16)(任意)



必ず、ポートを正しく設定してください。詳細については、「EtherChannel 設定時の注意事項」 (P.36-10) を参照してください。

(注)

EtherChannel の設定後、ポートチャネルインターフェイスに適用した設定変更は、そのポートチャネ ルインターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用 した設定変更は、設定を適用したポートだけに作用します。

EtherChannel のデフォルト設定

表 36-3 に、EtherChannel のデフォルト設定を示します。

表 36-3 EtherChannel のデフォルト設定

機能	デフォルト設定
チャネル グループ	割り当てなし
ポートチャネル論理インターフェイス	未定義
PAgP モード	デフォルトなし
PAgP 学習方式	すべてのポートで集約ポート ラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし
LACP 学習方式	すべてのポートで集約ポート ラーニング
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システム プライオリティとスイッチ MAC アドレ
	ス
ロードバランシング	着信パケットの送信元 MAC アドレスに基づいてスイッ チ上で負荷を分散

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワーク ループおよびその他の問題を回避 するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問 題を防ぐため、次の注意事項に従ってください。

- スイッチ上では、6を超える数の EtherChannel を設定しないでください。
- PAgP EtherChannel は、同じタイプのイーサネットポートを8つまで使用して設定します。
- LACP EtherChannel は、同じタイプのイーサネット ポートを最大 16 まで使用して設定します。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックス モードで動作するように 設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。shutdown インターフェイス コンフィ ギュレーション コマンドによってディセーブルにされた EtherChannel 内のポートは、リンク障害 として扱われます。そのポートのトラフィックは、EtherChannel 内の他のポートの1つに転送さ れます。
- グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値 をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ 内のすべてのポートでも変更する必要があります。
 - 許可 VLAN リスト
 - 各 VLAN のスパニング ツリー パス コスト
 - 各 VLAN のスパニング ツリー ポート プライオリティ
 - スパニング ツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバーになるように設定しないでください。
- 1 つの EtherChannel に PAgP モードと LACP モードの両方を設定しないでください。PAgP および LACP が稼動している複数の EtherChannel グループは、同じスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用はできません。
- EtherChannel の一部として Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 宛先 ポートを設定しないでください。
- EtherChannel の一部としてセキュア ポートを設定したり、セキュア ポートの一部として EtherChannel を設定したりしないでください。
- EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにする ポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになり ません。
- EtherChannel がスイッチ インターフェイス上に設定されている場合、dot1x system-auth-control グローバル コンフィギュレーション コマンドを使用して、IEEE 802.1x をスイッチ上でグローバ ルにイネーブルにする前に、EtherChannel の設定をインターフェイスから削除してください。
- レイヤ 2 EtherChannel の場合
 - EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。

- トランクポートから EtherChannel を設定する場合は、すべてのトランクでトランキングモード(ISL [スイッチ間リンク]または IEEE 802.1Q)が同じであることを確認してください。 EtherChannel ポートのトランクのモードが一致していないと、予想外の結果になる可能性があります。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が auto モード または desirable モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニング ツリー パス コストが異なるポートは、設定上の矛盾がないかぎり、EtherChannel を形成できます。異なるスパニング ツリー パス コストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

レイヤ 2 EtherChannel の設定

2 EtherChannel を設定するには、channel-group インターフェイス コンフィギュレーション コマンド を使用して、チャネル グループにポートを割り当てます。このコマンドにより、ポートチャネル論理 インターフェイスが自動的に作成されます。

レイヤ 2 EtherChannel にレイヤ 2 イーサネット ポートを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的	
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 2	interface interface-id	物理ポートを指定し、インターフェイス コンフィギュレーション モード を開始します。	
		指定できるインターフェイスとして、物理ポートも含まれます。	
		PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同 じグループに設定できます。	
		LACP EtherChannel の場合、同じタイプのイーサネット ポートを 16 ま で設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。	
ステップ 3	<pre>switchport mode {access trunk}</pre>	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り	
	switchport access vlan vlan-id	当てるか、またはトランクとして設定します。	
		ポートをスタティックアクセス ポートとして設定する場合は、ポートを1つの VLAN にのみ割り当ててください。指定できる範囲は1~4094です。	

	コマンド	目的
ステップ 4	channel-group channel-group-number mode {auto [non-silent] desirable [non-silent] on} {active passive}	チャネル グループにポートを割り当て、PAgP モードまたは LACP モー ドを指定します。
		<i>channel-group-number</i> の範囲は $1 \sim 6$ です。
		mode には、次のキーワードのいずれか1つを選択します。
		 auto: PAgP デバイスが検出された場合に限り、PAgP をイネーブル にします。ポートをパッシブ ネゴシエーション ステートにします。 この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。
		 desirable: PAgP を無条件でイネーブルにします。ポートをアクティ ブネゴシエーションステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーション を開始します。
		 on: PAgP または LACP を使用せずにポートが強制的にチャネル化されます。onモードの場合、EtherChannel が存在するのは、onモードのポート グループが同じく on モードの別のポート グループに接続される場合だけです。
		 non-silent:(任意) PAgP 対応のデバイスに接続されたスイッチの ポートが auto または desirable モードの場合に、非サイレント動作 を行うようにこのポートを設定します。non-silent を指定しなかった 場合は、サイレントが指定されたものと見なされます。サイレント設 定は、ファイル サーバまたはパケット アナライザとの接続に適して います。サイレントを設定すると、PAgP が動作してチャネル グルー プにポートを結合し、このポートが伝送に使用されます。
		 active:LACP デバイスが検出された場合に限り、LACP をイネーブ ルにします。ポートをアクティブ ネゴシエーション ステートにしま す。この場合、ポートは LACP パケットを送信することによって、 相手ポートとのネゴシエーションを開始します。
		 passive:ポート上でLACPをイネーブルにして、ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する LACPパケットに応答しますが、LACPパケットネゴシエーション を開始することはありません。
		スイッチおよびデバイスのモードの互換性に関する情報については、 「PAgP モード」(P.36-4)および「LACP モード」(P.36-6)を参照してく ださい。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

EtherChannel グループからポートを削除するには、no channel-group インターフェイス コンフィギュ レーション コマンドを使用します。

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティック アクセス ポートとして、PAgP モードが desirable であるチャネル 5 に割り当てます。

Switch# configure terminal Switch(config)# interface range gigabitethernet0/1 -2 Switch(config-if-range)# switchport mode access

```
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

次に、スイッチに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティック アクセス ポートとして、LACP モードが active であるチャネル 5 に割り当てられます。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

EtherChannel ロードバランシングの設定

ここでは、送信元ベースまたは宛先ベースの転送方式を使用することによって、EtherChannelのロードバランシングを設定する手順について説明します。詳細については、「ロードバランシングおよび転送方式」(P.36-7)を参照してください。

EtherChannel のロードバランシングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的 グローバル コンフィギュレーション モードを開始します。 ac EtherChannel のロードバランシング方式を設定します。 デフォルトは src-mac です。	
ステップ 1	configure terminal port-channel load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}		
ステップ 2			
		次のいずれかの負荷分散方式を選択します。	
		 dst-ip: 宛先ホスト IP アドレスに基づいて負荷を分散します。 	
		 dst-mac:着信パケットの宛先ホスト MAC アドレスに 基づいて負荷を分散します。 	
		 src-dst-ip:送信元および宛先ホスト IP アドレスに基づいて負荷を分散します。 	
		• src-dst-mac:送信元および宛先ホスト MAC アドレスに 基づいて負荷を分散します。	
		 src-ip:送信元ホスト IP アドレスに基づいて負荷を分散 します。 	
	end show etherchannel load-balance	 src-mac:着信パケットの送信元 MAC アドレスに基づいて負荷を分散します。 	
ステップ 3		特権 EXEC モードに戻ります。	
ステップ 4		設定を確認します。	
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

EtherChannel のロードバランシングをデフォルトの設定に戻す場合は、**no port-channel load-balance** グローバル コンフィギュレーション コマンドを使用します。

PAgP 学習方式およびプライオリティの設定

ネットワーク デバイスは、PAgP 物理ラーナーまたは集約ポート ラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約(論理)ポートによってアドレスを学習するデバイスは、集約ポート ラーナーです。学習方式はリンクの両端で同じ方式に設定する必要があります。

デバイスとそのパートナーが両方とも集約ポート ラーナーの場合、論理ポートチャネル上のアドレス を学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパ ケットを送信します。集約ポート ラーニングを使用している場合、どの物理ポートにパケットが届く かは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポート ラーナー の場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカル デバ イスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定し て、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要もあります。

グループ内の1つのポートですべての伝送を行うように設定して、他のポートをホットスタンバイに 使用することもできます。選択された1つのポートでハードウェア信号が検出されなくなった場合は、 数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に 常に選択されるように、ポートを設定するには、pagp port-priority インターフェイス コンフィギュ レーション コマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポー トが選択される可能性が高まります。

(注)

CLI (コマンドライン インターフェイス) で physical-port キーワードを指定した場合でも、スイッチ がサポートするのは、集約ポート上でのアドレス ラーニングのみです。pagp learn-method コマンド および pagp port-priority コマンドはスイッチ ハードウェアに影響を与えませんが、物理ポートによ るアドレス学習だけをサポートしているデバイスとの PAgP の相互運用性のために必要です。

スイッチのリンクの相手側が物理ラーナー(Catalyst 1900 シリーズ スイッチなど)の場合、pagp learn-method physical-port インターフェイス コンフィギュレーション コマンドを使用して、 Catalyst 2960 スイッチを物理ポート ラーナーとして設定することを推奨します。送信元 MAC アドレ スに基づいて負荷の分散方式を設定するには、port-channel load-balance src-mac グローバル コン フィギュレーション コマンドを使用します。このように設定すると、送信元アドレスの学習元である EtherChannel 内の同じポートを使用して、パケットが Catalyst 1900 スイッチに送信されます。pagp learn-method コマンドは、このような場合のみ使用してください。

スイッチを PAgP 物理ポート ラーナーとして設定し、バンドル内の同じポートがパケット送信用とし て選択されるようにプライオリティを調整するには、特権 EXEC モードで次の手順を実行します。こ の手順は任意です。

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

	コマンド	目的	
ステップ 3	pagp learn-method physical-port	PAgP 学習方式を選択します。	
		デフォルトでは、 aggregation-port learning が選択されてい ます。つまり、EtherChannel 内のポートのいずれかを使用し て、パケットが送信元に送信されます。集約ポート ラーニン グを使用している場合、どの物理ポートにパケットが届くか は重要ではありません。	
		ラーナーである別のスイッチに接続するには、physical-port を選択します。port-channel load-balance グローバル コン フィギュレーション コマンドは、必ず src-mac に設定してく ださい(「EtherChannel ロードバランシングの設定」 (P.36-13)を参照)。	
		学習方式はリンクの両端で同じ方式に設定する必要がありま す。	
ステップ 4	pagp port-priority priority	選択したポートがパケット伝送用として選択されるように、 プライオリティを割り当てます。	
		<i>priority</i> に指定できる範囲は 0 ~ 255 です。デフォルト値は 128 です。プライオリティが高いほど、ポートが PAgP 伝送 に使用される可能性が高くなります。	
ステップ 5	end	特権 EXEC モードに戻ります。	
ステップ 6	show running-config	設定を確認します。	
	または		
	show pagp channel-group-number internal		
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

プライオリティをデフォルト設定に戻すには、no pagp port-priority インターフェイス コンフィギュ レーション コマンドを使用します。学習方式をデフォルト設定に戻すには、no pagp learn-method イ ンターフェイス コンフィギュレーション コマンドを使用します。

LACP ホット スタンバイ ポートの設定

イネーブルの場合、LACP はチャネル内の LACP 互換ポート数を最大に設定しようとします(最大 16 ポート)。同時にアクティブになれる LACP リンクは 8 つだけです。リンクが追加されるとソフトウェ アによってホット スタンバイモードになります。アクティブ リンクの 1 つが非アクティブになると、 ホット スタンバイ モードのリンクが代わりにアクティブになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリ ティに基づいてアクティブにするホット スタンバイ ポートを決定します。ソフトウェアは、LACP を 操作するシステム間のすべてのリンクに、以下の要素(プライオリティ順)で構成された一意のプライ オリティを割り当てます。

- LACP システム プライオリティ
- システム ID (スイッチの MAC アドレス)
- LACP ポート プライオリティ
- ポート番号

プライオリティを比較する場合、数値的により低い方が高いプライオリティを持っています。プライオ リティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバ イモードにするポートを決定します。

アクティブ ポートかホット スタンバイ ポートかを判別するには、次の(2つの)手順を使用します。 はじめに、数値的に低いシステム プライオリティとシステム ID を持つシステムの方を選びます。次 に、ポート プライオリティおよびポート番号の値に基づいて、そのシステムのアクティブ ポートと ホット スタンバイ ポートを決定します。他のシステムのポート プライオリティとポート番号の値は使 用されません。

ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響を与えるように、LACP システム プライオリティおよび LACP ポート プライオリティのデフォルト値を変更できます。詳細については、「LACP システム プライオリティの設定」(P.36-16) および「LACP ポート プライオリティの設定」(P.36-17) を参照してください。

LACP システム プライオリティの設定

lacp system-priority グローバル コンフィギュレーション コマンドを使用して LACP をイネーブルに しているすべての EtherChannel に対してシステム プライオリティを設定できます。LACP を設定済み の各チャネルに対しては、システム プライオリティを設定できません。デフォルト値を変更すると、 ソフトウェアのアクティブおよびスタンバイ リンクの選択方法に影響します。

show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを 確認できます (ポートステート フラグが H になっています)。

LACP システム プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lacp system-priority priority	LACP システム プライオリティを設定します。
		<i>priority</i> に指定できる範囲は 1 ~ 65535 です。デフォルト値は 32768 です。
		値が小さいほど、システム プライオリティは高くなります。
ステップ 3	end	特権 EXEC モードに戻ります。

ステップ 4	show running-config	設定を確認します。
	または	
	show lacp sys-id	
ステップ 5	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま
		す。

LACP システム プライオリティをデフォルトの値に戻すには、no lacp system-priority グローバル コ ンフィギュレーション コマンドを使用します。

LACP ポート プライオリティの設定

デフォルトでは、すべてのポートは同じポート プライオリティです。ローカル システムのシステム プ ライオリティおよびシステム ID の値がリモート システムよりも小さい場合は、LACP EtherChannel ポートのポート プライオリティをデフォルトよりも小さい値に変更して、最初にアクティブになる ホットスタンバイ リンクを変更できます。ホット スタンバイ ポートは、番号が小さい方が先にチャネ ルでアクティブになります。show etherchannel summary 特権 EXEC コマンドを使用して、ホット スタンバイ モードのポートを確認できます (ポートステート フラグが *H* になっています)。

(注)

LACP がすべての互換ポートを集約できない場合(たとえば、ハードウェアの制約が大きいリモート システム)、EtherChannel 中でアクティブにならないポートはすべてホット スタンバイ ステートにな り、チャネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポート プライオリティを設定するには、特権 EXEC モードで次の手順を実行します。この手順 は任意です。

	コマンド	目的		
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。		
ステップ 2	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーショ ン モードを開始します。		
ステップ 3	lacp port-priority <i>priority</i>	LACP ポート プライオリティを設定します。		
		<i>priority</i> に指定できる範囲は 1 ~ 65535 です。デフォルト値は 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可 能性が高くなります。		
ステップ 4	end	特権 EXEC モードに戻ります。		
ステップ 5	show running-config	設定を確認します。		
	または			
	show lacp [channel-group-number] internal			
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。		

LACP ポート プライオリティをデフォルト値に戻すには、no lacp port-priority インターフェイス コ ンフィギュレーション コマンドを使用します。

EtherChannel、PAgP、および LACP ステータスの表示

表 36-4	EtherChannel.	PAaP.	および LACP ステータ	スを表示するためのコマント	1
					•

コマンド	説明
<pre>show etherchannel [channel-group-number {detail port port-channel protocol summary}] {detail load-balance port port-channel protocol summary}</pre>	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロードバランシング方式またはフレーム配布方式、ポート、ポートチャネル、プロトコルの情報も表示されます。
<pre>show pagp [channel-group-number] {counters internal neighbor}</pre>	トラフィック情報、内部 PAgP 設定、近接情報などの PAgP 情報 が表示されます。
show pagp [channel-group-number] dual-active	デュアルアクティブ検出ステータスを表示します。
<pre>show lacp [channel-group-number] {counters internal neighbor}</pre>	トラフィック情報、内部 LACP 設定、近接情報などの LACP 情報が表示されます。

PAgP チャネルグループ情報およびトラフィック カウンタをクリアするには、clear pagp {*channel-group-number* counters | counters} 特権 EXEC コマンドを使用します。

LACP チャネルグループ情報およびトラフィック カウンタをクリアするには、clear lacp {*channel-group-number* counters | counters} 特権 EXEC コマンドを使用します。

出力内の各フィールドについては、このリリースのコマンドリファレンスを参照してください。

リンクステート トラッキングの概要

(注)

リンクステート トラッキングを使用するには、スイッチが LAN Base イメージを実行している必要が あります。

リンクステート トラッキングは、トランク フェールオーバーとも呼ばれ、複数のインターフェイスの リンクステートをバインドする機能です。たとえば、リンクステート トラッキングをサーバ NIC アダ プタ チーミング機能とともに使用すると、ネットワークで冗長性が実現されます。サーバ ネットワー ク アダプタが、チーミングと呼ばれるプライマリまたはセカンダリ関係で設定され、プライマリ イン ターフェイスでリンクが消失した場合、接続はセカンダリ インターフェイスに透過的に変更されます。



インターフェイスは、ポートの集約 (EtherChannel)、またはアクセス モードかトランク モードの単一 物理ポートです。

図 36-4 (P.36-21)は、リンクステートトラッキングを使用して設定されたネットワークを示していま す。リンクステートトラッキングをイネーブルにするには、*リンクステート グループ*を作成して、リ ンクステート グループに割り当てられるインターフェイスを指定します。リンクステート グループで は、これらのインターフェイスは互いにバンドルされています。ダウンストリーム インターフェイス は、アップストリーム インターフェイスにバインドされています。サーバに接続されているインター フェイスは、ダウンストリーム インターフェイスと呼ばれ、分散スイッチやネットワーク デバイスに 接続されているインターフェイスはアップストリーム インターフェイスと呼ばれます。
図 36-4 の設定により、ネットワーク トラフィック フローのバランスが、次のように保たれます。

- スイッチと他のネットワーク デバイスへのリンクの場合
 - サーバ1とサーバ2は、プライマリリンクにスイッチAを使用し、セカンダリリンクにス イッチBを使用しています。
 - サーバ3とサーバ4は、プライマリリンクにスイッチBを使用し、セカンダリリンクにス イッチAを使用しています。
- スイッチ A のリンクステート グループ1
 - スイッチAはリンクステートグループ1を介して、プライマリリンクをサーバ1およびサーバ2に使用します。ポート1はサーバ1に、ポート2はサーバ2にそれぞれ接続されます。 ポート1およびポート2はリンクステートグループ1でダウンストリームインターフェイスとして使用します。
 - ポート5およびポート6は、リンクステートグループ1を介して分散スイッチ1に接続されます。ポート5およびポート6は、リンクステートグループ1でアップストリームインターフェイスとして使用します。
- スイッチ A のリンクステート グループ 2
 - スイッチAはリンクステートグループ2を介して、セカンダリリンクをサーバ3およびサーバ4に使用します。ポート3はサーバ3に、ポート4はサーバ4にそれぞれ接続されます。 ポート3およびポート4はリンクステートグループ2でダウンストリームインターフェイスとして使用します。
 - ポート7およびポート8は、リンクステートグループ2を介して分散スイッチ2に接続されます。ポート7およびポート8は、リンクステートグループ2でアップストリームインターフェイスとして使用します。
- スイッチBのリンクステートグループ2
 - スイッチBはリンクステートグループ2を介して、プライマリリンクをサーバ3およびサーバ4に使用します。ポート3はサーバ3に、ポート4はサーバ4にそれぞれ接続されます。 ポート3およびポート4はリンクステートグループ2でダウンストリームインターフェイスとして使用します。
 - ポート5およびポート6は、リンクステートグループ2を介して分散スイッチ2に接続されます。ポート5およびポート6は、リンクステートグループ2でアップストリームインターフェイスとして使用します。
- スイッチ B のリンクステート グループ 1
 - スイッチBはリンクステートグループ1を介して、セカンダリリンクをサーバ1およびサーバ2に使用します。ポート1はサーバ1に、ポート2はサーバ2にそれぞれ接続されます。 ポート1およびポート2はリンクステートグループ1でダウンストリームインターフェイスとして使用します。
 - ポート7およびポート8は、リンクステートグループ1を介して分散スイッチ1に接続されます。ポート7およびポート8は、リンクステートグループ1でアップストリームインターフェイスとして使用します。

分散スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リン クステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。これ らは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアッ プストリーム インターフェイス間の相互作用です。

 アップストリーム インターフェイスがリンクアップ ステートの場合、ダウンストリーム インター フェイスをリンクアップ ステートに変更したり、リンクアップ ステートのままにしたりすること ができます。 すべてのアップストリーム インターフェイスが利用不能になった場合、リンクステート トラッキ ングが自動的にダウンストリーム インターフェイスを errdisable ステートにします。サーバ間の接 続は、自動的にプライマリ サーバ インターフェイスからセカンダリ サーバ インターフェイスに変 更されます。

スイッチ A のリンクステート グループ 1 からリンクステート グループ 2 への接続の変更例につい ては、図 36-4 (P.36-21) を参照してください。ポート 6 のアップストリーム リンクが切断されて も、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップスト リーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンク ダウン ステートに変更されます。サーバ 1 およびサーバ 2 の接続については、リンクステート グ ループ 1 からリンクステート グループ 2 へ変更します。ダウンストリーム ポート 3 およびダウン ストリーム ポート 4 は、リンクグループ 2 であるためステートを変更しません。

 リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、 アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ス テートは変更されないままになります。サーバはこのアップストリーム接続が切断されたことを認 識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。複数のダウンストリーム インターフェイ スを復旧させるには、リンクステート グループをディセーブルにします。



リンクステート トラッキングの設定

- 「デフォルトのリンクステート トラッキングの設定」(P.36-22)
- 「リンクステート トラッキングの設定時の注意事項」(P.36-22)
- 「リンクステート トラッキングの設定」(P.36-22)
- 「リンクステート トラッキング ステータスの表示」(P.36-23)

デフォルトのリンクステート トラッキングの設定

リンクステート グループは定義されておらず、リンクステート トラッキングはどのグループでもイ ネーブルではありません。

リンクステート トラッキングの設定時の注意事項

設定上の問題を防ぐため、次の注意事項に従ってください。

- アップストリーム インターフェイスとして定義されているインターフェイスは、同じまたは異なるリンクステート グループ内でダウンストリーム インターフェイスとして定義できません。その逆も同様です。
- 1 つのインターフェイスが、複数のリンクステート グループのメンバーになることはできません。
- スイッチ1つにつき、設定できるリンクステートグループは2つだけです。

リンクステート トラッキングの設定

リンクステート グループを設定し、そのグループにインターフェイスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	link state track number	リンクステート グループを作成して、リンクステート トラッ キングをイネーブルにします。グループ番号は1~2に設定 できます。デフォルトは1です。
ステップ 3	interface interface-id	物理インターフェイスまたはインターフェイスの範囲を設定 して、インターフェイス コンフィギュレーション モードを開 始します。
		有効なインターフェイスには、アクセス モードまたはトラン ク モード (IEEE 802.1q) のスイッチ ポート、ルーテッド ポート、EtherChannel インターフェイス (スタティックまた は LACP) にバンドルされた、トランク モードの複数ポート が含まれます。
ステップ 4	link state group [<i>number</i>] {upstream downstream}	リンクステート グループを指定し、グループ内のインター フェイスを upstream または downstream インターフェイス に設定します。グループ番号は $1 \sim 2$ に設定できます。デ フォルトは 1 です。

	コマンド	目的
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config	設定を確認します。
ステップ 7	copy running-config startup-config	(任意)コンフィギュレーション ファイルに設定を保存しま
		す。

次に、リンクステートグループを作成してインターフェイスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range gigabitethernet0/21 -22
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# link state group 1 downstream
```

リンクステート グループをディセーブルにするには、no link state track number グローバル コンフィ ギュレーション コマンドを使用します。

リンクステート トラッキング ステータスの表示

show link state group コマンドを使用してリンクステート グループの情報を表示します。すべてのリ ンクステート グループの情報を表示するには、このコマンドをキーワードなしで入力します。特定の グループの情報を表示するには、グループ番号を入力します。グループの詳細情報を表示するには、 detail キーワードを入力します。

次に、show link stage group 1 コマンドの出力例を示します。

Switch> show link state group 1

Link State Group: 1 Status: Enabled, Down

次に、show link stage group detail コマンドの出力例を示します。

Switch> show link state group detail

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn) Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn) Gi1/0/17(Dwn) Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

■ リンクステート トラッキングの設定

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド



снартев 37

トラブルシューティング

この章では、Catalyst 2960 スイッチで使用する、Cisco IOS ソフトウェアに関連する、ソフトウェア の問題点を特定および解決する方法について説明します。問題の性質に応じて、CLI (コマンドライン インターフェイス)、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決 できます。

LED の説明など、トラブルシューティングの詳細については、『Hardware Installation Guide』を参照 してください。

(注)

このセクションで使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスおよび『*Cisco IOS Commands Master List, Release 12.2*』を参照してください。これらの マニュアルは、Cisco.com の Documentation > Cisco IOS Software > 12.2 Mainline > Command References を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- •「ソフトウェアで障害が発生した場合の回復」(P.37-2)
- 「パスワードを忘れた場合の回復」(P.37-4)
- •「コマンドスイッチで障害が発生した場合の回復」(P.37-8)
- 「クラスタメンバースイッチとの接続の回復」(P.37-12)

(注) 回復手順を実行するには、スイッチを直接操作しなければなりません。

- •「自動ネゴシエーションの不一致の防止」(P.37-13)
- 「PoE スイッチ ポートのトラブルシューティング」(P.37-13)
- •「SFP モジュールのセキュリティと識別」(P.37-14)
- 「SFP モジュール ステータスのモニタリング」(P.37-14)
- 「ping の使用」(P.37-15)
- 「レイヤ 2 traceroute の使用」(P.37-16)
- 「IP traceroute の使用」(P.37-18)
- 「TDR の使用」(P.37-20)
- 「debug コマンドの使用」(P.37-21)
- 「show platform forward コマンドの使用」(P.37-23)
- 「crashinfo ファイルの使用」(P.37-24)
- 「トラブルシューティング表」(P.37-25)

ソフトウェアで障害が発生した場合の回復

スイッチ ソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤った ファイルをダウンロードした場合、イメージファイルを削除した場合などが考えられます。いずれの 場合にも、スイッチは Power-On Self-Test (POST; 電源投入時セルフテスト)に失敗し、接続できな くなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージ ファイルまたは間違ったイメー ジファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多数あ り、使用するエミュレーション ソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作しなければなりません。

ステップ1 PC上で、Cisco.comからtar形式のソフトウェアイメージファイル(*image_filename.tar*)をダウン ロードします。

Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージ ファイルの検索方法については、リリース ノートを参照してください。

- ステップ2 tar ファイルから bin ファイルを抽出します。
 - Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
 - UNIX を使用している場合は、次の手順に従ってください。
 - **1.** tar -tvf <*image_filename.tar*> UNIX コマンドを使用して、tar ファイルの内容を表示します。 unix-1% tar -tvf *image filename.tar*
 - **2.** tar -xvf <*image_filename.tar*> <*image_filename.bin*>UNIX コマンドを使用して、bin ファイ ルを特定し、抽出します。

```
unix-1% tar -xvf image_filename.tar image_filename.bin
x c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin, 2928176 bytes, 5720
tape blocks
```

3. Is -I <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認 します。

```
unix-1% ls -1 image_filename.bin
-rw-r--r- 1 boba 2928176 Apr 21 12:01
c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin
```

- **ステップ 3** XMODEM プロトコルをサポートする端末エミュレーション ソフトウェアを備えた PC を、スイッチ のコンソール ポートに接続します。
- **ステップ4** エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。
- **ステップ5** スイッチの電源コードを取り外します。
- **ステップ6** Mode ボタンを押しながら、電源コードをサイドスイッチに接続します。

ポート1の LED が消灯してから1~2 秒後に、Mode ボタンを放します。ソフトウェアに関する数行 分の情報と指示が表示されます。

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software#

flash_init
load_helper
boot

- **ステップ7** フラッシュ ファイル システムを初期化します。 switch: **flash_init**
- **ステップ8** コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレー ション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。
- **ステップ9** ヘルパー ファイルがある場合にはロードします。 switch: load helper
- **ステップ 10** XMODEM プロトコルを使用して、ファイル転送を開始します。 switch: copy xmodem: flash:image_filename.bin
- **ステップ 11** XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに適切なコマンドを使用して、 転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。
- **ステップ 12** 新規にダウンロードされた Cisco IOS イメージを起動します。 switch:boot flash:image_filename.bin
- **ステップ 13** archive download-sw 特権 EXEC コマンドを使用して、スイッチにソフトウェア イメージをダウン ロードします。
- **ステップ 14** reload 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。
- ステップ 15 スイッチから、flash:image filename.bin ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンドユーザが、スイッチの電源投入時に 起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復 できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

(注)

これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンド ユーザによるパス ワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回 復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようとすると、回復 プロセスの間、ステータスメッセージにその旨が表示されます。

ここでは、スイッチのパスワードを忘れた場合の回復手順について説明します。

- 「パスワード回復がイネーブルになっている場合の手順」(P.37-5)
- 「パスワード回復がディセーブルになっている場合の手順」(P.37-7)

パスワードの回復をイネーブルまたはディセーブルにするには、service password-recovery グローバ ル コンフィギュレーション コマンドを使用します。

スイッチのパスワードを忘れた場合には、次の手順に従ってください。

- **ステップ1** 端末エミュレーション ソフトウェアが稼動している端末または PC をスイッチのコンソール ポートに 接続します。
- **ステップ 2** エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。
- **ステップ3** Power off the スイッチの電源を切ります。
- ステップ4 スイッチに電源コードを再接続してから 15 秒以内に Mode ボタンを押します。このときシステム
 LED はグリーンに点滅しています。システム LED が一瞬オレンジに点灯してからグリーンになるまで
 Mode ボタンを押したままにしてください。グリーンになったら Mode ボタンを離します。

ソフトウェアについての情報および指示が数行表示され、パスワード回復手順がディセーブルであるか どうかが示されます。

• 次の内容で始まるメッセージが表示された場合

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system

「パスワード回復がイネーブルになっている場合の手順」(P.37-5)に進んで、その手順に従います。

• 次の内容で始まるメッセージが表示された場合

The password-recovery mechanism has been triggered, but is currently disabled.

「パスワード回復がディセーブルになっている場合の手順」(P.37-7)に進んで、その手順に従います。

ステップ 5 パスワードが回復したら、スイッチをリロードします。

Switch> reload Proceed with reload?[confirm] y

パスワード回復がイネーブルになっている場合の手順

パスワード回復メカニズムがイネーブルになっている場合は、次のメッセージが表示されます。

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

flash_init load_helper boot

ステップ1 フラッシュファイルシステムを初期化します。

switch: flash_init

- **ステップ2** コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレー ション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。
- ステップ3 ヘルパーファイルがある場合にはロードします。

switch: load_helper

ステップ4 フラッシュメモリの内容を表示します。

switch: dir flash:

スイッチのファイルシステムが表示されます。

Directory of flash: 13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX 11 - rwy 5825 Mar 01 1993 22:31:59 config text

11 -rwx 5825 Mar 01 1993 22:31:59 config.text 18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat

16128000 bytes total (10003456 bytes free)

- **ステップ5** コンフィギュレーション ファイルの名前を config.text.old に変更します。 このファイルには、パスワード定義が収められています。 switch: rename flash:config.text flash:config.text.old
- **ステップ 6** システムを起動します。

switch: boot

セットアップ プログラムを起動するように求められます。プロンプトに N を入力します。 Continue with the configuration dialog?[yes/no]: N

- **ステップ7** スイッチ プロンプトで、特権 EXEC モードを開始します。 Switch> enable
- **ステップ8** コンフィギュレーションファイルを元の名前に戻します。 Switch# rename flash:config.text.old flash:config.text
- **ステップ9** コンフィギュレーションファイルをメモリにコピーします。 Switch# copy flash:config.text system:running-config

Source filename [config.text]? Destination filename [running-config]?

確認を求めるプロンプトに、Return キーを押して応答します。

これで、コンフィギュレーションファイルがリロードされ、パスワードを変更できます。

ステップ 10 グローバル コンフィギュレーション モードを開始します。

Switch# configure terminal

ステップ 11 パスワードを変更します。

Switch (config) # enable secret password

シークレットパスワードは1~25文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 特権 EXEC モードに戻ります。

Switch (config)# **exit** Switch#

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。 Switch# copy running-config startup-config

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

- (注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウンステートになる ことがあります。このステートになっているインターフェイスを調べるには、show running-config 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにす るには、interface vlan vlan-id グローバル コンフィギュレーション コマンドを入力して、 シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コ ンフィギュレーション モードの状態で、no shutdown コマンドを入力します。
- ステップ 14 スイッチをリロードします。

Switch# reload

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルになっている場合は、次のメッセージが表示されます。

The password-recovery mechanism has been triggered, but is currently disabled.Access to the boot loader prompt through the password-recovery mechanism is disallowed at this point.However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?

Æ 注意

スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わ せて、バックアップ スイッチと VLAN(仮想 LAN) コンフィギュレーション ファイルがあるかど うかを確認してください。

 n (no) を入力すると、Mode ボタンを押さなかった場合と同様に、通常のブート プロセスが継続 されます。ブート ローダ プロンプトにはアクセスできません。したがって、新しいパスワードを 入力できません。次のメッセージが表示されます。

Press Enter to continue.....

- y (yes) を入力すると、フラッシュメモリ内のコンフィギュレーションファイルおよび VLAN データベースファイルが削除されます。デフォルト設定がロードされるときに、パスワードをリ セットできます。
- **ステップ1** パスワード回復手順の継続を選択すると、既存の設定が失われます。 Would you like to reset the system back to the default configuration (y/n)?Y
- ステップ2 ヘルパーファイルがある場合にはロードします。

Switch: load_helper

ステップ3 フラッシュメモリの内容を表示します。

switch: **dir flash:** スイッチのファイル システムが表示されます。 Directory of flash: 13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX.0

16128000 bytes total (10003456 bytes free)

ステップ4 システムを起動します。 Switch: boot

> セットアップ プログラムを起動するように求められます。パスワード回復手順を継続するには、プロ ンプトに N を入力します。

Continue with the configuration dialog?[yes/no]: ${\bf N}$

- **ステップ5** スイッチ プロンプトで、特権 EXEC モードを開始します。 Switch> enable
- **ステップ6** グローバル コンフィギュレーション モードを開始します。 Switch# configure terminal

ステップ 7 パスワードを変更します。

Switch (config) # enable secret password

シークレットパスワードは1~25文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ8 特権 EXEC モードに戻ります。

Switch (config)# **exit** Switch#

ステップ9 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。 Switch# copy running-config startup-config

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。



上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになる ことがあります。このステートになっているインターフェイスを調べるには、show running-config 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにす るには、interface vlan vlan-id グローバル コンフィギュレーション コマンドを入力して、 シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コ ンフィギュレーション モードの状態で、no shutdown コマンドを入力します。

コマンド スイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)を使用すると、冗長コマンドスイッチ グループを設定できます。詳細については、第5章「スイッチのクラスタ化」および Cisco.com から 入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。



HSRP は、クラスタを冗長構成にする場合に適しています。

スタンバイ コマンド スイッチが未設定で、かつコマンド スイッチで電源故障などの障害が発生した場合には、メンバー スイッチとの管理接続が失われるので、新しいコマンド スイッチに交換する必要があります。ただし、接続されているスイッチ間の接続は影響を受けません。また、メンバー スイッチ も通常どおりにパケットを転送します。メンバー スイッチは、コンソール ポートを介してスタンドアロンのスイッチとして管理できます。また、IP アドレスが与えられている場合は、他の管理インターフェイスを使用して管理できます。

コマンド対応メンバースイッチまたは他のスイッチに IP アドレスを割り当て、コマンドスイッチのパ スワードを書き留め、メンバースイッチと交換用コマンドスイッチ間の冗長接続が得られるようにク ラスタを配置することにより、コマンドスイッチ障害に備えます。ここでは、故障したコマンドス イッチの交換方法を2通り紹介します。

- 「故障したコマンドスイッチをクラスタメンバーと交換する場合」(P.37-9)
- 「故障したコマンドスイッチを他のスイッチと交換する場合」(P.37-11)

ステップ 10 ここでスイッチを再設定する必要があります。システム管理者によって、バックアップ スイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

コマンド対応スイッチについては、リリース ノートを参照してください。

故障したコマンド スイッチをクラスタ メンバーと交換する場合

故障したコマンド スイッチを同じクラスタ内のコマンド対応メンバー スイッチに交換するには、次の 手順に従ってください。

- **ステップ1** コマンド スイッチとメンバー スイッチとの接続を切断し、クラスタからコマンド スイッチを物理的に 取り外します。
- **ステップ2** 故障したコマンドスイッチの代わりに新しいメンバースイッチを取り付け、コマンドスイッチとクラ スタメンバー間の接続を復元します。
- **ステップ3**新しいコマンドスイッチでCLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てら れている場合は、Telnet を使用してアクセスできます。コンソール ポートの詳しい使用方法について は、スイッチの『Hardware Installation Guide』を参照してください。

ステップ4 スイッチ プロンプトで、特権 EXEC モードを開始します。

Switch> **enable** Switch#

ステップ5 *故障したコマンドスイッチ*のパスワードを入力します。

ステップ6 グローバル コンフィギュレーション モードを開始します。 Switch# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z.

ステップ7 クラスタからメンバースイッチを削除します。

特権 Switch(config)# no cluster commander-address

- ステップ8 EXEC モードに戻ります。 Switch(config)# end Switch#
- ステップ9 セットアップ プログラムを使用して、スイッチの IP 情報を設定します。IP アドレス情報およびパス ワードを入力するように要求されます。特権 EXEC モードから setup と入力し、Return キーを押しま す。

Switch# **setup** --- System Configuration Dialog ---Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:

ステップ 10 最初のプロンプトに Y を入力します。

セットアップ プログラムのプロンプトは、コマンド スイッチとして選択したメンバー スイッチによっ て異なります。

```
Continue with configuration dialog? [yes/no]: \mathbf{y} 
 \texttt{tch}
```

Configuring global parameters:

このプロンプトが表示されなければ、enable と入力し、Return キーを押してください。セットアップ プログラムを開始するには、setup と入力し、Return キーを押してください。

ステップ 11 セットアップ プログラムの質問に応答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は28 文字、メンバースイッチ上では31文字に制限されていることに注意してください。どのスイッチで も、ホスト名の最終文字として-n(nは数字)を使用しないでください。

Telnet(仮想端末)パスワードを入力するように要求された場合、パスワードには1~25文字の英数 字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されるこ とに注意してください。

- **ステップ 12** enable secret および enable パスワードを入力するように要求された場合、*故障したコマンドスイッチ*のパスワードを再び入力してください。
- **ステップ 13** スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、Return キーを押します (要求された場合)。
- **ステップ 14** クラスタに名前を指定し、Return キーを押します(要求された場合)。 クラスタ名には1~31文字の英数字、ダッシュ、または下線を使用できます。
- ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。
- **ステップ 16** 表示された情報が正しい場合は、Y を入力し、Return キーを押します。 情報に誤りがある場合には、N を入力し、Return キーを押して、ステップ 9 からやり直します。
- **ステップ 17** ブラウザを起動し、新しいコマンド スイッチの IP アドレスを入力します。
- ステップ 18 クラスタ メニューから、Add to Cluster を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンド スイッチを他のスイッチと交換する場合

故障したコマンドスイッチを、クラスタに組み込まれていないコマンド対応スイッチと交換する場合、 次の手順に従ってください。

- **ステップ1** 故障したコマンド スイッチの代わりに新しいスイッチを取り付け、コマンド スイッチとクラスタ メン バー間の接続を復元します。
- **ステップ2**新しいコマンドスイッチでCLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てら れている場合は、Telnet を使用してアクセスできます。コンソール ポートの詳しい使用方法について は、スイッチの『Hardware Installation Guide』を参照してください。

- **ステップ3** スイッチ プロンプトで、特権 EXEC モードを開始します。 Switch> enable Switch#
- **ステップ** 4 *故障したコマンド スイッチ*のパスワードを入力します。
- **ステップ 5** セットアップ プログラムを使用して、スイッチの **IP** 情報を設定します。

IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから setup と入力し、Return キーを押します。

Switch# setup

--- System Configuration Dialog ---Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:

ステップ6 最初のプロンプトに **Y** を入力します。

セットアップ プログラムのプロンプトは、コマンドスイッチとして選択したスイッチによって異なり ます。

Continue with configuration dialog? [yes/no]: ${\bf y}$

または

Configuring global parameters:

このプロンプトが表示されなければ、enable と入力し、Return キーを押してください。セットアップ プログラムを開始するには、setup と入力し、Return キーを押してください。

ステップ7 セットアップ プログラムの質問に応答します。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は28 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として -n (n は数字)を使用しないでください。

Telnet(仮想端末)パスワードを入力するように要求された場合、パスワードには1~25文字の英数 字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されるこ とに注意してください。

- **ステップ8** enable secret および enable パスワードを入力するように要求された場合、*故障したコマンドスイッチ*のパスワードを再び入力してください。
- **ステップ9** スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、**Return** キーを押します (要求された場合)。
- **ステップ 10** クラスタに名前を指定し、**Return** キーを押します(要求された場合)。 クラスタ名には1~31 文字の英数字、ダッシュ、または下線を使用できます。
- **ステップ 11** 初期設定が表示されたら、アドレスが正しいことを確認してください。
- **ステップ 12** 表示された情報が正しい場合は、Y を入力し、Return キーを押します。 情報に誤りがある場合には、N を入力し、Return キーを押して、ステップ 9 からやり直します。
- **ステップ 13** ブラウザを起動し、新しいコマンド スイッチの IP アドレスを入力します。
- ステップ 14 クラスタ メニューから、Add to Cluster を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

クラスタ メンバー スイッチとの接続の回復

構成によっては、コマンドスイッチとメンバースイッチ間の接続を維持できない場合があります。メ ンバーに対する管理接続を維持できなくなった場合で、かつ、メンバースイッチが正常にパケットを 転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバー スイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 ス イッチ) は、ネットワーク ポートとして定義されたポートを介してコマンド スイッチに接続する ことはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバー スイッチは、 同じ管理 VLAN に所属するポートを介してコマンド スイッチに接続する必要があります。
- セキュアポートを介してコマンドスイッチに接続するメンバースイッチ(Catalyst 3750、 Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、 Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ)は、セキュリティ違反が原因 でポートがディセーブルになった場合、接続不能になることがあります。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度(10 Mbps、100 Mbps、および Small Form-Factor Pluggable [SFP] モジュール ポート以外の 1000 Mbps) およびデュプレックス(半二重ま たは全二重)に関するスイッチの設定を管理します。このプロトコルは設定を適切に調整しないことが あり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度 またはデュプレックスのパラメータと異なっている場合。
- ポートが自動ネゴシエーションモードに設定されており、接続ポートが自動ネゴシエーションを 指定せずに全二重に設定されている場合。

スイッチのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に 従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両端のポートに自動ネゴシエーションを実行させます。
- 接続の両端で、ポートの速度およびデュプレックスパラメータを手動設定します。

(注)

リモート デバイスが自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定が 一致するように設定します。速度パラメータは、接続ポートが自動ネゴシエーションを行わない場合で も、自動調整が可能です。

PoE スイッチ ポートのトラブルシューティング

ここでは、Power over Ethernet (PoE) ポートのトラブルシューティングについて説明します。

電力消失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電装置(Cisco IP Phone 7910 など)に AC 電源から電力が供給されない場合、そのデバイスは errdisable ステートになることがあり ます。errdisable ステートから回復するには、shutdown インターフェイス コンフィギュレーション コ マンドを入力してから、no shutdown インターフェイス コマンドを入力します。スイッチで自動回復 を設定し、errdisable ステートから回復することもできます。errdisable recovery cause loopback お よび errdisable recovery interval *seconds* グローバル コンフィギュレーション コマンドは、指定した 期間が経過したあと自動的にインターフェイスを errdisable ステートから復帰させます。

このリリースのコマンド リファレンスに記載されている次のコマンドを使用すると、PoE ポート ス テータスをモニタできます。

- show controllers power inline 特権 EXEC コマンド
- show power inline 特権 EXEC コマンド
- debug ilpower 特権 EXEC コマンド

不正リンク アップによるポート障害

シスコ受電装置をポートに接続詞、power inline never インターフェイス コンフィギュレーション コ マンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが errdisable ステート になることがあります。ポートを errdisable ステートから回復するには、shutdown および no shutdown インターフェイス コンフィギュレーション コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電装置を接続しないでください。

SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリ ティ コード、および Cyclic Redundancy Check (CRC; 巡回冗長検査) が格納されたシリアル EEPROM (電気的に消去可能でプログラミング可能な ROM)を備えています。スイッチに SFP モ ジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー 名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、 ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セ キュリティ エラー メッセージを生成し、インターフェイスを errdisable ステートにします。



セキュリティ エラー メッセージは、GBIC_SECURITY ファシリティを参照します。スイッチは、SFP モジュールをサポートしていますが、GBIC(ギガビット インターフェイス コンバータ)モジュール はサポートしていません。エラー メッセージ テキストは、GBIC インターフェイスおよびモジュール を参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェ イスを参照します。エラー メッセージの詳細については、このリリースに対応するシステム メッセー ジガイドを参照してください。

他社の SFP モジュールを使用している場合、スイッチから SFP モジュールを取り外し、シスコのモ ジュールに交換します。シスコの SFP モジュールを装着したら、errdisable recovery cause gbic-invalid グローバル コンフィギュレーション コマンドを使用してポート ステータスを確認し、 errdisable ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチは errdisable ステートからインターフェイスを復帰させ、操作を再試行します。errdisable recovery コマ ンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ 情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生 成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生す る場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ス テータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現 状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマン ドリファレンスに記載された「show interfaces transceiver」コマンドの説明を参照してください。

ping の使用

ここでは、次の情報について説明します。

- 「ping の概要」(P.37-15)
- 「ping の実行」 (P.37-15)

ping の概要

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。 ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返し ます。

- 正常な応答:正常な応答(hostname が存在する)は、ネットワークトラフィックにもよりますが、1~10秒以内で発生します。
- 宛先の応答なし:ホストが応答しない場合、no-answerメッセージが返ってきます。
- ホスト不明:ホストが存在しない場合、unknown host メッセージが返ってきます。
- 宛先に到達不能:デフォルトゲートウェイが指定されたネットワークに到達できない場合、 destination-unreachableメッセージが返ってきます。
- ネットワークまたはホストに到達不能:ルートテーブルにホストまたはネットワークに関するエントリがない場合、network or host unreachable メッセージが返ってきます。

ping の実行

スイッチからネットワーク上の別のデバイスに ping を実行するには、特権 EXEC モードで次のコマン ドを使用します。

コマンド	目的
ping ip host address	IP またはホスト名やネットワーク アドレスを指定してリモート
	ホストへ ping を実行します。

<u>》</u> (注)

ping コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされて いません。 次に、IP ホストに ping を実行する例を示します。

Switch# ping 172.20.52.3

Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms Switch#

表 37-1 で、ping の文字出力について説明します。

表 37-1 ping の出力表示文字

文字	説明
!	感嘆符1個につき1回の応答を受信したことを示します。
	ピリオド1個につき応答待ちの間にネットワーク サーバのタイムアウトが1回発 生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
Ι	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス(デフォルトでは Ctrl+^ X)を入力してくだ さい。Ctrl キー、Shift キー、および 6 キーを同時に押してから離し、そのあと X キーを押します。

レイヤ 2 traceroute の使用

ここでは、次の情報について説明します。

- 「レイヤ 2 traceroute の概要」(P.37-16)
- 「使用上のガイドライン」(P.37-17)
- 「物理パスの表示」(P.37-18)

レイヤ 2 traceroute の概要

レイヤ2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パス を識別できます。レイヤ2 traceroute はユニキャスト送信元および宛先 MAC (メディア アクセス制 御) アドレスのみをサポートします。パス内にあるスイッチの MAC アドレス テーブルを使用してパ スを識別します。スイッチがレイヤ2 traceroute をサポートしないデバイスをパスで検出すると、ス イッチはレイヤ2 トレース キューを送信し続けてタイムアウトにしてしまいます。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送 信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できませ ん。

使用上のガイドライン

レイヤ2 tracerouteの使用上の注意事項を次に示します。

 Cisco Discovery Protocol (CDP) がネットワーク上のすべてのデバイスでイネーブルでなければ なりません。レイヤ 2 traceroute が適切に動作するために、CDP をディセーブルにしないでください。

レイヤ 2 traceroute をサポートするスイッチの一覧については、「使用上のガイドライン」 (P.37-17) を参照してください。物理パス内のデバイスが CDP に対してトランスペアレントな場 合、スイッチはこれらのデバイスを通過するパスを識別できません。CDP をイネーブルにする場 合の詳細については第 25 章「CDP の設定」を参照してください。

- スイッチは、ping 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別可能なホップ数は10です。
- 送信元デバイスから宛先デバイスの物理パス内にないスイッチに、traceroute mac または traceroute mac ip 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このス イッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、traceroute mac コマンド 出力はレイヤ2パスのみを表示します。異なる VLAN にある送信元および宛先 MAC アドレスを 指定する場合、レイヤ2パスは識別されず、エラーメッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定する場合、パスは識別されず、エラーメッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属している場合、送信元および宛先 MAC ア ドレスの両方が属する VLAN を指定しなければなりません。VLAN が指定されない場合、パスは 識別されず、エラーメッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、traceroute mac ip コ マンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル)を使用して、IP アドレスを対応する MAC アドレスおよび VLAN ID に関連付けます。
 - ARP エントリが指定した IP アドレスにある場合、スイッチは関連する MAC アドレスを使用 して物理パスを識別します。
 - ARP エントリが存在しない場合、スイッチは ARP クエリーを送信して IP アドレスを解決し ようとします。IP アドレスが解決されない場合、パスは識別されず、エラー メッセージが表 示されます。
- 複数のデバイスがハブを介して1つのポートに接続されている場合(たとえば複数の CDP ネイバ がポートで検出された場合)、レイヤ2 traceroute 機能はサポートされません。複数の CDP ネイバ が1つのポート上で検出されると、レイヤ2パスは識別されず、エラーメッセージが表示されま す。
- この機能は、トークンリング VLAN 上ではサポートされません。

物理パスの表示

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを表示できます。

- tracetroute mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]
- tracetroute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]

詳細については、このリリースのコマンドリファレンスを参照してください。

IP traceroute の使用

ここでは、次の情報について説明します。

- 「IP traceroute の概要」(P.37-18)
- 「IP traceroute の実行」(P.37-19)

IP traceroute の概要

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク レイヤ (レイヤ 3) デバイスが表示されます。

スイッチは、traceroute 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッ チは traceroute コマンドの出力でホップとして表示される場合があります。スイッチを traceroute の 宛先とすると、スイッチは、traceroute の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、traceroute の出力に中間スイッチは表 示されません。ただし、中間スイッチが、特定のパケットをルーティングするマルチレイヤ スイッチ の場合、中間スイッチは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの Time To Live (TTL;存続可能時間) フィールドを 使用して、ルータおよびサーバで特定のリターン メッセージが生成されるようにします。traceroute の 実行は、UDP データグラムを、TTL フィールドが1に設定されている宛先ホストへ送信することから 始まります。ルータで TTL 値が1または0であることを検出すると、データグラムをドロップし、 Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) time-to-live-exceeded メッセージを送信元に送信します。traceroute は、ICMP time-to-live-exceeded

メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、traceroute は TTL 値が 2 の UDP パケットを送信します。1 番めの ルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めの ルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、time-to-live-exceeded メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで(または TTL の最大値に達するまで)TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 宛先ポー ト番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用され ない宛先ポート番号を持つ自分自身宛のデータグラムを受信すると、送信元に ICMP ポート到達不能 エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、 ポート到達不能エラーを受信するということは、このメッセージが宛先ポートから送信されたことを意 味します。

IP traceroute の実行

ネットワーク上でパケットが通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip host	ネットワーク上でパケットが通過するパスを追跡します。

```
<u>》</u>
(注)
```

traceroute 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースで はサポートされていません。

次に、IP ホストに traceroute を実行する例を示します。

Switch# traceroute ip 171.9.15.10

Type escape sequence to abort. Tracing the route to 171.69.115.10

1 172.2.52.1 0 msec 0 msec 4 msec 2 172.2.1.203 12 msec 8 msec 0 msec 3 171.9.16.6 4 msec 0 msec 0 msec 4 171.9.4.5 0 msec 4 msec 0 msec 5 171.9.121.34 0 msec 4 msec 4 msec 6 171.9.15.9 120 msec 132 msec 128 msec 7 171.9.15.10 132 msec 128 msec 128 msec Switch#

ディスプレイには、送信される3つのプローブごとに、ホップカウント、ルータのIPアドレス、およびラウンドトリップタイム(ミリ秒単位)が表示されます。

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブ ロックしていることを表しています。
Н	ホストが到達不能です。
N	ネットワークが到達不能です。
Р	プロトコルが到達不能です。
Q	ソース クエンチ。
U	ポートが到達不能です。

表 37-2 traceroute の出力表示文字

実行中の追跡を終了するには、エスケープ シーケンス(デフォルトでは **Ctrl+^ X**)を入力してください。**Ctrl キー、Shift キー、**および**6** キーを同時に押してから離し、そのあと **X** キーを押します。

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

TDR の使用

ここでは、次の情報について説明します。

- 「TDR の概要」(P.37-20)
- 「TDR の実行および結果の表示」(P.37-20)

TDR の概要

Time Domain Reflector (TDR)機能を使用してケーブル配線の問題を診断して解決できます。TDR 稼 動時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号 を比べます。

TDR は、10/100 および 10/100/1000 の銅線イーサネット ポート上のみでサポートされます。SFP モ ジュール ポート上ではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペアケーブルの導線のオープン、損傷、切断:導線がリモートデバイスからの導線に接続されていない状態。
- ツイストペアケーブルの導線のショート:導線が互いに接触している状態、またはリモートデバイスからの導線に接触している状態。たとえば、ツイストペアケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペアケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを 検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2つのデバイス間の接続のトラブルシューティング

TDR の実行および結果の表示

TDR を実行する場合、test cable-diagnostics tdr interface *interface-id* 特権 EXEC コマンドを実行します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンド を実行します。出力フィールドの説明に関しては、このリリースに対応するコマンド リファレンスを 参照してください。

debug コマンドの使用

ここでは、debug コマンドを使用してインターネットワーキングの問題を診断し、解決する方法について説明します。

- 「特定機能に関するデバッグのイネーブル化」(P.37-21)
- 「システム全体診断のイネーブル化」(P.37-22)
- 「デバッグおよびエラーメッセージ出力のリダイレクト」(P.37-22)



デバッグ出力には、CPU プロセスで高いプライオリティが与えられるので、システムが使用不能に なる可能性があります。したがって、debug コマンドを使用するのは、特定の問題のトラブル シューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを 行う場合に限定してください。debug コマンドは、ネットワーク トラフィックが少なく、ユーザも 少ないときに使用するのが最良です。このような時間にデバッグを実行すると、debug コマンドの 処理の負担によってシステム使用が影響を受ける可能性が少なくなります。



特定の debug コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレン スを参照してください。

特定機能に関するデバッグのイネーブル化

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの debug コマンドは引数を取りま せん。たとえば、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) に対するデバッグ をイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

Switch# debug span-session

スイッチは no 形式のコマンドが入力されるまで、出力を生成し続けます。

debug コマンドをイネーブルにしても、出力が表示されない場合は、次の状況が考えられます。

- モニタするトラフィックタイプを生成するようにスイッチが正しく設定されていない可能性があります。show running-config コマンドを使用して、設定を確認してください。
- スイッチが正しく設定されていても、デバッグがイネーブルである間にモニタすべきタイプのトラフィックを生成しないことがあります。デバッグする機能によっては、TCP/IPの ping コマンドなどを使用すると、ネットワークトラフィックを生成できます。

SPAN のデバッグをディセーブルにする場合は、特権 EXEC モードで次のコマンドを入力します。

Switch# no debug span-session

また、特権 EXEC モードで undebug 形式のコマンドを入力することもできます。

Switch# undebug span-session

各デバッグ オプションのステートを表示するには、特権 EXEC モードで次のコマンドを入力します。 Switch# show debugging

システム全体診断のイネーブル化

システム全体診断をイネーブルにするには、特権 EXEC モードで、次のコマンドを入力します。 Switch# **debug all**

/!\ 注意

デバッグ出力は他のネットワーク トラフィックより優先され、debug all 特権 EXEC コマンドは他の debug コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い debug コマンドを使用するのが原則です。

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いず れかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンド を使用すると便利です。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、debug コマンドおよびシステム エラー メッセージの出力をコン ソールに送信します。このデフォルトの設定を使用する場合は、コンソール ポートに接続する代わり に、仮想端末接続によってデバッグ出力をモニタできます。

出力先に指定できるのは、コンソール、仮想端末、内部バッファ、および Syslog サーバが稼動している UNIX ホストです。Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。



デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。コンソールでメッセージロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージロギングを行うと、オーバーヘッドが小さくなります。Syslog サーバでメッセージロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージ ロギングの詳細については、第 29 章「システム メッセージ ロギングの設定」を 参照してください。

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシス テムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関 して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、 ビットマップ、および出力側の情報が表示されます。

(注

show platform forward コマンドの構文および使用方法の詳細については、このリリースに対応する スイッチ コマンド リファレンスを参照してください。

このコマンドで出力される情報のほとんどは、主に、スイッチの Application Specific Integrated Circuit (ASIC; 特定用途向け集積回路) に関する詳細情報を使用するテクニカル サポート担当者に役 立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 のポート 1 に入るパケットが、不明な MAC アドレスにアドレス指定されている場合の show platform forward コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべての ポートに対してフラッディングされなければなりません。

Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2 udp 10 20

Global Port Number:24, Asic Number:5 Src Real Vlan Id:5, Mapped Vlan Id:5

 Ingress:
 Index-Hit
 A-Data

 lnptACL
 40_0D020202_0D010101-00_40000014_000A0000
 01FFA
 03000000

 L2Local
 80_00050002_00020002-00_00000000_0000000
 00C71
 0000002B

 Station
 Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

Egress:Asic 2, switch 1

Output Packets:

Packet 1 Lookup Key-Used Index-Hit A-Data OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 03000000 Port Vlan SrcMac DstMac Cos Dscpv

Gi0/1 0005 0001.0001.0001 0002.0002.0002

Packet dropped due to failed DEJA VU Check on Gi0/2

-----Packet 2
Lookup Key-Used Index-Hit A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 03000000

 Port
 Vlan
 SrcMac
 DstMac
 Cos
 Dscpv

 Gi0/2
 0005
 0001.0001
 0002.0002.0002

<output truncated>

Packet 10
Lookup Key-Used Index-Hit A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2

次に、VLAN 5 のポート1に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送 信する場合の出力例を示します。パケットは、アドレスを学習したポートから転送する必要がありま す。 Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1 13.2.2.2 udp 10 20 Global Port Number:24, Asic Number:5 Src Real Vlan Id:5, Mapped Vlan Id:5 Ingress: Lookup Key-Used Index-Hit A-Data InptACL 40_0D020202_0D010101-00_40000014_000A0000 01FFA 03000000 L2Local 80_00050009_43A80145-00_00000000_00000000 00086 02010197 Station Descriptor: F0050003, DestIndex: F005, RewriteIndex: 0003 _____ Egress:Asic 3, switch 1 Output Packets: _____ Packet 1 Lookup Key-Used Index-Hit A-Data OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FFE 0300000 Port Vlan SrcMac DstMac Cos Dscpv interface-id 0005 0001.0001.0001 0009.43A8.0145

crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害(クラッシュ)が原因で起きた問題をデバッグするときに使用する情報が保存されます。スイッチは障害発生時にその情報をコンソールに書き込みます。スイッチは次の2つのタイプの crashinfo ファイルを作成します。

- 基本 crashinfo ファイル:障害発生後に Cisco IOS イメージを起動すると、スイッチが自動的にこのファイルを作成します。
- 拡張 crashinfo ファイル:システム障害の発生時に、スイッチがこのファイルを自動的に作成します。

基本 crashinfo ファイル

この基本ファイルに保存される情報は、障害が発生した Cisco IOS イメージの名前、バージョン、プロ セッサ レジスタのリスト、および他のスイッチ特有の情報です。show tech-support 特権 EXEC コマ ンドを使用することによって、この情報をシスコのテクニカル サポート担当者に提供できます。

基本 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。 flash:/crashinfo/

ファイル名は crashinfo n になります。n には一連の番号が入ります。

新しい crashinfo ファイルが作成されるたびに、前のシーケンス番号より大きいシーケンス番号が使用 されるので、シーケンス番号が最大のファイルに、最新の障害が記述されています。タイムスタンプで はなく、バージョン番号を使用するのは、スイッチにリアルタイム クロックが組み込まれていないか らです。ファイル作成時にシステムが使用するファイル名を変更することはできません。ただし、ファ イルが作成されたあとに、rename 特権 EXEC コマンドを使用して名前を変更することもできますが、 show tech-support 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示され ません。delete 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo ファイル (つまり、ファイル名の末尾のシーケンス番号が最大であるファイル)を表示する場合は、show tech-support 特権 EXEC コマンドを使用します。more 特権 EXEC コマンド、 copy 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、 ファイルにアクセスすることもできます。

拡張 crashinfo ファイル

スイッチは、システム障害の発生時に拡張 crashinfo ファイルを作成します。拡張ファイルに保存され る情報は、スイッチの障害となった原因を特定するのに役立つ追加情報です。このファイルに手動でア クセスし、more または copy 特権 EXEC コマンドを使用すると、シスコのテクニカル サポート担当者 にこの情報を提供できます。

拡張 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。 flash:/crashinfo ext/

ファイル名は crashinfo_ext_n になります。n には一連の番号が入ります。

no exception crashinfo グローバル コンフィギュレーション コマンドを使用すると、スイッチが拡張 crashinfo ファイルを作成しないように設定できます。

トラブルシューティング表

次の表は、Cisco.com のトラブルシューティング マニュアルから抽出した内容をまとめたものです。

- 「CPU 使用率に関するトラブルシューティング」(P.-25)
- 「Power over Ethernet (PoE) のトラブルシューティング」(P.-27)

CPU 使用率に関するトラブルシューティング

ここでは、CPU 利用の過重が原因で起こりうる問題の症状を一覧し、CPU 使用率の問題の検証方法に ついて説明します。表 37-3 は、CPU 使用率に関する特定可能な主な問題を一覧しています。この表に は、考えられる原因と修正措置が示してあり、それぞれに Cisco.com の『*Troubleshooting High CPU Utilization*』ドキュメントへのリンクが張られています。

CPU 使用率が高い場合に起こりうる症状

過重な CPU 使用率が原因で次の症状が発生する可能性がありますが、他の原因で発生する場合もあり ます。

- スパニング ツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求(ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション)に応答で きない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理 の失敗

レイヤ3スイッチの場合:

- ソフトウェアでルーティングされるパケットの廃棄または遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

問題と原因の検証

CPU 使用率が高いことが問題となっているかどうか判別するには、show processes cpu sorted 特権 EXEC コマンドを入力します。出力例の1行目にある下線が付いた部分に注目してください。

```
Switch# show processes cpu sorted

<u>CPU utilization for five seconds: 8%/0%;</u> one minute: 7%; five minutes: 8%

PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers

140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request

100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters

192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree

143 8 37 216 0.15% 0.01% 0.00% 0 Exec

...
```

<output truncated>

この例は、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8 パーセント
- 割り込みの処理にかかった時間は全体の0パーセント

表 37-3 CPU 使用率に関する問題のトラブルシューティング

問題のタイプ	原因	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケッ ト数が多すぎる	ネットワーク パケットのソースを判別 する。データの流れを遮断するか、ス イッチの設定を変更します。「Analyzing Network Traffic」を参照してください。
割り込みの所要時間は最小限であっ たにもかかわらず CPU の合計使用率 が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処 理が1つ以上存在する。これは通常、処 理をアクティブ化するイベントによって 始動されます。	異常なイベントを特定して根本的な原因 を解消する。「Debugging Active Processes」を参照してください。

CPU使用率の詳細および使用率の問題を解決する方法については、**Cisco.com**の『*Troubleshooting High CPU Utilization*』ドキュメントを参照してください。

Power over Ethernet (PoE) のトラブルシューティング

症状または問題	考えられる原因と解決法	
あるポートでだけ PoE が機能しない	この受電装置が他の PoE ポートで動作するかを確認する	
1 つのスイッチ ポートに限り問題が発生 する。このポートでは PoE 装置と PoE 非 対応の装置のいずれも動作しないが、他	ポートがシャットダウンまたは error disabled になっていないかを確認するため に、ユーザ特権 EXEC コマンドの show run、show interface status、または show power inline detail を使用します。	
のポートでは動作します。	(注) ほとんどのスイッチはポートがシャットダウンしているときはポートの 電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指 定されている場合も同様です。	
	受電装置からスイッチ ポートまでのイーサネット ケーブルの動作が正常である ことを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置 とイーサネット ケーブルを接続して、受電装置がリンクを確立し他のホストと トラフィックを交換することを確認します。	
	スイッチのフロント パネルから受電装置までのケーブル長の合計が 100 メート ル以下であることを確認します。	
	スイッチ ポートからイーサネット ケーブルを切断します。短いイーサネット ケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロント パネルの (パッチ パネルではない) このポートに直接接続します。これによっ てイーサネット リンクが確立され他のホストとトラフィックを交換できること を確認します。あるいは、ポートの VLAN SVI で ping を実行してください。 次に、受電装置をこのポートに接続し、電源がオンになることを確認します。	
	パッチコードをスイッチポートに接続しても受電装置の電源がオンにならない場合、接続する受電装置の合計数とスイッチのパワーバジェット(使用可能な PoE)とを比較してください。show inline power コマンドおよび show inline power detail コマンドを使用して使用可能な電力量を確認します。	
	詳細については、Cisco.com の『No PoE On One Port』を参照してください。	

図 37-1 Power Over Ethernet のトラブルシューティング シナリオ

図 37-1 Power Over Ethernet のトラブルシューティング シナリオ (続き)

 症状または問題	考えられる原因と解決法
すべてのポートまたは1つのポートグ ループで PoE が機能しない すべてのスイッチ ポートで問題が発生す	連続して断続的に繰り返し発生する、電力に関するアラームがある場合、現場 交換が可能であれば電源装置を交換します。そうでない場合はスイッチを交換 してください。
る。電力が供給されていないイーサネット装置がどのポートでもイーサネットリンクを確立できず、PoE 装置の電源がオ	連続する複数のポートで問題があるものの、すべてのポートで問題が発生する わけではない場合、電源の故障ではないと考えられ、スイッチの PoE レギュ レータに関連した異常の可能性があります。
ンになりません。	PoE の状況やステータスの変更について過去に報告されているアラームまたは システム メッセージがないか、show log 特権 EXEC コマンドを使用して調べま す。
	アラームがない場合は、show interface status コマンドを使用して、ポートが シャットダウンしていないか errdisable になっていないかを確認します。ポー トが errdisable の場合、shut および no shut インターフェイス コンフィギュ レーション コマンドを使用してポートを再びイネーブルにします。
	特権 EXEC コマンドの show env power および show power inline を使用して、 PoE のステータスおよびパワー バジェット(使用可能な PoE)を調べます。
	実行コンフィギュレーションを調べて power inline never がこのポートに設定 されていないことを確認します。
	受電していないイーサネット装置をスイッチ ポートに直接接続します。接続に は短いパッチ コードだけを使用します。既存の配線ケーブルは使用しないでく ださい。shut および no shut インターフェイス コンフィギュレーション コマン ドを入力し、イーサネット リンクが確立されていることを確認します。正しく 接続している場合、短いパッチ コードを使用して受電装置をこのポートに接続 し、電源がオンになることを確認します。装置の電源がオンになったら、すべ ての中間パッチ パネルが正しく接続されているか確認してください。
	1 本を除くすべてのイーサネット ケーブルをスイッチ ポートから抜きます。短 いパッチ コードを使用して、1 つの PoE ポートにだけ受電装置を接続します。 スイッチ ポートからの受電に比較して、受電装置が多くの電力を必要としない ことを確認してください。
	show power inline 特権 EXEC コマンドを使用して、ポートがシャットダウン していない場合に、受電装置に電力が供給されることを確認します。あるいは、 受電装置を観察して電源がオンになることを確認してください。
	1 台の受電装置だけがスイッチに接続しているときに電力が供給される場合、 残りのポートで shut および no shut インターフェイス コンフィギュレーション コマンドを入力してから、イーサネット ケーブルをスイッチの PoE ポートに 1 本ずつ再び接続してください。show interface status および show power inline 特権 EXEC コマンドを使用して、インライン電力統計およびポート ステータス をモニタします。
	すべてのポートで、まだ PoE が機能しない場合は、電源装置の PoE セクション でヒューズを開くことができる場合があります。この場合、アラームが生成さ れるのが一般的です。過去にシステム メッセージでアラームが報告されていな いか、ログをもう一度チェックしてください。
	詳細については、Cisco.com の『No PoE On Any Port or a Group of Ports』を参照してください。

図 37-1 Power Over Ethernet のトラブルシューティング シナリオ (続き)

症状または問題	考えられる原因と解決法
Cisco IP Phone が切断またはリセットされる 正常に動作したあとで、Cisco phone また	スイッチから受電装置までのすべての電気系統を確認してください。信頼性の 低い接続は、電力供給の中断や受電装置の機能が不安定になる原因となり、受 電装置の断続的な切断やリロードなどが発生します。
はワイヤレス アクセス ポイントが断続的 にリロードしたり、PoE から切断された	スイッチ ポートから受電装置までのケーブル長が 100 メートル以下であること を確認してください。
りします。	スイッチが配置されている場所で電気環境にどのような変化があるか、切断時 に、受電装置に何が起きるかについて注意してください。
	切断と同時にエラー メッセージが表示されたか注意します。show log 特権 EXEC コマンドを使用してエラー メッセージを確認します。
	リロードの発生直前に IP Phone から Call Manager へのアクセスが失われてい ないか確認してください (PoE の障害ではなくネットワークに問題が発生して いる場合があります)。
	受電装置を PoE 非対応の装置に交換し、装置が正しく動作することを確認しま す。PoE 非対応の装置にリンク障害または高いエラー率がある場合、スイッチ ポートと受電装置を接続する信頼性の低いケーブル接続が問題の可能性があり ます。
	詳細については、Cisco.com の『Cisco Phone Disconnects or Resets』を参照し てください。
シスコ以外の受電装置がシスコ PoE ス イッチで動作しない シスコ PoE スイッチに接続するシスコ以 外の受電装置に電源が供給されないか、	show power inline コマンドを使用して、受電装置の接続前後に、スイッチのパ ワー バジェット(使用可能な PoE)が使い果たされていないか確認してくださ い。受電装置を接続する前に、このタイプの装置に十分な電力が使用可能であ ることを確認します。
電源投入後すぐに電源が切れます。PoE 非対応装置は正常に動作します。	show interface status コマンドを使用して、接続されている受電装置をスイッ チが検出することを確認します。
	show log コマンドを使用して、ポートの過電流状態を報告したシステム メッ セージがないか確認します。症状を正確に特定してください。最初に電力が受 電装置に供給され、その後、切断される状態ですか。その場合は、問題は最初 のサージ電流(<i>突入</i> 電流)が原因で、ポートの電流上限しきい値が超過した可 能性があります。
	詳細については、Cisco.com の『Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch』を参照してください。

トラブルシューティング表




サポート対象 MIB

この付録では、このリリースでサポートされている Catalyst 2960 スイッチの Management Information Base (MIB; 管理情報ベース)を示します。内容は次のとおりです。

- 「MIB の一覧」 (P.A-1)
- 「FTP による MIB ファイルへのアクセス」(P.A-3)

• BRIDGE-MIB



- (注) BRIDGE-MIB は単一 VLAN (仮想 LAN)のコンテキストをサポートします。デフォルトで、設定済みのコミュニティストリングを使用している SNMP (簡易ネットワーク管理プロトコル)メッセージは、常に VLAN 1 の情報を提供します。他の VLAN (VLAN x など)の BRIDGE-MIB 情報を取得するには、SNMP メッセージ内でコミュニティストリング configured community string @x を使用します。
- CISCO-ADMISSION-POLICY-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- CISCO-CABLE-DIAG-MIB
- CISCO-CDP-MIB
- CISCO-CLUSTER-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-ERR-DISABLE-MIB
- CISCO-FLASH-MIB (すべてのスイッチのフラッシュ メモリは着脱式フラッシュ メモリとしてモ デル化されています)
- CISCO-FTP-CLIENT-MIB
- CISCO-IETF-IP-MIB
- CISCO-IETF-IP-FORWARDING-MIB

- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO IP-STAT-MIB
- CISCO-LAG-MIB
- CISCO-MAC-AUTH-BYPASS
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB (パケットカウンタだけがサポートされ、オクテットカウンタはサポートされません)
- CISCO-POWER-ETHERNET-EXT-MIB
- CISCO-PRODUCTS-MIB
- CISCO-PROCESS-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TC-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-CONFIG-COPY-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8021-PAE-MIB
- IEEE8023-LAG-MIB
- IF-MIB (VLAN の入出力カウンタはサポートされていません)
- IGMP-MIB
- INET-ADDRESS-MIB
- LLDP MED MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB

- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB (機能は CISCO-RFC1213-CAPABILITY.my で指定されているエージェント機能 により異なります)
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

(注)

また、次の URL を使用して Catalyst 2960 スイッチでサポートされる MIB の一覧を表示することもできます。

ftp://ftp.cisco.com/pub/mibs/supportlists/cat2960/cat2960-supportlist.html

MIB およびシスコ製品に関する他の情報は、次の Cisco Web サイトからアクセスできます。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

FTP による MIB ファイルへのアクセス

各 MIB ファイルを入手する手順は、次のとおりです。

ステップ1 ご使用の FTP クライアントがパッシブ モードであることを確認してください。



- _______ パッシブ モードをサポートしていない FTP クライアントもあります。

- ステップ 2 FTP を使用してサーバ ftp.cisco.com にアクセスします。
- ステップ 3 ユーザ名 anonymous を使用してログインします。
- ステップ4 パスワードが要求されたら、Eメールのユーザ名を入力します。
- ステップ 5 ftp> プロンプトで、ディレクトリを /pub/mibs/v1 および /pub/mibs/v2 に変更します。
- ステップ 6 get MIB_filename コマンドを使用して、MIB ファイルのコピーを入手します。





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

この付録では、Catalyst 2960 スイッチ フラッシュ ファイル システムの操作方法、コンフィギュレー ション ファイルのコピー方法、スイッチにソフトウェア イメージをアーカイブ(アップロードおよび ダウンロード)する方法について説明します。

(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチ コマンド リファレンスおよび『*Cisco IOS Interface Command Reference, Release 12.2*』を参照してく ださい。これには、Cisco.com のホームページ(**Documentation** > **Cisco IOS Software** > **12.2 Mainline** > **Command References**)からアクセス可能です。

この付録で説明する内容は、次のとおりです。

- 「フラッシュファイルシステムの操作」(P.B-2)
- 「コンフィギュレーションファイルの操作」(P.B-10)
- 「ソフトウェアイメージの操作」(P.B-28)

フラッシュ ファイル システムの操作

フラッシュ ファイル システムは、ファイルを格納できる単一のフラッシュ デバイスです。ソフトウェ ア イメージおよびコンフィギュレーション ファイルの管理に役立つ複数のコマンドも備えています。 スイッチのデフォルトのフラッシュ ファイル システムは *flash*: です。

ここでは、次の設定情報について説明します。

- 「使用可能なファイル システムの表示」(P.B-2)
- 「ファイル システムのファイルに関する情報の表示」(P.B-4)
- 「ディレクトリの作成および削除」(P.B-5)
- 「ファイルのコピー」(P.B-6)
- 「ファイルの削除」(P.B-7)
- 「tar ファイルの作成、表示、および抽出」(P.B-7)
- 「ファイルの内容の表示」(P.B-10)

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、show file systems 特権 EXEC コマンドを使用します(次の例を参照)。

Switch# **show file systems** File Systems:

· ·	10 01000000				
	Size(b)	Free(b)	Туре	Flags	Prefixes
ł	15998976	5135872	flash	rw	flash:flash3:
	-	-	opaque	rw	bs:
	-	-	opaque	rw	vb:
	524288	520138	nvram	rw	nvram:
	-	-	network	rw	tftp:
	-	-	opaque	rw	null:
	-	-	opaque	rw	system:
	-	-	opaque	ro	xmodem:
	-	-	opaque	ro	ymodem:

表 B-1

show file systems フィールドの説明

フィールド	值	
Size (b)	ファイル システムのメモリ サイズ(バイト単位)です。	
Free (b)	ファイル システムの空きメモリ サイズ(バイト単位)です。	
Туре	/pe ファイルシステムのタイプです。	
flash:ファイル システムはフラッシュ メモリ デバイス用です。		
	nvram : ファイル システムは NVRAM(不揮発性 RAM)デバイス用です。	
	opaque : ファイル システムはローカルに生成された <i>pseudo</i> ファイル システム(<i>system</i> など)、または brimux などのダウンロード インターフェイスです。	
	unknown : ファイル システムのタイプは不明です。	

フラッシュ ファイル システムの操作 🔳

フィールド	值	
Flags	ファイル システムの権限です。	
	ro:読み取り専用です。	
	rw:読み取り/書き込みです。	
	wo:書き込み専用です。	
Prefixes	ファイル システムのエイリアスです。	
flash: : フラッシュ ファイル システムです。		
nvram: : NVRAM です。		
	null: : コピーのヌル宛先です。リモート ファイルをヌルヘコピーして、サイズを判別できます。	
	rcp: : Remote Copy Protocol (RCP) ネットワーク サーバです。	
	system: : 実行コンフィギュレーションを含むシステム メモリが格納されています。	
	tftp: : TFTP ネットワーク サーバです。	
	xmodem: : XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。	
	ymodem: : YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。	

表 B-1 show file systems フィールドの説明 (続き)

デフォルト ファイル システムの設定

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するに は、cd filesystem: 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関 連するコマンドを実行するときに filesystem: 引数を省略できます。たとえば、オプションの filesystem: 引数を持つすべての特権 EXEC コマンドでは、cd コマンドで指定されたファイル システム が使用されます。

デフォルトでは、デフォルト ファイル システムは flash: です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマ ンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィ ギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコン フィギュレーション ファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィ ギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマ ンドで使用できます。

ファイル システムのファイルに関する情報を表示するには、表 B-2 に記載された特権 EXEC コマンド のいずれかを使用します。

表 B-2 ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [filesystem:][filename]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information <i>file-url</i>	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファ イルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開か れているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	dir filesystem:	指定されたファイル システムのディレクトリを表示します。
		<i>filesystem</i> : には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。
ステップ 2	cd new_configs	目的のディレクトリに変更します。
		コマンド例では、new_configs という名前のディレクトリに変更する方法を 示します。
ステップ 3	pwd	作業ディレクトリを表示します。

ディレクトリの作成および削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的	
ステップ 1	dir filesystem:	指定されたファイル システムのディレクトリを表示します。	
		<i>filesystem</i> : には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。	
ステップ 2	mkdir old_configs	新しいディレクトリを作成します。	
		コマンド例では、old_configs という名前のディレクトリの作成方法を示します。	
		ディレクトリ名では大文字と小文字が区別されます。	
		スラッシュ(/)間に指定できるディレクトリ名は最大 45 文字です。ディ レクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セ ミコロン、コロンは使用できません。	
ステップ 3	dir filesystem:	設定を確認します。	

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete** /**force/recursive** *filesystem:|file-url* 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除 するには、/recursive キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を 確認するためのプロンプトを省略するには、/force キーワードを使用します。この削除プロセスを実行 すると、最初に1度だけプロンプトが表示されます。archive download-sw コマンドでインストール され、不要になった古いソフトウェア イメージを削除するには、/force キーワードおよび /recursive キーワードを使用します。

filesystem には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用します。 file-url には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディ レクトリが削除されます。



ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、copy source-url destination-url 特権 EXEC コマンドを 使用します。送信元および宛先の URL には、running-config および startup-config キーワード ショートカットを使用できます。たとえば、copy running-config startup-config コマンドを実行する と、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存さ れ、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元と して特殊なファイル システム (xmodem:、ymodem:)を指定し、そこからコピーすることもできま す。

ネットワーク ファイル システムの URL には、ftp:、rcp:、tftp: などがあります。構文は次のとおりです。

- FTP (ファイル転送プロトコル): **ftp:**[[//username [:password]@location]/directory]/filename
- RCP : rcp:[[//username@location]/directory]/filename
- TFTP : **tftp:**[[//location]/directory]/filename

ローカルにある書き込み可能なファイル システムには flash: などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合 は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ(たとえば、copy flash: flash: コマンドは無効)

コンフィギュレーション ファイルによる copy コマンドの具体的な使用例については、「コンフィギュ レーション ファイルの操作」(P.B-10)を参照してください。

新しいバージョンをダウンロードするか、または既存のバージョンをアップロードして、ソフトウェア イメージをコピーするには、archive download-sw または archive upload-sw 特権 EXEC コマンドを 使用します。詳細については、「ソフトウェア イメージの操作」(P.B-28) を参照してください。

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。 指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、delete [/force] [/recursive] [*filesystem*:]/*file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、/recursive キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロン プトを省略するには、/force キーワードを使用します。この削除プロセスを実行すると、最初に1度だ けプロンプトが表示されます。archive download-sw コマンドでインストールされ、不要になった古 いソフトウェア イメージを削除するには、/force キーワードおよび /recursive キーワードを使用しま す。

filesystem: オプションを省略すると、cd コマンドで指定したデフォルトのデバイスが使用されます。 *file-url* には、削除するファイルのパス(ディレクトリ)および名前を指定します。

ファイルを削除しようとすると、削除の確認を求めるプロンプトが表示されます。



ファイルが削除された場合、その内容は回復できません。

次に、デフォルトのフラッシュメモリ デバイスからファイル *myconfig* を削除する例を示します。 Switch# **delete myconfig**

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます(次のセクションを参照)。

(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、copy 特権 EXEC コマ ンドまたは archive tar 特権 EXEC コマンドではなく、archive download-sw および archive upload-sw 特権 EXEC コマンドを使用することを推奨します。

tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

archive tar/create *destination-url* flash:/file-url

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、およ び作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。 flash:
- FTP の場合の構文は次のとおりです。 ftp:[[//username[:password]@location]/directory]/tar-filename.tar
- RCPの場合は、構文は次のとおりです。 rcp:[[//username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。 tftp:[[//location]/directory]/tar-filename.tar

tar-filename.tar は、作成される tar ファイルです。

flash:/file-url には、新しい tar ファイルの作成元になる、ローカル フラッシュ ファイル システム上の 場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリ のリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベル におけるすべてのファイルおよびディレクトリが、新規に作成された tar ファイルに書き込まれます。

次に、tar ファイルの作成方法を示します。次のコマンドを実行すると、ローカルなフラッシュデバイスのディレクトリ new-configs の内容が、172.20.10.30 にある TFTP サーバ上のファイル saved.tar に書き込まれます。

Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table source-url

*source-url*には、ローカルまたはネットワークファイルシステムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。 flash:
- FTP の場合の構文は次のとおりです。 ftp:[[//username[:password]@location]/directory]/tar-filename.tar
- RCPの場合は、構文は次のとおりです。 rcp:[[//username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。 tftp:[[//location]/directory]/tar-filename.tar

tar-filename.tar は、表示する tar ファイルです。

フラッシュ ファイル システムの操作

tar ファイルの後ろにオプションのファイルまたはディレクトリ リストを指定して、表示するファイル を制限することもできます。リストを指定すると、リスト内のファイルのみが表示されます。何も指定 しないと、すべてのファイルおよびディレクトリが表示されます。

次に、フラッシュメモリ内にあるスイッチ tar ファイルの内容を表示する例を示します。

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)
```

次に、/html ディレクトリおよびその内容のみを表示する例を示します。

```
Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>
```

tar ファイルの抽出

tar ファイルをフラッシュ ファイル システム上のディレクトリに抽出するには、次の特権 EXEC コマ ンドを使用します。

archive tar/xtract source-url flash:/file-url [dir/file...]

source-url には、ローカル ファイル システムの送信元 URL のエイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。 flash:
- FTP の場合の構文は次のとおりです。 ftp:[[//username[:password]@location]/directory]/tar-filename.tar
- RCPの場合は、構文は次のとおりです。 rcp:[[//username@location]/directory]/tar-filename.tar
- TFTP の場合の構文は次のとおりです。 tftp:[[//location]/directory]/tar-filename.tar

tar-filename.tar は、ファイルの抽出元の tar ファイルです。

flash:*lfile-url* [*dir/file...*] には、tar ファイルの抽出先にするローカル フラッシュ ファイル システム上の場所を指定します。抽出対象の tar ファイル内の任意のファイルまたはディレクトリの一覧を指定するには、*dir/file...* オプションを使用します。何も指定しないと、すべてのファイルおよびディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。このコマン ドを実行すると、*new-configs* ディレクトリがローカルなフラッシュ ファイル システムのルート ディ レクトリに抽出されます。*saved.tar* ファイルの残りのファイルは無視されます。

Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs

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

ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、 more [/ascii | /binary | /ebcdic] *file-url* 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

Switch# more tftp://serverA/hampton/savedconfig

```
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説 明します。

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力 されたコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成するには、 setup プログラムを使用するか、または setup 特権 EXEC コマンドを使用します。詳細は、第3章「ス イッチの IP アドレスおよびデフォルト ゲートウェイの割り当て」を参照してください。

TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコンフィギュレーション ファイルをコピー (ダウンロード) できます。次 のいずれかの目的でこの操作が必要になります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーションファイルを別のスイッチに使用するため。たとえば、ネットワークに別のスイッチを追加して、元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連部分を変更できます。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのス イッチに同じコンフィギュレーション コマンドをロードするため。

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー (アップロード) するには、 TFTP、FTP、または RCP を使用します。内容を変更する前に、現在のコンフィギュレーション ファ イルをサーバにバックアップしておくと、あとでサーバから元のコンフィギュレーション ファイルを 復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポートメカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。 これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

ここでは、次の設定情報について説明します。

- 「コンフィギュレーションファイルの作成および使用上の注意事項」(P.B-11)
- 「コンフィギュレーションファイルのタイプおよび場所」(P.B-11)
- 「テキストエディタによるコンフィギュレーションファイルの作成」(P.B-12)
- 「TFTP によるコンフィギュレーション ファイルのコピー」(P.B-12)

- 「FTP によるコンフィギュレーション ファイルのコピー」(P.B-15)
- 「RCP によるコンフィギュレーション ファイルのコピー」(P.B-19)
- 「設定情報の消去」(P.B-23)
- 「コンフィギュレーションの交換またはロール バック」(P.B-23)

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィ ギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要となるコマンドの一 部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコン フィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソールポートから接続することを推奨します。コンソールポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更によっては(スイッチのIPアドレスの変更やポートのディセーブル化など)、スイッチとの接続が切断される可能性があることにご注意ください。
- スイッチにパスワードが設定されていない場合は、enable secret secret-password グローバル コン フィギュレーション コマンドを使用して、パスワードを設定することを推奨します。



copy {ftp: | rcp: | tftp:} system:running-config 特権 EXEC コマンドを実行すると、コマンドライン にコマンドを入力した場合と同様に、スイッチにコンフィギュレーションファイルがロードされます。 コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコン フィギュレーションファイル内のコマンドによって既存のコンフィギュレーションファイル内のコマ ンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレー ションファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに 格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが 使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にし たりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーションファイルが組み合わされた(コピーされたコンフィ ギュレーションファイルが優先する)コンフィギュレーションファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成す るには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーし て (by using the copy {ftp: | rcp: | tftp:} nvram:startup-config 特権 EXEC コマンドを使用)、スイッ チを再起動します。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納 されています。2 つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に 設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した あと、copy running-config startup-config 特権 EXEC コマンドによる設定の保存は行わないようにし ます。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップ コンフィギュレーションは フラッシュ メモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンド を論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示し ます。

- ステップ1 スイッチからサーバに既存のコンフィギュレーションをコピーします。
 詳細については、「TFTP によるコンフィギュレーション ファイルのダウンロード」(P.B-13)、「FTP によるコンフィギュレーション ファイルのダウンロード」(P.B-16)、または「RCP によるコンフィ ギュレーション ファイルのダウンロード」(P.B-21) を参照してください。
- **ステップ 2** UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。
- **ステップ3** 目的のコマンドが格納されたコンフィギュレーションファイルの一部を抽出して、新しいファイルに 保存します。
- ステップ4 コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルを ワークステーションの TFTP ディレクトリ(UNIX ワークステーションの場合は、通常は /tftpboot) に コピーします。
- **ステップ5** ファイルに関する権限が world-read に設定されていることを確認します。

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用してスイッチを設定したり、別のスイッチからダウ ンロードしたり、TFTP サーバからダウンロードできます。また、コンフィギュレーション ファイルを TFTP サーバにコピー(アップロード)して、格納できます。

ここでは、次の設定情報について説明します。

- 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (P.B-12)
- 「TFTP によるコンフィギュレーション ファイルのダウンロード」(P.B-13)
- 「TFTP によるコンフィギュレーション ファイルのアップロード」(P.B-14)

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。
 Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot

/etc/services ファイルに次の行が含まれていることを確認します。

tftp 69/udp



- 注) /etc/inetd.conf および /etc/services ファイルを変更したあとに、inetd デーモンを再起動す る必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動する か、または fastboot コマンド (SunOS 4.x の場合) や reboot コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーショ ンのマニュアルを参照してください。
- スイッチにTFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとTFTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーションファイルがTFTPサーバ上の正しいディレクトリ内に あることを確認します(UNIXワークステーションの場合は、通常/tftpboot)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。 ファイルの権限は world-read でなければなりません。
- コンフィギュレーションファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、touch filename コマンドを入力します。 filename は、サーバにアップロードするときに使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル(空のファイルを作成する必要があった場合は、 空のファイルを含む)を上書きする場合は、そのファイルに関する権限が正しく設定されているこ とを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

- **ステップ1** コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。
- **ステップ2** 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.B-12) を参照して、TFTP サーバが適切に設定されていることを確認します。
- **ステップ3** コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
- ステップ4 TFTP サーバからコンフィギュレーション ファイルをダウンロードして、スイッチを設定します。 TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。 次に示す特権 EXEC コマンドのいずれかを使用します。
 - **copy tftp:**[[[//location]/directory]/filename] **system:running-config**
 - copy tftp:[[[//location]/directory]/filename] nvram:startup-config

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で 解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル tokyo-confg からソフトウェアを設定する例を示します。

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

- **ステップ1** 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.B-12) を参照して、TFTP サーバが適切に設定されていることを確認します。
- **ステップ 2** コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
- **ステップ3** スイッチのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレ スまたはホスト名、および宛先ファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- copy system:running-config tftp:[[[//location]/directory]/filename]
- copy nvram:startup-config tftp:[[[//location]/directory]/filename]

TFTP サーバにファイルがアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

Switch# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

コンフィギュレーション ファイルの操作

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバ に送信する必要があります。FTP を使用してコンフィギュレーション ファイルをスイッチからサーバ にコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- copy コマンドで指定されたユーザ名(ユーザ名が指定されている場合)
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- copy コマンドで指定されたパスワード(パスワードが指定されている場合)
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した username@switchname.domain パスワード。変数 username は現在のセッションに関連付けられているユーザ名、switchname は設定されているホスト名、domain はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられていなければなりません。 サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設 定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、ip ftp username および ip ftp password コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、 copy コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーションファイルはサーバ上のユーザ名に関 連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィ ギュレーションファイルがサーバ上のユーザのホームディレクトリに置かれている場合は、ユーザの 名前をリモートユーザ名として指定します。

詳細については、FTP サーバのマニュアルを参照してください。

ここでは、次の設定情報について説明します。

- 「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (P.B-16)
- 「FTP によるコンフィギュレーション ファイルのダウンロード」(P.B-16)
- 「FTP によるコンフィギュレーション ファイルのアップロード」(P.B-18)

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。
 show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip ftp username username グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名はNVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定します。
- コンフィギュレーションファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウン ロードまたはアップロードの準備」(P.B-16)を参照し て、FTP サーバが適切に設定されていることを確認しま す。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。
ステップ 3	configure terminal	スイッチ上で、グローバル コンフィギュレーション モー ドを開始します。
		このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ4、5、および6を参照)。
ステップ 4	ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password password	(任意) デフォルトのパスワードを変更します。

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の 手順を実行します。

コマンド	目的	
end	特権 EXEC モードに戻ります。	
сору	FTP を使用して、コンフィギュレーション ファイルを	
<pre>ftp:[[[//[username[:password]@]location]/director</pre>	ネットワーク サーバから実行コンフィギュレーション	
y]/filename] system:running-config	ファイルまたはスタートアップ コンフィギュレーション	
または	ファイルにコピーします。	
сору		
ftp: [[[//[username[:password]@]location]/director v]/filename] nvram:startup-config		

次に、*host1-confg*という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンド をロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウン ロードまたはアップロードの準備」(P.B-16)を参照し て、FTP サーバが適切に設定されていることを確認しま す。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
		このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ4、5、および6を参照)。
ステップ 4	ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password password	(任意) デフォルトのパスワードを変更します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	<pre>copy system:running-config ftp:[[[//[username[:password]@]location]/director y]/filename]</pre>	FTP を使用して、スイッチの実行コンフィギュレーショ ン ファイルまたはスタートアップ コンフィギュレーショ ン ファイルを指定場所に格納します。
	または	
	copy nvram:startup-config ftp: [[[//[username[:password]@]location]/director y]/filename]	

次に、実行コンフィギュレーション ファイル switch2-confg を、IP アドレスが 172.16.101.101 である リモート ホスト上のディレクトリ netadmin1 にコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイ ルをコピーする例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチ間でコンフィギュレーション ファイルをダウンロード、アップロード、お よびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP が サポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ(ま たはデーモン)を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のように ファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスす るだけですみます(ほとんどの UNIX システムは rsh をサポートしています)。ある場所から別の場所 ヘファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書 き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コ ンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次の リスト内の最初の有効なユーザ名を送信します。

- copy コマンドで指定されたユーザ名(ユーザ名が指定されている場合)
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定された ユーザ名(このコマンドが設定されている場合)
- 現在のTTY(端末)プロセスに関連付けられたリモートユーザ名。たとえば、ユーザがTelnetを 介してルータに接続されており、usernameコマンドを介して認証された場合は、リモートユーザ 名としてTelnetユーザ名がスイッチソフトウェアによって送信されます。
- スイッチのホスト名

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウント を定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイ ルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピー されます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内 に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

ここでは、次の設定情報について説明します。

- 「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (P.B-20)
- 「RCP によるコンフィギュレーション ファイルのダウンロード」(P.B-21)
- 「RCP によるコンフィギュレーション ファイルのアップロード」(P.B-22)

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない 場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。 show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使 用しない場合は、すべてのコピー処理中に ip rcmd remote-username username グローバル コン フィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユー ザ名がある場合は、そのユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。 特定のコピー操作にのみ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定 します。
- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求 が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上 のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッ チに次のコンフィギュレーション行が含まれているとします。

hostname Switch1 ip rcmd remote-username User0

このスイッチの IP アドレスを Switch1.company.com に変換する場合は、RCP サーバ上の User0 用の.rhosts ファイルに次の行が含まれている必要があります。

Switch1.company.com Switch1

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードま たはアップロードの準備」(P.B-20)を参照して、RCP サーバが 適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチ にログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名 を上書きする場合のみです (ステップ4および5を参照)。
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy rcp: [[[//[username@]location]/directory]/ filename] system:running-config	RCP を使用して、コンフィギュレーション ファイルをネット ワーク サーバから実行コンフィギュレーション ファイルまたは スタートアップ コンフィギュレーション ファイルにコピーしま
	または	す。
	copy rcp:[[[//[username@]location]/directory]/ filename] nvram:startup-config	

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンド をロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、netadmin1 というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル host2-confg が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ netadmin1 からスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の 手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウン
		ロードまたはアップロードの準備」(P.B-20)を参照し
		て、RCP サーバが適切に設定されていることを確認しま
		す。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス
		イッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始しま
		す。
		このステップが必要になるのは、デフォルトのリモート
		ユーザ名を上書きする場合のみです(ステップ4および
		5 を参照)。
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	copy system:running-config	RCP を使用して、コンフィギュレーション ファイルをス
	<pre>rcp:[[[//[username@]location]/directory]/filename</pre>	イッチの実行コンフィギュレーション ファイルまたはス
]	タートアップ コンフィギュレーション ファイルからネッ
	または	トワーク サーバにコピーします。
	copy nvram:startup-config	
	<pre>rcp:[[[//[username@]location]/directory]/filename</pre>	
]	

次に、実行コンフィギュレーション ファイル switch2-confg を、IP アドレスが 172.16.101.101 である リモート ホスト上のディレクトリ netadmin1 にコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュ レーションを使用しないでスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、 新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションを消去するには、erase nvram: または erase startup-config 特権 EXEC コマンドを使用します。



削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、delete flash:*filename* 特権 EXEC コマンドを 使用します。file prompt グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削 除する前に確認を求めるプロンプトが表示されます。デフォルトでは、有害なファイル操作を行った場 合に、確認を求めるプロンプトが表示されます。file prompt コマンドの詳細については、『*Cisco IOS Command Reference, Release 12.2*』を参照してください。

<u>/</u>] 注意

削除されたファイルは復元できません。

コンフィギュレーションの交換またはロール バック

コンフィギュレーション交換およびロールバック機能を使用すると、実行コンフィギュレーションと保存されている任意の Cisco IOS コンフィギュレーション ファイルを交換できます。ロールバック機能を使用すると以前のコンフィギュレーションに戻すことができます。

ここでは、次の情報について説明します。

- 「コンフィギュレーション交換およびロールバックの概要」(P.B-23)
- 「設定時の注意事項」(P.B-25)
- 「コンフィギュレーションアーカイブの設定」(P.B-26)
- 「コンフィギュレーション交換またはロールバック動作の実行」(P.B-27)

コンフィギュレーション交換およびロールバックの概要

コンフィギュレーション交換およびロールバック機能を使用する場合、次の内容を理解しておく必要が あります。

- 「コンフィギュレーションのアーカイブ」(P.B-24)
- 「コンフィギュレーションの交換」(P.B-24)
- 「コンフィギュレーションのロール バック」(P.B-25)

コンフィギュレーションのアーカイブ

コンフィギュレーション アーカイブは、コンフィギュレーション ファイルのアーカイブを保管、構成、 管理するメカニズムです。configure replace 特権 EXEC コマンドを使用すると、コンフィギュレー ション ロールバック機能が向上します。または、copy running-config destination-url 特権 EXEC コマ ンドを使用して実行コンフィギュレーションのコピーを保存し、交換ファイルをローカルまたはリモー トで保存することができます。ただし、この方法ではファイルの自動管理を行うことはできません。コ ンフィギュレーション交換およびロールバック機能を使用すれば、実行コンフィギュレーションのコ ピーを自動的にコンフィギュレーション アーカイブに保存できます。

archive config 特権 EXEC コマンドを使用して、コンフィギュレーションをコンフィギュレーション アーカイブに保存します。その際は標準のディレクトリとファイル名のプレフィクスが使用され、連続 ファイルを保存するたびにバージョン番号(およびオプションでタイムスタンプ)が自動的に付加され ます。このときのバージョン番号は1つずつ大きくなります。アーカイブに保存する実行コンフィギュ レーションの数は指定することができます。保存したファイル数が指定数に達した場合は、次の新しい ファイルを保存するときに最も古いファイルが自動的に削除されます。show archive 特権 EXEC コマ ンドを使用すると、コンフィギュレーション アーカイブに保存されたすべてのコンフィギュレーショ ンファイルを表示できます。

Cisco IOS コンフィギュレーション アーカイブでは、コンフィギュレーション ファイルを保存し、 configure replace コマンドで使用します。ファイル システムは、FTP、HTTP、RCP、TFTP のいずれ かです。

コンフィギュレーションの交換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存されている 任意のコンフィギュレーション ファイルを交換できます。configure replace コマンドを入力すると実 行コンフィギュレーションと指定した交換コンフィギュレーションが比較され、コンフィギュレーショ ンの差分が生成されます。生成された差分がコンフィギュレーションの交換に使用されます。コンフィ ギュレーション交換は、通常 3 回以下のパスで完了します。ループを防ぐために 6 回以上のパスが実行 されることはありません。

copy *source-url* **running-config** 特権 EXEC コマンドを使用すると、保存されているコンフィギュレーション ファイルが実行コンフィギュレーションに保存できます。このコマンドを **configure replace** *target-url* 特権コマンドの代わりに使用する場合は、次のような違いがある点に注意してください。

- copy source-url running-config コマンドはマージ動作であり、コピー元ファイルと実行コンフィ ギュレーションのコマンドをすべて保存します。このコマンドでは、コピー元ファイルに実行コン フィギュレーションのコマンドがない場合でも実行コンフィギュレーションのコマンドを削除しま せん。configure replace target-url コマンドの場合は、交換先のファイルに実行コンフィギュレー ションのコマンドがない場合は実行コンフィギュレーションから削除し、実行コンフィギュレー ションにないコマンドがある場合はそのコマンドを追加します。
- copy source-url running-config コマンドのコピー元ファイルとして、部分コンフィギュレーションファイルを使用できます。configure replace target-url コマンドの交換ファイルとして、完全なコンフィギュレーションファイルを使用する必要があります。

コンフィギュレーションのロール バック

configure replace コマンドを使用して、前回コンフィギュレーションを保存したあとで行った変更を ロール バックさせることもできます。コンフィギュレーション ロールバック機能では、コンフィギュ レーションを特定の変更時点に戻すのではなく、保存されているコンフィギュレーション ファイルに 基づいて特定のコンフィギュレーションに戻します。

コンフィギュレーション ロールバック機能を利用する場合は、コンフィギュレーションを変更する前 に実行コンフィギュレーションを保存する必要があります。その後、コンフィギュレーションを変更し たあとで configure replace *target-url* コマンドを使用し、保存したコンフィギュレーション ファイル を使って変更をロール バックします。

保存されている任意のファイルをロールバック コンフィギュレーションとして指定できます。一部の ロールバック モデルと同様、ロールバック回数は無制限です。

設定時の注意事項

コンフィギュレーション交換およびロールバックを設定し実行する場合は、次の注意事項に従ってくだ さい。

- スイッチのメモリの空き容量が、2つのコンフィギュレーションファイル(実行コンフィギュレーションと保存されている交換コンフィギュレーション)の合計容量よりも大きいことを確認します。スイッチのメモリ容量の方が小さい場合、コンフィギュレーション交換は実行されません。
- また、スイッチにコンフィギュレーション交換やロールバック コンフィギュレーション コマンド が実行できるほどの空き容量があることも確認してください。
- ネットワークデバイスの物理コンポーネント(物理インターフェイスなど)に関連するコンフィ ギュレーションコマンドを実行コンフィギュレーションに追加または削除することはできません。
 - インターフェイスがデバイス上に物理的に存在する場合、コンフィギュレーション交換を行っても実行コンフィギュレーションから interface interface-id コマンド行を削除することはできません。
 - インターフェイスがデバイス上に物理的に存在しない場合、interface interface-id コマンド行 を実行コンフィギュレーションに追加することはできません。
- configure replace コマンドを使用する場合、保存されているコンフィギュレーションを実行コンフィギュレーションの交換コンフィギュレーションファイルとして指定する必要があります。交換ファイルは Cisco IOS デバイスによって生成された完全なコンフィギュレーションであることが必要です(たとえば copy running-config destination-url コマンドで生成したコンフィギュレーション)。



交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび archive config コマンドとと もに使用することは任意ですが、コンフィギュレーション ロールバックを行うときに大きな利点があ ります。archive config コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく 必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順 を実行します。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	archive	アーカイブコンフィギュレーション モードを開始します。
ステップ 3	path url	コンフィギュレーション アーカイブに、ファイルのディレクトリとファイ ル名プレフィクスを指定します。
ステップ 4	maximum number	(任意) コンフィギュレーション アーカイブに保存する実行コンフィギュ レーションのアーカイブ ファイルの最大数を指定します。
		<i>number :</i> コンフィギュレーション アーカイブでの実行コンフィギュレー ション ファイルの最大数。有効な値は 1 ~ 14 で、デフォルトは 10 です。
		(注) このコマンドを使用する前に path アーカイブ コンフィギュレー ション コマンドを入力して、コンフィギュレーション アーカイブ のファイルのディレクトリとファイル名プレフィクスを指定して おく必要があります。
ステップ 5	time-period minutes	(任意) コンフィギュレーション アーカイブに実行コンフィギュレーショ ンのアーカイブ ファイルを自動保存する間隔を設定します。
		<i>minutes</i> :コンフィギュレーションアーカイブに実行コンフィギュレー ションのアーカイブを自動保存する間隔を、分単位で指定します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

コンフィギュレーション交換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換する には、特権 EXEC モードで次の手順を実行します。

	コマンド	目的	
ステップ 1	archive config	(任意)実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。	
		(注) path アーカイブ コンフィギュレーション コマンドを入力してか ら、このコマンドを実行します。	
ステップ 2	configure terminal	グローバル コンフィギュレーション モードを開始します。	
ステップ 3		実行コンフィギュレーションに必要な変更を行います。	
ステップ 4	exit	特権 EXEC モードに戻ります。	
ステップ 5	configure replace <i>target-url</i> [list] [force] [time <i>seconds</i>] [nolock]	実行コンフィギュレーション ファイルを保存されているコンフィギュレー ション ファイルと交換します。	
		<i>target-url</i> :保存されているコンフィギュレーション ファイルの URL (ファイル システムからアクセス可能)。実行コンフィギュレーションと交 換するファイルで、ステップ 2 で archive config 特権 EXEC コマンドを 使用して作成したコンフィギュレーション ファイルなどです。	
		list: コンフィギュレーション交換動作のパスごとにソフトウェアパー サーによって適用されるコマンドエントリのリストを表示します。パスの 合計数も表示されます。	
		force:実行コンフィギュレーション ファイルと指定した保存済みコン フィギュレーション ファイルの交換を確認なしで実行します。	
		time seconds: configure confirm コマンドを入力して実行コンフィギュ レーションファイルとの交換を確認するまでの時間を秒単位で指定しま す。指定時間内に configure confirm コマンドを入力しない場合、コン フィギュレーション交換動作が自動的に停止します (つまり、実行コン フィギュレーションファイルは configure replace コマンドを入力する以 前に存在していたコンフィギュレーションに保存されます)。	
		(注) time seconds コマンドライン オプションを使用する前に、コン フィギュレーション アーカイブをイネーブルにしておく必要があ ります。	
		nolock:コンフィギュレーション交換動作時に他のユーザが実行コンフィ ギュレーションを変更できないようにする実行コンフィギュレーション ファイルのロックをディセーブルにします。	
ステップ 6	configure confirm	(任意)実行コンフィギュレーションと保存されているコンフィギュレー ション ファイルとの交換を確認します。	
		(注) このコマンドは、time seconds キーワードと configure replace コ マンドの引数が指定されている場合にだけ使用します。	
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。	

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフト ウェアを格納するソフトウェア イメージ ファイルをアーカイブ (ダウンロードおよびアップロード) する方法を示します。

(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、copy 特権 EXEC コマンドまたは archive tar 特権 EXEC コマンドではなく、archive download-sw および archive upload-sw 特権 EXEC コマンドを使用することを推奨します。.

スイッチ ソフトウェアをアップグレードするには、TFTP、FTP、または RCP サーバからスイッチ イ メージ ファイルをダウンロードします。TFTP サーバへアクセスできない場合、Web ブラウザ (HTTP) で PC またはワークステーションへ直接ソフトウェア イメージ ファイルをダウンロードしま す。次にデバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードし ます。TFTP サーバまたは Web ブラウザ (HTTP) を使用したスイッチのアップグレードについては、 リリース ノートを参照してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュメ モリに保存したりできます。

バックアップのために、スイッチ イメージ ファイルを TFTP、FTP、または RCP サーバにアップロー ドします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダ ウンロードする場合に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポートメカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。 これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

ここでは、次の設定情報について説明します。

- 「スイッチ上のイメージの場所」(P.B-29)
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」(P.B-29)
- 「TFTP によるイメージファイルのコピー」(P.B-30)
- 「FTP によるイメージファイルのコピー」(P.B-34)
- 「RCP によるイメージファイルのコピー」(P.B-38)



ソフトウェア イメージ、およびサポートされているアップグレード パスの一覧については、スイッチ に付属のリリース ノートを参照してください。

ソフトウェア イメージの操作

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に .bin ファイルとして格納されます。サ ブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフ ラッシュ メモリ (flash:) に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼動しているソフトウェア バージョンを参照できます。画面上で、System image file is...で始まる行を調べます。この行は、イメージが格納されているフラッシュ メモリ内のディレクトリ名を示します。

dir *filesystem*: 特権 EXEC コマンドを使用して、フラッシュ メモリに格納されている他のソフトウェ アイメージのディレクトリ名を調べることもできます。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- tar ファイルの内容を表形式で示す info ファイル
- Cisco IOS イメージや Web 管理用ファイルなど、他のイメージおよびファイルが格納された1つまたは複数のサブディレクトリ

次に、info ファイルに格納された情報の一部の例を示します。表 B-3 に、この情報の詳細を示します。

```
system type:0x00000000:image-name
   image family:xxxx
   stacking number:x
   info end:
version suffix:xxxx
   version directory:image-name
   image system type id:0x0000000
   image name: image-nameB.bin
   ios image file size:6398464
    total image file size:8133632
   image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
   image family:xxxx
   stacking_number:x
   board ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
   info end:
```



stacking_number フィールドは無視してください。このフィールドはスイッチに適用されません。

表 B-3 info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージ バージョン ストリングのサフィックスを指定します。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされているディレクトリ を指定します。
image_name	tar ファイル内の Cisco IOS イメージの名前を指定します。
ios_image_file_size	tar ファイル内の Cisco IOS イメージのサイズを指定します。このサイズは、Cisco IOS イ メージのみを保持するために必要なフラッシュ メモリ サイズの概算値です。

表 B-3 info ファイルの説明 (続き)

フィールド	説明
total_image_file_size	tar ファイル内のすべてのイメージ (Cisco IOS イメージおよび Web 管理ファイル) のサイズ を指定します。このサイズは、これらのファイルを保持するために必要なフラッシュ メモリ サイズの概算値です。
image_feature	イメージの主な機能に関する説明です。
image_min_dram	このイメージを実行するために必要な DRAM の最小サイズを指定します。
image_family	ソフトウェアをインストールできる製品ファミリーに関する説明です。

TFTP によるイメージ ファイルのコピー

TFTP サーバからスイッチ イメージをダウンロードしたり、スイッチから TFTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウン ロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを 保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードさ れたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードするために使用 できます。



ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、copy 特権 EXEC コマンドまたは archive tar 特権 EXEC コマンドではなく、archive download-sw および archive upload-sw 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.B-31)
- 「TFTP によるイメージファイルのダウンロード」(P.B-31)
- 「TFTP によるイメージファイルのアップロード」(P.B-33)

ソフトウェア イメージの操作

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。
 Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot

/etc/services ファイルに次の行が含まれていることを確認します。

tftp 69/udp



- (etc/inetd.conf および /etc/services ファイルを変更したあとに、inetd デーモンを再起動す る必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動する か、または fastboot コマンド (SunOS 4.x の場合)や reboot コマンド (Solaris 2.x または SunOS 5.x の場合)を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。
- スイッチにTFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとTFTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 /tftpboot)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。 ファイルの権限は world-read でなければなりません。
- イメージファイルをアップロードする前に、TFTPサーバに空のファイルを作成する必要があります。空のファイルを作成するには、touch filenameコマンドを入力します。filenameは、イメージをサーバにアップロードするときに使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル(空のファイルを作成する必要があった場合は、 空のファイルを含む)を上書きする場合は、そのファイルに関する権限が正しく設定されているこ とを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。 TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ1~3を実行します。現在のイメージを保存するには、ステップ3へ進みます。

	コマンド	目的
ステップ 1		イメージをワークステーション上の適切な TFTP ディレクトリ
		にコピーします。TFTP サーバが適切に設定されていることを
		確認します(「TFTP によるイメージ ファイルのダウンロード
		またはアップロードの準備」(P.B-31)を参照)。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッ
		チにログインします。

	コマンド	目的
ステップ 3	archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロード して、現在のイメージを上書きします。
		 /overwrite オプションを指定すると、フラッシュメモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。
		 /reload オプションを指定すると、設定が変更されて保存 されなかった場合を除いて、イメージのダウンロード後に システムがリロードされます。
		• <i>Illocation</i> には、TFTP サーバの IP アドレスを指定します。
		 /directory/image-name.tar には、ディレクトリ(任意)お よびダウンロードするイメージを指定します。ディレクト リ名およびイメージ名では大文字と小文字が区別されま す。
ステップ 4	archive download-sw/leave-old-sw/reload tftp:[[//location]/directory]/image-name.tar	TFTP サーバからスイッチにイメージ ファイルをダウンロード して、現在のイメージを保存します。
		 /leave-old-sw オプションを指定すると、ダウンロード後に 古いソフトウェア バージョンが保存されます。
		 /reload オプションを指定すると、設定が変更されて保存 されなかった場合を除いて、イメージのダウンロード後に システムがリロードされます。
		• <i>Illocation</i> には、TFTP サーバの IP アドレスを指定します。
		 /directory/image-name.tar には、ディレクトリ(任意)お よびダウンロードするイメージを指定します。ディレクト リ名およびイメージ名では大文字と小文字が区別されま す。

ダウンロードアルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。/overwrite オプションを指定した場合、ダウンロードアルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注)

フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれ かを同じバージョンで上書きする場合は、/overwrite オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする 十分なスペースがない場合に、現在稼動中のイメージを保存しようとすると、ダウンロードプロセス が停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス(flash:) にアルゴリズムに よってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新 しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。
ソフトウェア イメージの操作

ダウンロード プロセス中に古いイメージを保存した場合は(/leave-old-sw キーワードを指定した場合 は)、delete /force/recursive filesystem:/file-url 特権 EXEC コマンドを入力して、そのイメージを削除 できます。filesystem には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用し ます。file-url には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイ ルおよびディレクトリが削除されます。

注意

ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。

TFTP によるイメージ ファイルのアップロード

スイッチから TFTP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチ や、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイスマネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		TFTP サーバが適切に設定されていることを確認します (「TFTP によるイメージ ファイルのダウンロードまたはアップ ロードの準備」(P.B-31)を参照)。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッ チにログインします。
ステップ 3	archive upload-sw tftp:[[//location]/directory]/image-name.tar	現在稼動中のスイッチ イメージを TFTP サーバにアップロード します。
		• <i>Illocation</i> には、TFTP サーバの IP アドレスを指定します。
		 /directorylimage-name.tar には、ディレクトリ(任意)お よびアップロードするソフトウェアイメージの名前を指定 します。ディレクトリ名およびイメージ名では大文字と小 文字が区別されます。image-name.tar は、サーバ上に格納 するソフトウェアイメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意

ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。

FTP によるイメージ ファイルのコピー

FTP サーバからスイッチ イメージをダウンロードしたり、スイッチから FTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウン ロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを 保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードさ れたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用 できます。

(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、copy 特権 EXEC コマンドまたは archive tar 特権 EXEC コマンドではなく、archive download-sw および archive upload-sw 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「FTP によるイメージファイルのダウンロードまたはアップロードの準備」(P.B-34)
- 「FTP によるイメージファイルのダウンロード」(P.B-35)
- 「FTP によるイメージファイルのアップロード」(P.B-37)

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバ に送信する必要があります。FTP を使用してイメージ ファイルをスイッチからサーバにコピーすると、 Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- archive download-sw または archive upload-sw 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- archive download-sw または archive upload-sw 特権 EXEC コマンドで指定されたパスワード (パスワードが指定されている場合)
- ip ftp password password グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した username@switchname.domain パスワード。変数 username は現在のセッションに関連付けられているユーザ名、switchname は設定されているホスト名、domain はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられていなければなりません。 サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設 定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、ip ftp username および ip ftp password コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、archive download-sw または archive upload-sw 特権 EXEC コマンドでユーザ名を指定します。

ソフトウェア イメージの操作

サーバがディレクトリ構造である場合、イメージファイルはサーバ上のユーザ名に関連付けられた ディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージファイルが サーバ上のユーザのホームディレクトリ内に置かれている場合は、ユーザの名前をリモートユーザ名 として指定します。

FTP を使用してイメージファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない 場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。 show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使 用しない場合は、ip ftp username username グローバル コンフィギュレーション コマンドを使用 して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用され ます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセ スしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定 する必要はありません。ユーザ名をこの処理のためだけに指定する場合は、archive download-sw または archive upload-sw 特権 EXEC コマンド内でユーザ名を指定します。
- イメージファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み 要求が許可されるように、適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。 FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ1~7の手順を実行します。現在のイメージを保存するには、ステップ7へ進みま す。

	コマンド	目的
ステップ 1		「FTP によるイメージ ファイルのダウンロードまたはアッ
		プロードの準備」(P.B-34)を参照して、FTP サーバが適 切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始します。
		このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです(ス テップ4、5、および6を参照)。
ステップ 4	ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password password	(任意) デフォルトのパスワードを変更します。
ステップ 6	end	特権 EXEC モードに戻ります。

	コマンド	目的	
ステップ 7	archive download-sw /overwrite /reload ftp:[[//username[:password]@location]/director y]/image-name.tar	FTP サーバからスイッチにイメージ ファイルをダウンロー ドして、現在のイメージを上書きします。	
		 /overwrite オプションを指定すると、フラッシュメモリ内のソフトウェアイメージがダウンロードされたイメージによって上書きされます。 	
		 /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 	
		 //username[:password] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられていなければなりません。詳細については、「FTP によるイメージファイルのダウンロードまたはアップロードの準備」(P.B-34)を参照してください。 	
		• <i>@location</i> には、FTP サーバの IP アドレスを指定しま す。	
		 directorylimage-name.tar には、ディレクトリ(任意) およびダウンロードするイメージを指定します。ディ レクトリ名およびイメージ名では大文字と小文字が区 別されます。 	
ステップ 8	archive download-sw/leave-old-sw/reload ftp:[[//username[:password]@location]/director y]/image-name.tar	FTP サーバからスイッチにイメージ ファイルをダウンロー ドして、現在のイメージを保存します。	
		 /leave-old-sw オプションを指定すると、ダウンロード 後に古いソフトウェア バージョンが保存されます。 	
		 /reload オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 	
		 //username[:password] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられていなければなりません。詳細については、「FTP によるイメージファイルのダウンロードまたはアップロードの準備」(P.B-34)を参照してください。 	
		• <i>@location</i> には、FTP サーバの IP アドレスを指定しま す。	
		 directorylimage-name.tar には、ディレクトリ(任意) およびダウンロードするイメージを指定します。ディ レクトリ名およびイメージ名では大文字と小文字が区 別されます。 	

ダウンロードアルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。/overwrite オプションを指定した場合、ダウンロードアルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

ソフトウェア イメージの操作



フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれ かを同じバージョンで上書きする場合は、/overwrite オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする 十分なスペースがない場合に、現在稼動中のイメージを保存しようとすると、ダウンロードプロセス が停止して、エラーメッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (flash:) にアルゴリズムに よってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新 しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は (/leave-old-sw キーワードを指定した場合 は)、delete /force/recursive filesystem:/file-url 特権 EXEC コマンドを入力して、そのイメージを削除 できます。filesystem には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使用し ます。file-url には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のす べてのファイルおよびディレクトリが削除されます。

注意

ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。

FTP によるイメージ ファイルのアップロード

スイッチから FTP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチや、 同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされて いる場合に限って、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
	「FTP によるコンフィギュレーション ファイルのダウン ロードまたはアップロードの準備」(P.B-16)を参照し て、FTP サーバが適切に設定されていることを確認しま す。
	コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。
configure terminal	グローバル コンフィギュレーション モードを開始しま す。
	このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ip ftp password password	(任意) デフォルトのパスワードを変更します。
	コマンド configure terminal ip ftp username username ip ftp password password

	コマンド	目的
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	<pre>archive upload-sw ftp:[[//[username[:password]@]location]/director y]/image-name.tar</pre>	現在稼動中のスイッチ イメージを FTP サーバにアップ ロードします。
		 <i>Ilusername:password</i>には、ユーザ名およびパスワードを指定します。これらは、FTPサーバのアカウントに関連付けられていなければなりません。詳細については、「FTPによるイメージファイルのダウンロードまたはアップロードの準備」(P.B-34)を参照してください。
		• <i>@location</i> には、FTP サーバの IP アドレスを指定します。
		 <i>Idirectorylimage-name.tar</i>には、ディレクトリ(任意)およびアップロードするソフトウェアイメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 <i>image-name.tar</i>は、サーバ上に格納するソフトウェアイメージの名前です

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理 ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイル がアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。

注意

ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。

RCP によるイメージ ファイルのコピー

RCP サーバからスイッチ イメージをダウンロードしたり、スイッチから RCP サーバにスイッチ イ メージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウン ロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを 保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用 できます。

(注)

ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、copy 特権 EXEC コマンドまたは archive tar 特権 EXEC コマンドではなく、archive download-sw および archive upload-sw 特権 EXEC コマンドを使用することを推奨します。

ここでは、次の設定情報について説明します。

- 「RCP によるイメージファイルのダウンロードまたはアップロードの準備」(P.B-39)
- 「RCP によるイメージファイルのダウンロード」(P.B-40)
- 「RCP によるイメージファイルのアップロード」(P.B-42)

ソフトウェア イメージの操作

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別 の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と 異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP が サポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ (ま たはデーモン)を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のように ファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスす るだけですみます (ほとんどの UNIX システムは rsh をサポートしています)。ある場所から別の場所 ヘファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書 き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。 RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは 次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)
- **ip rcmd remote-username** *Username* グローバル コンフィギュレーション コマンドで設定された ユーザ名(このコマンドが設定されている場合)
- 現在のTTY(端末)プロセスに関連付けられたリモートユーザ名。たとえば、ユーザが Telnet を 介してルータに接続されており、username コマンドを介して認証された場合は、リモートユーザ 名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウント を定義する必要があります。サーバがディレクトリ構造である場合、イメージファイルはサーバ上の リモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たと えば、イメージファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザ の名前をリモート ユーザ名として指定します。

RCP を使用してイメージファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない 場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。 show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使 用しない場合は、すべてのアーカイブ処理中に使用される ip rcmd remote-username username グ ローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新し いユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、 有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要は ありません。この処理のためだけにユーザ名を指定する場合は、archive download-sw または archive upload-sw 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求 が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上 のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。

たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

hostname Switch1 ip rcmd remote-username User0

このスイッチの IP アドレスを Switch1.company.com に変換する場合は、RCP サーバ上の User0 用の.rhosts ファイルに次の行が含まれている必要があります。

Switch1.company.com Switch1

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。 RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ1~6の手順を実行します。現在のイメージを保存するには、ステップ6へ進みま す。

	コマンド	目的	
ステップ 1		「RCP によるイメージファイルのダウンロードまたは アップロードの準備」(P.B-39)を参照して、RCP サー バが適切に設定されていることを確認します。	
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。	
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始しま す。	
		このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです(ステップ4および 5を参照)。	
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。	
ステップ 5	end	特権 EXEC モードに戻ります。	

	 コマンド	目的
ステップ6	archive download-sw /overwrite /reload	PCP サーバからスイッチにイメージファイルをダウン
	rcp:[[[//[username@]location]/directory]/image-n ame.tar]	ロードして、現在のイメージを上書きします。
		 /overwrite オプションを指定すると、フラッシュメ モリ内のソフトウェア イメージがダウンロードされ たイメージによって上書きされます。
		 /reload オプションを指定すると、設定が変更されて 保存されなかった場合を除いて、イメージのダウン ロード後にシステムがリロードされます。
		 <i>Ilusername</i>には、ユーザ名を指定します。RCP コ ピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義す る必要があります。詳細については、「RCP による イメージファイルのダウンロードまたはアップロー ドの準備」(P.B-39)を参照してください。
		• <i>@location</i> には、RCP サーバの IP アドレスを指定します。
		 <i>Idirectorylimage-name.tar</i>には、ディレクトリ(任意)およびダウンロードするイメージを指定します。 ディレクトリ名およびイメージ名では大文字と小文 字が区別されます。
ステップ 7	archive download-sw/leave-old-sw/reload rcp:[[[//[username@]location]/directory]/image-n ame.tar]	RCP サーバからスイッチにイメージ ファイルをダウン ロードして、現在のイメージを保存します。
		 /leave-old-sw オプションを指定すると、ダウンロー ド後に古いソフトウェアバージョンが保存されます。
		 /reload オプションを指定すると、設定が変更されて 保存されなかった場合を除いて、イメージのダウン ロード後にシステムがリロードされます。
		 <i>Ilusername</i>には、ユーザ名を指定します。RCP コ ピー要求を実行するためには、ネットワークサーバ 上にリモートユーザ名のアカウントを定義する必要 があります。詳細については、「RCPによるイメー ジファイルのダウンロードまたはアップロードの準 備」(P.B-39)を参照してください。
		• <i>@location</i> には、RCP サーバの IP アドレスを指定します。
		 <i>Idirectory</i>]<i>/image-name.tar</i>には、ディレクトリ(任意)およびダウンロードするイメージを指定します。 ディレクトリ名およびイメージ名では大文字と小文 字が区別されます。

ダウンロードアルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。/overwrite オプションを指定した場合、ダウンロードアルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注)

フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれ かを同じバージョンで上書きする場合は、/overwrite オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする 十分なスペースがない場合に、稼動中のイメージを保存しようとすると、ダウンロード プロセスが停 止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (flash:) にアルゴリズムに よってインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新 しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は(/leave-old-sw キーワードを指定した 場合は)、delete /force/recursive filesystem:/file-url 特権 EXEC コマンドを入力して、そのイメージを 削除できます。filesystem には、システム ボードのフラッシュ デバイスを指定する場合は flash: を使 用します。file-url には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内 のすべてのファイルおよびディレクトリが削除されます。



ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。あとでこのイメージをこのスイッチや、 同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイスマネージャと連携する Web 管理ページが既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるイメージファイルのダウンロードまたは アップロードの準備」(P.B-39)を参照して、RCP サー バが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、ス イッチにログインします。
ステップ 3	configure terminal	グローバル コンフィギュレーション モードを開始しま す。
		このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです(ステップ4および 5を参照)。
ステップ 4	ip rcmd remote-username username	(任意) リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 5 ステップ 6	end archive upload-sw rcp:[[[//[username@]location]/directory]/image-n ame.tar]	 特権 EXEC モードに戻ります。 現在稼動中のスイッチ イメージを RCP サーバにアップ ロードします。 <i>Ilusername</i> には、ユーザ名を指定します。RCP コ ピー要求を実行するためには、ネットワーク サーバ 上にリモート ユーザ名のアカウントを定義する必要 があります。詳細については、「RCP によるイメー ジファイルのダウンロードまたはアップロードの準 備」(P.B-39)を参照してください。 <i>@location</i> には、RCP サーバの IP アドレスを指定し ます。 <i>Idirectoryllimage-name</i>.tar には、ディレクトリ(任
		 <i>Idirectory]/image-name</i>.tar には、デイレクトリ(任意)およびアップロードするソフトウェアイメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 <i>image-name</i>.tar は、サーバ上に格納するソフトウェ

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これ らのファイルがアップロードされたあとに、アップロード アルゴリズムによって tar ファイル形式が作成されます。



ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更 しないでください。 ■ ソフトウェア イメージの操作

■ Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド



Catalyst 2950 スイッチから Catalyst 2960 スイッチへのアップグレードの推奨

ここでは、Catalyst 2950 スイッチから Catalyst 2960 スイッチへのアップグレードの際に問題となる、 設定の互換性の問題と、機能的な動作の相違点について説明します。

この付録で説明する内容は、次のとおりです。

- 「設定の互換性の問題」(P.C-1)
- 「機能的な動作の非互換項目」(P.C-6)

設定の互換性の問題

2 つのスイッチ プラットフォームでコンフィギュレーション コマンドに違いがあるのには、次のよう な理由があります。

- Catalyst 2950 スイッチでは Cisco IOS 12.1EA ソフトウェアが稼動していて、Catalyst 2960 スイッ チでは Cisco IOS 12.2SE ソフトウェアが稼動していること。
- それぞれのスイッチファミリーで使用しているハードウェアが異なること。

Catalyst 2950 スイッチのコマンドを使用した場合、Catalyst 2960 スイッチではサポートされていない ことがあります。Catalyst 2960 スイッチのソフトウェアは、互換性のないコマンドを次のように処理 します。

- 受け付けられ、変換されます。メッセージが表示されます。
- 拒否されます。メッセージが表示されます。

ほとんどの場合、コンフィギュレーション ファイルは拒否されることなくロードされます。表 C-1 に、 Catalyst 2950 の例外を示します。アルファベット順に機能を示し、Catalyst 2950 コマンドとその説 明、それに対する Catalyst 2960 スイッチの動作を記載します。

機能	Catalyst 2950 スイッチのコマンドと説明	Catalyst 2960 スイッチでの結果
Authentication, Authorization, Accounting	これらのグローバル コンフィギュレーション コマン ドは Cisco IOS 12.1EA のものです。 aaa preauth	Cisco IOS 12.2E の構築時、これらのコマンド は意図的に削除され、Cisco IOS 12.2SE では サポートされていません。
(AAA;認証、 許可、 アカウンティング)	aaa processes 1-64 aaa route download 1-1440	Catalyst 2960 スイッチでは、これらのコマン ドは拒否され、次のメッセージが表示されま す。 Switch(config)# aaa processes 10
		%Invalid input detected at `^' marker.
クラスタ	Catalyst 2950 スイッチでサポートされている管理 VLAN(仮想LAN)は1台のみです。これを変更す るには、次のグローバル コンフィギュレーションコ マンドを使用します。	Catalyst 2960 スイッチでは、候補およびクラ スタ メンバー スイッチとの接続は、クラスタ コマンド スイッチと共通の任意の VLAN を介 して行えます。
	cluster management-vlan <i>vlan-id</i> スイッチでクラスタが設定されている場合、このコマ	Catalyst 2960 スイッチでは、このコマンドは 拒否され、次のメッセージが表示されます。
	ンドで管理 VLAN と通信します。	Switch(config) # cluster management-vlan 2
		%Invalid input detected at `^' marker.
DHCP スヌーピング	Catalyst 2950 スイッチの DHCP スヌーピング機能 は、インターフェイスが受信できる 1 秒あたりの DHCP パケットの数を制限します。これを設定する	Cisco IOS 12.2SE では、指定できる範囲が 1 秒あたり 1 ~ 2048 メッセージに変わっていま す。
	には、次のインターフェイス コンフィギュレーショ ン コマンドを使用します。 ip dhcp snooping limit rate <i>rate</i> 指定できる範囲は 1 ~ 4294967294 です。デフォルト では制限は設定されていません。	Catalyst 2960 スイッチでは、どのような範囲 値も受け付けられます。ただし、値が 2048 を 超えている場合は、最大値の 2048 に変更さ れ、メッセージが表示されます。
		%Invalid input detected at `^' marker.%
フロー制御	Catalyst 2950 スイッチでは、ギガビット イーサネット インターフェイスでのポーズ フレームがサポート されています。これを設定するには、次のインター フェイス コンフィギュレーション コマンドを使用し ます。	Catalyst 2960 スイッチでは、受信したポーズ フレームを受け付けますが、送信はできませ ん。flowcontrol send コマンドは Catalyst 2960 スイッチではサポートされていません。
	flowcontrol send {desired off on}	Catalyst 2960 スイッチでは、このコマンドは 拒否され、次のメッセージが表示されます。
		Switch(config-if)# flowcontrol send desired
		%Invalid input detected at `^' marker.
		制御トラフィックに影響を与えずにデータト ラフィックを制限するため、Quality of Service (QoS; サービス品質)を設定できます。フロー 制御を行うと、すべてのトラフィックが停止し ます。詳細は、第 33 章「QoS の設定」を参照 してください。

表 C-1 Catalyst 2950 スイッチと Catalyst 2960 スイッチの設定の非互換項目

機能	Catalyst 2950 スイッチのコマンドと説明	Catalyst 2960 スイッチでの結果
IEEE 802.1x	Cisco IOS 12.1EA では、Catalyst 2950 スイッチの IEEE 802.1x server-timeout、supp-timeout、 tx-period の指定可能範囲は 1 ~ 65535 です。これを 設定するには、次のインターフェイス コンフィギュ	Cisco IOS 12.2SE では、IEEE 802.1x server-timeout および supp-timeout の指定可能 範囲は 30 ~ 65535 になっています。tx-period の指定可能範囲は 15 ~ 65535 です。
	レーション コマンドを使用します。 dot1x timeout server-timeout seconds dot1x timeout supp-timeout seconds dot1x timeout tx-period seconds	server-timeout については、Catalyst 2960 ス イッチは 1 ~ 29 の値も有効な値として受け付 け、30 に変更します。
		supp-timeout については、Catalyst 2960 ス イッチは 1 ~ 29 の値も有効な値として受け付 け、30 に変更します。
		tx-timeout については、Catalyst 2960 スイッ チは 1 ~ 14 の値も有効な値として受け付け、 15 に変更します。
		この3つのコマンドに対して、次のメッセージ が表示されます。
		%Invalid input detected at `^' marker.
IGMP ¹ スヌーピング	Catalyst 2950 スイッチでは、MAC(メディア アクセ ス制御)アドレスに基づいて IGMP スヌーピングを 実装します。スタティック グループを設定するには、 次のグローバル コンフィギュレーション コマンドを 使用します。	Catalyst 2960 スイッチでは、IP アドレスに基 づいて IGMP スヌーピングを実装し、より高 度なハードウェアを使用します。Catalyst 2950 の IGMP スヌーピング コマンドは拒否され、 次のメッセージが表示されます。
	ip igmp snooping vlan vlan-id static mac-address interface interface-id	Switch(config)# ip igmp snooping vlan 1 static 0002.4b28.c482 interface gigabitethernet0/1
	Catalyst 2950 スイッチでは、ハードウェアの制約に 対処するために、次のグローバル コンフィギュレー ション コマンドが実装されています。	<pre></pre>
	ip igmp snooping source-only-learning [age-timer <i>value</i>]	Switch(config)# ip igmp snooping source-only-learning
	no ip igmp snooping mrouter learn pim v2	<pre>%Invalid input detected at ``` marker. Switch(config)# no ip igmp snooping mrouter learn pim v2</pre>
インターフェイス MAC アドレス	Catalyst 2950 スイッチでは、次のインターフェイス コンフィギュレーション コマンドを使用して、物理 インターフェイスと Switch Virtual Interface (SVI;	Catalyst 2960 スイッチでは、物理インター フェイスおよび SVI に対して MAC アドレス を設定することはできません。
	スイッチ仮想インターフェイス)の両方に対して MACアドレスを設定できます。	Catalyst 2960 スイッチでは、このコマンドは 拒否され、次のメッセージが表示されます。
	mac-address mac-address	<pre>Switch(config-if)# mac-address 0100.0ccc.cccc</pre>

表 C-1 Catalyst 2950 スイッチと Catalyst 2960 スイッチの設定の非互換項目 (続き)

%Invalid input detected at `^' marker.

表 C-1 Catalyst 2950 スイッチと Catalyst 2960 スイッチの設定の非互換項目 (続き)

機能	Catalyst 2950 スイッチのコマンドと説明	Catalyst 2960 スイッチでの結果
QoS ²	 Catalyst 2950 スイッチと Catalyst 2960 スイッチでは、QoS 設定の互換性に制約があります。 Catalyst 2950 スイッチでは、auto qos voip {cisco-phone cisco-softphone trust} インターフェイス コンフィギュレーション コマンドを使用して、自動 QoS (auto-QoS) をイネーブル化することを推奨します。 Catalyst 2950 スイッチでカスタム QoS 設定を行っている場合、Catalyst 2960 スイッチへの移行のためにauto-QoS を使用することを推奨します。 (注) auto-QoS によってネットワークで必要な設定が得られない場合、Catalyst 2950 スイッチのOoS 設定を削除して、Catalyst 2960 スイッチ 	Catalyst 2960 スイッチは、auto qos コマンド を受け付けて、Catalyst 2960 スイッチに対応 した QoS コマンドを生成します。ポリサーの 粒度は 1 Mbps になります。 生成されるコマンドの詳細については、このリ リースに対応するコマンド リファレンスにあ る auto qos voip コマンドの項を参照してくだ さい。
	で新しく設定を作成することを推奨します。	C. 1 . 2050 7 . T. T. M. T. T. M. T. T. M. T. T. M. M. T. M. M. T. T. M. M. T. T. M. M. T. T. M. M. T. M. T. M. M. M. T. M. M. T. M. M. T. M.
	auto-QoS は Catalyst 2950 スイッナではイネーノル化 されませんが、その他の QoS コマンドは設定されま す。	Catalyst 2950 スイッチの次のコマントは、 Catalyst 2960 スイッチで実行すると、エラー になる場合があります。
		mls qos map dscp-cos グローバル コンフィ ギュレーション コマンド
		wrr-queue cos-map グローバル コンフィギュ レーション コマンド
		wrr-queue cos-bandwidth グローバル コン フィギュレーション コマンド
		mls qos trust cos pass-through dscp インター フェイス コンフィギュレーション コマンド
		police ポリシーマップ クラス コンフィギュ レーション コマンド
		次のメッセージが表示されることがあります。 ^
		%Invalid input detected at `^' marker.

機能	Catalyst 2950 スイッチのコマンドと説明	Catalyst 2960 スイッチでの結果
RSPAN ³	次のグローバル コンフィギュレーション コマンドを 使用して、ポートの1つをリフレクタ ポートとして 指定する必要があります。	Catalyst 2960 スイッチでは、ハードウェアの 改良に従い、リフレクタ ポートを設定する必 要がなくなっています。
	monitor session session_number destination remote vlan vlan-id reflector-port interface-id	Catalyst 2960 スイッチでは、monitor session session-number destination remote vlan vlan-id reflector-port interface-id コマンドが 受け付けられ、次のメッセージが表示されま す。 Note: Reflector port configuration is not required on this platform, ignoring the reflector port configuration
STP	Catalyst 2950 スイッチでは、GBIC ⁴ インターフェイ スのクロススタック UplinkFast がサポートされてい ます。次のインターフェイス コンフィギュレーショ ン コマンドを使用して、スタック ポートをイネーブ ル化します。 spanning-tree stack-port	Catalyst 2960 スイッチでは、GBIC インター フェイスがサポートされていません。 Catalyst 2960 スイッチでは、このコマンドは 拒否され、次のメッセージが表示されます。 Switch(config-if)# spanning-tree stack-port ^ %Invalid input detected at `^' marker.

表 C-1 Catalyst 2950 スイッチと Catalyst 2960 スイッチの設定の非互換項目 (続き)

1. IGMP = Internet Group Management Protocol

2. QoS = Quality of Service

3. RSPAN = Remote Switched Port Analyzer

4. GBIC = Gigabit Interface Converter

機能的な動作の非互換項目

Catalyst 2950 スイッチと Catalyst 2960 スイッチでは、一部の機能の動作が異なり、Catalyst 2960 ス イッチではサポートされていない機能もあります。

• Access Control List (ACL; アクセス制御リスト)

Catalyst 2950 スイッチと Catalyst 2960 スイッチでコマンドの構文は同じですが、IP と MAC ACL のセマンティックは異なります。たとえば、Catalyst 2950 スイッチでは IP パケットに対して MAC ACL を適用できますが、Catalyst 2960 スイッチでは次のようになります。

- IP パケットに MAC ACL を適用できません。
- IPv6 フレームのために ACL を適用できません。
- MAC ACL については、Appletalk の Ethertype はサポートされていません。
- QoS

Catalyst 2950 スイッチと Catalyst 2960 スイッチでは使用するポート ハードウェアが異なり、 Catalyst 2960 スイッチで利用できる QoS 機能は豊富になっています。たとえば、Catalyst 2950 ス イッチでサポートされているのが WRR スケジューリングであるのに対し、Catalyst 2960 スイッ チでは SRR スケジューリングがサポートされています。また、Catalyst 2950 スイッチでは QoS がデフォルトでイネーブル化されているのに対し、Catalyst 2960 スイッチでは QoS をグローバル にイネーブル化する必要があります。詳細は、第 33 章「QoS の設定」を参照してください。

RSPAN

Catalyst 2950 スイッチでは、RSPAN 実装のために、リフレクタ ポートという特別なポートを使用します。このポートは、Catalyst 2960 スイッチの RSPAN 実装では不要です。Catalyst 2960 ス イッチでは、SPAN 送信元として VLAN もサポートしており、SPAN 宛先ポートで受信したパ ケットを転送できます。

• マルチキャスト

Catalyst 2960 スイッチのマルチキャスト転送の決定は、IP アドレスに基づいて行われます。プ ラットフォームの制約に対処するため、次善の策として Catalyst 2950 スイッチで取られていた手 段(ip igmp snooping source-only-learning グローバル コンフィギュレーション コマンドなど) は、Catalyst 2960 スイッチでは不要となっています。





Cisco IOS Release 12.2(52)SE でサポート されていないコマンド

この付録では、Catalyst 2960 スイッチのプロンプトに疑問符(?)を入力したときに表示される Command-Line Lnterface(CLI; コマンドラインインターフェイス)コマンドの中で、まだテストが済 んでいないため、または Catalyst スイッチのハードウェアの制限により、このリリースでサポートさ れていないコマンドを示します。このリストは完全ではありません。これらのサポートされていないコ マンドは、ソフトウェア機能およびコマンド モード別に掲載されています。

- 「アクセス コントロール リスト」(P.D-2)
- 「ブートローダ コマンド」(P.D-2)
- $\lceil \text{debug} = \forall \forall \forall \downarrow (P.D-3) \rangle$
- 「IGMP スヌーピング コマンド」(P.D-3)
- 「インターフェイス コマンド」(P.D-3)
- 「MAC アドレス コマンド」 (P.D-4)
- 「その他」 (P.D-4)
- 「NAT コマンド」 (P.D-5)
- $\lceil QoS \rfloor$ (P.D-5)
- 「RADIUS」 (P.D-6)
- **SNMP** (P.D-6)
- 「SNMPv3」 (P.D-6)
- 「スパニングツリー」(P.D-7)
- 「VLAN」 (P.D-7)
- 「VTP」 (P.D-8)

アクセス コントロール リスト

アクセス コントロール リスト

サポートされていない特権 EXEC コマンド

access-enable [host] [timeout minutes] access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes] clear access-template [access-list-number | name] [dynamic-name] [source] [destination] show access-lists rate-limit [destination] show accounting show ip accounting [checkpoint] [output-packets | access violations] show ip cache [prefix-mask] [type number]

サポートされていないグローバル コンフィギュレーション コマンド

access-list rate-limit *acl-index* {*precedence* | mask *prec-mask*} access-list dynamic extended

サポートされていないルートマップ コンフィギュレーション コマンド

match ip address prefix-list prefix-list-name [prefix-list-name...]

ブート ローダ コマンド

サポートされていないグローバル コンフィギュレーション コマンド

boot buffersize

debug コマンド

サポートされていない特権 EXEC コマンド

debug platform cli-redirection main debug platform configuration

IGMP スヌーピング コマンド

サポートされていないグローバル コンフィギュレーション コマンド

ip igmp snooping tcn

インターフェイス コマンド

サポートされていない特権 EXEC コマンド

show interfaces [*interface-id* | vlan *vlan-id*] [crb | fair-queue | irb | mac-accounting | precedence | irb | random-detect | rate-limit | shape]

サポートされていないグローバル コンフィギュレーション コマンド

interface tunnel

サポートされていないインターフェイス コンフィギュレーション コマンド

transmit-interface type number

MAC アドレス コマンド

サポートされていない特権 EXEC コマンド

show mac-address-table show mac-address-table address show mac-address-table aging-time show mac-address-table count show mac-address-table dynamic show mac-address-table interface show mac-address-table multicast show mac-address-table notification show mac-address-table static show mac-address-table static show mac-address-table vlan

(注)

VLAN(仮想 LAN)のレイヤ 2 マルチキャスト アドレス テーブル エントリを表示するには、 show ip igmp snooping groups 特権 EXEC コマンドを使用します。

サポートされていないグローバル コンフィギュレーション コマンド

mac-address-table aging-time mac-address-table notification mac-address-table static

その他

サポートされていないユーザ EXEC コマンド

verify

サポートされていない特権 EXEC コマンド

file verify auto show cable-diagnostics prbs test cable-diagnostics prbs

サポートされていないグローバル コンフィギュレーション コマンド

errdisable recovery cause unicast flood l2protocol-tunnel global drop-threshold memory reserve critical service compress-config stack-mac persistent timer

NAT コマンド

サポートされていない特権 EXEC コマンド

show ip nat statistics show ip nat translations

QoS

サポートされていないグローバル コンフィギュレーション コマンド

priority-list

サポートされていないインターフェイス コンフィギュレーション コマンド

priority-group rate-limit

サポートされていないポリシーマップ コンフィギュレーション コマンド

class-default が class-map-name である場合の class class-default

RADIUS

サポートされていないグローバル コンフィギュレーション コマンド

aaa nas port extended

- aaa authentication feature default enable
- aaa authentication feature default line

aaa nas port extended

authentication command bounce-port ignore(LAN Lite イメージが稼動しているスイッチに限る) **authentication command disable-port ignore**(LAN Lite イメージが稼動しているスイッチに限る)

- radius-server attribute nas-port
- radius-server configure
- radius-server extended-portnames

SNMP

サポートされていないグローバル コンフィギュレーション コマンド

no monitor session all (LAN Lite イメージが稼動しているスイッチに限る) snmp-server enable informs snmp-server enable traps hsrp snmp-server enable traps rtr (LAN Lite イメージが稼動しているスイッチに限る) snmp-server ifindex persist

SNMPv3

サポートされていない 3DES 暗号化コマンド

すべて

スパニングツリー

サポートされていないグローバル コンフィギュレーション コマンド

spanning-tree pathcost method {long | short}

サポートされていないインターフェイス コンフィギュレーション コマンド

spanning-tree stack-port

VLAN

サポートされていないグローバル コンフィギュレーション コマンド

vlan internal allocation policy {ascending | descending}

サポートされていない vlan-config コマンド

private-vlan

サポートされていないユーザ EXEC コマンド

show running-config vlan show vlan ifindex vlan database

サポートされていない vlan-config コマンド

private-vlan

サポートされていない VLAN データベース コマンド

vtp

vlan

show vlan private-vlan

VTP

サポートされていない特権 EXEC コマンド

vtp {password password | pruning | version number}



VTP



数字

802.1x ユーザ ディストリビューションの設定 9-58

Α

access-class コマンド 31-38 ACE IP **31-22** QoS **33-8** イーサネット 31-22 定義 31-22 ACL ACE **31-22** any キーワード 31-31 host キーワード 31-31 IP 暗示のマスク 31-28 暗黙の拒否 31-28, 31-33, 31-34 一致条件 31-26 作成 31-26 フラグメントおよび QoS の注意事項 33-33 未定義 31-39 IPv4 一致条件 31-26 インターフェイスへの適用 31-38 作成 31-26 サポートされていない機能 31-25 端末回線、設定 31-37 名前付き 31-33 番号 31-26 MAC 拡張 31-43, 33-45 QoS 33-8, 33-43

ΙΝΟΕΧ

QoS のためのトラフィックの分類 33-43 31-26, 31-39 一致 エントリの並べ替え 31-33 拡張 IP、OoS 分類のための設定 33-44 拡張 IPv4 一致条件 31-26 作成 31-29 クラス マップごとの数 33-33 コメント 31-37 コンパイル 31-41 サポート 1-10 サポートされていない機能、IPv4 31-25 時間範囲 31-35 定義 31-22, 31-26 適用 QoS ~ **33-8** インターフェイスへの 31-38 時間範囲 31-35 名前付き、IPv4 **31-33** ハードウェアおよびソフトウェアの処理 31-39 ハードウェアでのサポート 31-39 標準 IP、QoS 分類のための設定 33-43 標準 IPv4 一致条件 31-26 作成 31-27 31-46 モニタ 31-41, 33-43 例 ACL エントリの並べ替え 31-33 ACL での時間範囲 31-35 ACL の IP プロトコル 31-30 AC(コマンド スイッチ) 5-11 Address Resolution Protocol 「ARP」を参照

ARP

定義 1-6, 6-34 テーブ アドレスの解決 6-34 6-34 管理 Auto-MDIX 設定 11-23 説明 11-23 Auto SmartPort マクロ Cisco Medianet 12-3 IOS シェル 12-2, 12-16 LLDP 12-2 イネーブル化 12-6, 12-9 イベント トリガー 12-13 組み込みマクロ 12-4, 12-10 設定時の注意事項 12-5 定義 12-2 デフォルト設定 12-4 表示 12-21 マッピング 12-10 ユーザ定義マクロ 12-16 「Smartport マクロ」も参照

В

BackboneFast

```
イネーブル化
               18-16
  サポート
          1-8
  説明
        18-6
  ディセーブル化
                18-16
Berkeley r-tools 交換
                 8-54
BPDU
  errdisable ステート
                   18-3
  RSTP フォーマット
                   17-13
  フィルタリング
               18-3
BPDU ガード
  イネーブル化
               18-12
  サポート
            1-8
  説明
         18-3
```

```
ディセーブル化 18-13
BPDU フィルタリング
イネーブル化 18-14
サポート 1-8
説明 18-3
ディセーブル化 18-14
Bridge Protocol Data Unit
「BPDU」を参照
broadcast storm-control コマンド 23-4
```

С

Catalyst 2950 スイッチのアップグレード 機能的な動作の非互換項目 C-6 互換性のないコマンド メッセージ C-1 コンフィギュレーション コマンドでの相違 C-1 推奨 C-1 設定の互換性の問題 C-1 Catalyst 6000 スイッチ 認証の互換性 9-9 Catalyst 6000 スイッチとの認証の互換性 9-9 CA の信頼点 設定 8-50 定義 8-47 CDP イネーブル化およびディセーブル化 インターフェイス 25-4 25-3 スイッチ 概要 25-1 更新 25-2 サポート 1-6 信頼境界 33-39 スイッチ クラスタの自動検出 5-5 設定 25-2 説明 25-1 送信タイマーおよびホールドタイム、設定 25-2 定義、LLDP を使用 26-2 デフォルト設定 25-2 電力ネゴシエーションの拡張 11-5

モニタ 25-5 ルーティング デバイスでディセーブル 25-3 ~ 25-4 化 CGMP IGMP スヌーピング学習方式として 22-9 マルチキャスト グループへの加入 22-3 CipherSuites 8-48 Cisco 32-1 Cisco 7960 IP Phone 15-1 Cisco Discovery Protocol 「CDP」を参照 Cisco Intelligent Power Management 11-5 Cisco IOS IP Service Level Agreements (SLA) responder 1-4 Cisco IOS IP SLA 32-2 Cisco IOS ファイル システム 「IFS」を参照 Cisco Medianet 「Auto SmartPort マクロ」を参照 Cisco Secure ACS ダウンロード可能 ACL のアトリビュート値ペ P 9-21 リダイレクト URL のアトリビュート値ペア 9-20 Cisco Secure ACS 設定時の注意事項 9-63 CiscoWorks 2000 1-5, 30-5 CISP 9-31 CIST リージョナル ルート 「MSTP」を参照 CIST ルート 「MSTP」を参照 Class of Service 「CoS」を参照 CLI エラー メッセージ 2-5 クラスタの管理 5-16 コマンド出力のフィルタリング 2-10 コマンドの no 形式および default 形式 2-4 コマンドの省略 2-4 コマンドモード 2-1 コンフィギュレーション ロギング 2-5

説明 1-5 ヘルプについて 2-3 編集機能 イネーブル化およびディセーブル化 2-7 キーストローク編集 2-7 ラップアラウンド機能で折り返された行 2-9 履歴 コマンドの呼び出し 2-6 説明 2-6 ディセーブル化 2-7 バッファ サイズの変更 2-6 **Client Information Signalling Protocol** 「CISP」を参照 CNS 1-5 **Configuration Engine** ConfigID、DeviceID、ホスト名 4-3 イベント サービス 4-3 コンフィギュレーション サービス 4-2 説明 4-1 管理機能 1-5 組み込み型エージェント イベント エージェントのイネーブル化 4-7 コンフィギュレーション エージェントのイネーブ ル化 4-9 自動設定のイネーブル化 4-7 説明 4-5 Coarse Wave Division Multiplexer 「CWDM SFP」を参照 CoA 要求コマンド 8-25 config.text 3-18 configure terminal $\neg \neg \checkmark ee$ 11-11 config-vlan モード 2-2 CoS プライオリティの上書き 15-7 プライオリティを信頼する 15-7 レイヤ2フレーム 33-2 CPU 使用率、トラブルシューティング 37-25 crashinfo ファイル 37-24 CWDM SFP 1-24

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

D

DACL 「ダウンロード可能 ACL」を参照 default コマンド 2-4 description コマンド 11-29 DHCP **20-15** Cisco IOS サーバ データベース 設定 20-13 イネーブル化 リレー エージェント 20-11 **DHCP** Option 82 回線 ID サブオプション 20-6 概要 20-4 設定時の注意事項 20-9 デフォルト設定 20-9 パケット形式、サブオプション 回線 ID 20-6 リモート ID 20-6 表示 20-15 リモート ID サブオプション 20-6 DHCP サーバ ポートベースのアドレス割り当て イネーブル化 20-25 サポート 1-5 設定時の注意事項 20-25 説明 20-24 デフォルト設定 20-25 20-28 表示 予約されたアドレス 20-26 DHCP スヌーピング Option 82 データ挿入 20-4 エッジ スイッチから信頼できないパケットを受 20-4, 20-12 信 信頼できないインターフェイス 20-3 信頼できないメッセージ 20-3 信頼できるインターフェイス 20-3 設定時の注意事項 20-9 デフォルト設定 20-9 バインディング データベース

「DHCP スヌーピング バインディング データベー ス」を参照 バインディング テーブルの表示 20-15 メッセージ交換プロセス 20-5 DHCP スヌーピング バインディング データベース イネーブル化 20-13 エージェントに関する統計情報をクリア 20-14 エントリ 20-7 削除 データベース エージェント 20-14 バインディング 20-14 バインディング ファイル 20-14 ステータスおよび統計情報の表示 20-15 20-13 設定 設定時の注意事項 20-10 説明 20-7 データベースの更新 20-14 デフォルト設定 20-9 バインディング 20-7 バインディング エントリ、表示 20-15 バインディングの追加 20-13 バインディング ファイル 形式 20-8 ロケーション 20-7 表示 20-15 リセット タイムアウトの値 20-14 遅延時間の値 20-14 DHCP スヌーピング バインディング テーブル 「DHCP スヌーピング バインディング データベース」 を参照 DHCP バインディング データベース 「DHCP スヌーピング バインディング データベース」 を参照 DHCP バインディング テーブル 「DHCP スヌーピング バインディング データベース」 を参照 DHCP プールの予約されたアドレス 20-26 DHCP ベースの自動設定 BOOTP との関係 3-4

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

概要 3-4 クライアントのメッセージ交換要求 3-4 サポート 1-5 設定 DNS **3-8** TFTP サーバ 3-8 クライアント側 3-4 サーバ側 3-7 リレー デバイス 3-9 リース オプション IP アドレス情報 3-7 コンフィギュレーションファイルの受信 3-7 リレー サポート 1-5 例 3-11 DHCP ベースの自動設定およびイメージ アップデート 概要 3-5 ~ 3-6 設定 3-12 ~ 3-16 Differentiated Services Code Point 33-2 Differentiated Services アーキテクチャ、QoS 33-2 DNS DHCP ベースの自動設定 3-8 IPv6 34-4 概要 6-17 サポート 1-5 6-18 設定 設定の表示 6-19 デフォルト設定 6-17 Domain Name System 「DNS」を参照 DoS 攻撃 23-1 DRP サポート 1-15 DSCP 1-13, 33-2 DSCP 透過 33-40 DTP 1-9, 13-14 dynamic auto トランキング モード 13-15 dynamic desirable トランキング モード 13-15 **Dynamic Host Configuration Protocol** 「DHCP ベースの自動設定」を参照

Dynamic Trunking Protocol 「DTP」を参照

Ε

ELIN ロケーション 26-4 errdisable ステート、BPDU 18-3 EtherChannel IEEE 802.3ad、説明 36-6 LACP システム プライオリティ 36-16 ステータスの表示 36-18 説明 36-6 他の機能との相互作用 36-6 ポート プライオリティ 36-17 ホット スタンバイ ポート 36-16 モード 36-6 PAgP Catalyst 1900 との互換性 36-14 学習方式およびプライオリティの設定 36-14 仮想スイッチとの相互交流 36-5 サポート 1-3 集約ポート ラーナー 36-14 ステータスの表示 36-18 説明 36-4 他の機能との相互作用 36-5 デュアルアクティブ検出 36-5 モード 36-4 サポート 1-3 自動作成 36-4, 36-6 ステータスの表示 36-18 設定時の注意事項 36-10 説明 36-2 相互作用 STP 36-10 VLAN 36-10 チャネル グループ 数 36-3

物理インターフェイスと論理インターフェイスの バインディング 36-3 デフォルト設定 36-9 転送方式 36-7, 36-13 ポート グループ 11-4 ポートチャネル インターフェイス 36-3 数 説明 36-3 レイヤ2インターフェイスの設定 36-11 ロードバランシング 36-7, 36-13 EtherChannel ガード イネーブル化 18-16 説明 18-8 ディセーブル化 18-17 EUI **34-3** Express Setup 1-2 『Getting Started Guide』も参照 Extended Universal Identifier 「EUI」を参照 Extensible Authentication Protocol over LAN 9-1

F

```
fa0 インターフェイス
                  1-6
Flex Link
  Link ロード バランシング
                        19-3
  VLAN 19-3
  VLAN ロード バランシングの設定
                              19-12
  設定
         19-10, 19-11
  設定時の注意事項
                  19-9
  説明
         19-2
  デフォルト設定
                 19-9
  モニタ
          19-16
  優先 VLAN の設定
                   19-13
Flex Link の VLAN ロード バランシング
                               19-3
   設定時の注意事項
                  19-9
Flex Link マルチキャスト高速コンバージェンス
                                    19-3
flowcontrol
   設定
         11-22
```

```
説明 11-22
```

FTP

```
MIB ファイルにアクセス
                  A-3
イメージ ファイル
  アップロード
             B-37
  サーバの準備
             B-34
  ダウンロード
             B-35
  古いイメージの削除
                 B-37
コンフィギュレーション ファイル
  アップロード
             B-18
  概要
        B-15
  サーバの準備
             B-16
  ダウンロード
             B-16
```

G

get-bulk-request 動作 30-3 get-next-request 動作 30-3, 30-5 get-request 動作 30-3, 30-5 get-response 動作 30-3 GUI 「デバイス マネージャ」および「Network Assistant」 を参照

Η

```
Hello タイム

MSTP 17-24

STP 16-22

HP OpenView 1-5

HSRP

クラスタ スタンバイ グループに関する考慮事

項 5-12

クラスタの自動復旧 5-13

「クラスタ」、「クラスタ スタンバイ グループ」および

「スタンバイ コマンド スイッチ」も参照

HTTP over SSL

「HTTPS」を参照
```

```
HTTPS 8-47
```

自己署名証明書 **8-47** 設定 **8-51**

I

ICMP IPv6 **34-4** time-exceeded メッセージ 37-18 traceroute 37-18 ICMP ping 概要 37-15 37-15 実行 ICMPv6 34-4 IDS 装置 入力 RSPAN 27-21 入力 SPAN 27-14 IEEE 802.1D 「STP」を参照 IEEE 802.1p 15-1 IEEE 802.1Q カプセル化 13-14 設定時の制限事項 13-15 タグなしトラフィック用ネイティブ VLAN 13-20 トンネル ポート **11-3** IEEE 802.1s 「MSTP」を参照 IEEE 802.1w 「RSTP」を参照 IEEE 802.1x 「ポートベース認証」を参照 IEEE 802.3ad 「EtherChannel」を参照 IEEE 802.3af 「**PoE」**を参照 IEEE 802.3x フロー制御 11-22 ifIndex 值、SNMP **30-6** IFS 1-6 IGMP join メッセージ 22-3

クエリー 22-4 サポート 1-4 サポートされているバージョン 22-3 脱退タイマーの設定 イネーブル化 22-12 説明 22-6 脱退プロセス、イネーブル化 22-11, 35-10 フラッディングしたマルチキャスト トラフィック クエリー送信要求 22-14 グローバル Leave 22-14 時間の制御 22-13 ディセーブル化、インターフェイス上 22-14 フラッディング モードからの回復 22-14 マルチキャスト グループからの脱退 22-5 マルチキャスト グループへの加入 22-3 レポート抑制 説明 22-6 ディセーブル化 22-17, 35-12 IGMP グループ 最大数の設定 22-30 フィルタリングの設定 22-31 IGMP スヌーピング VLAN コンフィギュレーション 22-8 アドレスエイリアス 22-2 イネーブル化およびディセーブル化 22-8, 35-7 クエリア 設定 22-15 設定時の注意事項 22-15 グローバル コンフィギュレーション 22-8 サポート 1-4 サポートされているバージョン 22-3 設定 22-7 即時脱退 22-6 定義 22-2 デフォルト設定 22-7, 35-6 方法 22-9 モニタ 22-18, 35-13 IGMP スロットリング アクションの表示 22-32

22-31 設定 説明 22-27 デフォルト設定 22-28 IGMP 即時脱退 イネーブル化 22-11 設定時の注意事項 22-12 説明 22-6 IGMP フィルタリング サポート 1-4 設定 22-28 説明 22-27 デフォルト設定 22-28 モニタ 22-32 IGMP プロファイル コンフィギュレーション モード 22-28 設定 22-28 適用 22-29 IGMP レポートの生成 19-4 IGMP レポートのリーク 19-4 interfaces range macro $\neg \neg \checkmark \lor$ 11-14 interface コマンド 11-11 Intrusion Detection System 「IDS 装置」を参照 IOS シェル 「Auto SmartPort マクロ」を参照 IP 5-3, 5-12 IP ACL OoS 分類のため 33-8 暗示のマスク 31-28 暗黙の拒否 31-28, 31-33 名前付き 31-33 未定義 31-39 ip igmp profile $\neg \neg \checkmark \lor$ 22-28 **IP** Phone QoS 15-1 **OoS** の信頼境界 33-39 OoS を使用してポートセキュリティを確保 自動分類およびキューイング 33-20 設定 15-5

```
IP precedence 33-2
IP Service Level Agreement
   「IP SLA」を参照
IP SLA
  responder
     イネーブル化
                  32-6
     説明
            32-4
  SNMP サポート
                 32-2
  応答時間
            32-4
   コントロール プロトコル
                      32-4
  サポートされているメトリック
                          32-2
  設定時の注意事項
                  32-5
  定義
         32-1
  デフォルト設定
                32-5
  動作
         32-3
  ネットワーク パフォーマンスの測定
                              32-3
  モニタ
          32-7
  利点
         32-2
IP traceroute
   概要
         37-18
  実行
         37-19
IPv4 ACL
  インターフェイスへの適用
                        31-38
  拡張、作成
             31-29
  名前付き
            31-33
  標準、作成
             31-27
IPv4 および IPv6
  デュアル プロトコル スタック
                          34-5
IPv6
  ICMP 34-4
  SDM テンプレート
                   35-1
  アドレス
            34-2
  アドレスの割り当て
                   34-8
   アドレス フォーマット
                     34-2
   アプリケーション
                  34-4
  近接ディスカバリ
                  34-4
  サポートされている機能
                      34-3
   自動設定
            34-4
   スタティック ルートの概要
                        34-6
```

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

33-39

スタティック ルートの設定 34-11 ステートレス自動設定 34-4 34-2 定義 デフォルト設定 34-7 34-8 転送 モニタ 34-13 IPv6 による SNMP および Syslog 34-6 IPアドレス 128 ビット 34-2 IPv6 **34-2** クラスタ アクセス 5-2 検出 6-34 候補またはメンバー 5-4, 5-14 コマンド スイッチ 5-3, 5-12, 5-14 冗長クラスタ 5-12 スタンバイ コマンド スイッチ 5-12, 5-14 「IP 情報」も参照 IP サービス レベル、分析 32-1 IP 情報 デフォルト設定 3-3 割り当て DHCP ベースの自動設定を使用 3-4 手動で 3-16 IP 送信元ガード 802.1x **20-18** DHCP スヌーピング 20-15 EtherChannel **20-18** TCAM エントリ 20-18 VRF **20-18** イネーブル化 20-19, 20-20 スタティック バインディング 削除 20-19 追加 20-19, 20-20 設定時の注意事項 20-18 説明 20-15 送信元 IP アドレスのフィルタリング 20-16 送信元 IP と MAC アドレスのフィルタリン 20-16 グ ディセーブル化 20-19

デフォルト設定 20-18 トランク インターフェイス 20-18 バインディング テーブル 20-15 バインディングの設定 自動 20-15 主導 20-15 表示 設定 20-24 バインディング 20-24 フィルタリング 送信元 IP アドレス 20-16 送信元 IP と MAC アドレス 20-16 プライベート VLAN 20-18 ポート セキュリティ 20-18 ルーテッド ポート 20-18 IP ソース ガード スタティック ホスト 20-20 表示 アクティブな IP または MAC バインディン 20-24 ゲ

J

join メッセージ、IGMP 22-3

L

LACP 「EtherChannel」を参照 LDAP 4-2 LED、スイッチ 『Hardware Installation Guide』を参照 Lightweight Directory Access Protocol 「LDAP」を参照 Link Aggregation Control Protocol 「EtherChannel」を参照 Link Layer Discovery Protocol 「CDP」を参照 LLDP

Catalyst 2960 スイッチ ソフトウェア コンフィギュレーション ガイド

イネーブル化 26-7 概要 26-2 サポートされている TLV 26-2 スイッチ スタックに関する考慮事項 26-2 設定 26-5 デフォルト設定 26-6 特性 26-8 送信タイマーおよびホールドタイム、設定 26-8 モニタおよびメンテナンス 26-13 LLDP-MED 概要 26-2, 26-3 サポートされている TLV 26-3 設定 TLV 26-9 手順 26-5 モニタおよびメンテナンス 26-13 LLDP Media Endpoint Discovery 「LLDP-MED」を参照 Long-Reach Ethernet (LRE) テクノロジー 1-20 LRE プロファイル、スイッチ クラスタに関する考慮事 項 5-16 Μ MAB 「認証バイパス」を参照 MAB 非アクティブ タイマー デフォルト設定 9-35 範囲 9-37 MAC/PHY コンフィギュレーション / ステータス TLV 26-2 MACアドレス ACL 31-43

IP 送信元のバインディングテーブルに表示 20-24
 VLAN アソシエーション 6-23
 VLAN での学習のディセーブル化 6-33
 アドレステーブルの作成 6-23
 エージングタイム 6-24
 検出 6-34

スタティック 許可 6-32, 6-33 削除 6-30 追加 6-30 6-30 特性 破棄 6-31 ダイナミック 削除 6-24 ラーニング 6-23 デフォルト設定 6-23 表示 6-33 MAC アドレス学習 1-6 MAC アドレス学習、VLAN 上でディセーブル化 6-33 MAC アドレス通知、サポート 1-15 MAC アドレス テーブル移動更新 設定 19-14 設定時の注意事項 19-9 説明 19-7 デフォルト設定 19-9 モニタ 19-16 MAC アドレスと VLAN のマッピング 13-25 MAC 拡張アクセス リスト OoS のための設定 33-45 OoS 分類のため 33-5 作成 31-43 定義 31-43 レイヤ2インターフェイスへの適用 31-45 MAC 認証バイパス 9-37 概要 9-17 設定 9-58 MDA 設定時の注意事項 9-13 ~ 9-14 説明 1-11, 9-13 例外、認証プロセス 9-6 Medianet 「Auto SmartPort マクロ」を参照 MIB SNMP と相互作用 30-5

概要 30-1
サポートされている A-1 ファイルにアクセス、FTP を使用 A-3 ファイルの場所 A-3 mrouter ポート 19-4, 19-5 MSTP BPDU ガード イネーブル化 18-12 説明 18-3 BPDU フィルタリング イネーブル化 18-14 18-3 説明 CIST、説明 17-3 CIST リージョナル ルート 17-3, 17-5 CIST ルート 17-5 CST 定義 17-3 リージョン間の動作 17-4 EtherChannel $\mathcal{I} - \mathcal{K}$ イネーブル化 18-16 説明 18-8 IEEE 802.1D との相互運用性 移行プロセスの再起動 17-27 説明 17-9 IEEE 802.1s 実装 17-7 ポートの役割名の変更 17-7 用語 17-5 IST 定義 17-2 マスター 17-3 リージョン内の動作 17-3 MST リージョン CIST 17-3 IST 17-2 サポートされるスパニング ツリー インスタン 17-2 ス 設定 17-16 説明 17-2 ホップ カウント メカニズム 17-6

PortFast イネーブル化 18-11 説明 18-2 PortFast 対応ポートのシャットダウン 18-3 VLAN を MST インスタンスにマッピング 17-17 インターフェイス ステート、ブロッキングからフォ ワーディングへ 18-2 概要 17-2 拡張システム ID セカンダリ ルート スイッチでの影響 17-20 予期しない動作 17-18 ルート スイッチでの影響 17-18 境界ポート 設定時の注意事項 17-16 説明 17-6 サポートされているインスタンス 16-11 サポートされているオプション機能 1-8 ステータスの表示 17-28 ステータス、表示 17-28 設定 Hello タイム 17-24 MST リージョン 17-16 高速コンバージェンスのリンク タイプ 17-26 最大エージング タイム 17-25 最大ホップ カウント 17-25 スイッチ プライオリティ 17-23 セカンダリ ルート スイッチ 17-20 転送遅延時間 17-24 ネイバ タイプ 17-27 パス コスト 17-22 ポート プライオリティ 17-21 ルート スイッチ 17-18 設定時の注意事項 17-16, 18-11 デフォルト設定 17-15 デフォルトのオプション機能の設定 18-11 モード間の相互運用性と下位互換性 16-12 モードのイネーブル化 17-16 ルート ガード イネーブル化 18-17

説明 18-8 ルート スイッチ 拡張システム ID の影響 17-18 設定 17-18 予期しない動作 17-18 ルート スイッチの選択の防止 18-8 ループ ガード イネーブル化 18-18 説明 18-10 multiauth アクセス不能認証バイパスのサポート 9-24 multiauth モード 「複数認証モード」を参照 multicast storm-control コマンド 23-4 Multicast VLAN Registration 「MVR」を参照 MVR IGMPv3 22-23 アドレス エイリアス 22-23 アプリケーションの例 22-20 インターフェイスの設定 22-25 グローバル パラメータの設定 22-23 サポート 1-4 設定時の注意事項 22-23 説明 22-19 デフォルト設定 22-22 マルチキャスト TV アプリケーション 22-20 モード 22-24 モニタ 22-26

Ν

NAC

RADIUS サーバを使用する IEEE 802.1x 検証 9-60
RADIUS サーバを使用する IEEE 802.1x 認証 9-60
アクセス不能認証バイパス 9-55
クリティカル認証 9-24, 9-55
レイヤ 2 IEEE 802.1x 検証 1-12, 9-29, 9-60
NameSpace Mapper

「NSM」を参照 NEAT 概要 9-31 設定 9-61 Network Admission Control 「NAC」を参照 Network Assistant イメージ ファイルのダウンロード 1-2 ウィザード **1-2** ガイド モード 1-2 管理オプション 1-2 スイッチのアップグレード **B-28** 説明 1-5 利点 1-2 Network Edge Access Topology 「NEAT」を参照 Network Time Protocol 「NTP」を参照 no コマンド 2-4 NSM 4-3 NTP アクセスの制限 アクセス グループの作成 6-9 インターフェイス単位での NTP サービスのディ セーブル化 6-10 アソシエーション サーバ 6-6 定義 6-2 認証 6-5 ピア 6-6 ブロードキャスト メッセージのイネーブル 6-7 化 概要 6-2 サポート 1-6 ストラタム 6-2 設定の表示 6-11 送信元 IP アドレス、設定 6-11 タイム サービス 6-2

同期化 6-2デバイスの同期化 6-6デフォルト設定 6-4

0

Open1x 設定 9-66 Open1x 認証 概要 9-30

Ρ

PAgP 「EtherChannel」を参照 PC(パッシブ コマンド スイッチ) 5-11 Per-VLAN Spanning-Tree Plus 「PVST+」を参照 PIM-DVMRP、スヌーピング方法として 22-9 ping 概要 37-15 実行 37-15 文字出力の説明 37-16 PoE auto モード 11-7 CDP、電力消費、説明 11-5 CDP、電力ネゴシエーション、説明 11-5 CDP における電力ネゴシエーションの拡張 11-5 Cisco Intelligent Power Management 11-5 IEEE 電源分類レベル 11-6 カットオフ電力 サポート 11-8 判別 11-9 サポートされているデバイス 11-5 サポートされている標準 11-5 受電装置検出および初期電力割り当て 11-6 使用可能な総電力 11-9 消費電力のポリシング 11-8, 11-28 スタティック モード 11-7

```
設定
        11-24
  低電力モードで動作する高電力デバイス
                               11-5
  電源管理モード
               11-7
  電源予算
           11-26
  電力検知
           11-8
  電力消費
           11-9, 11-26
  電力モニタリング
                 11-8, 11-28
  トラブルシューティング
                     37-13
  モニタ
         11-8
PortFast
  イネーブル化
             18-11
  サポート 1-8
        18-2
  説明
  モード、スパニング ツリー
                       13-26
Power over Ethernet
  「PoE」を参照
PVST+
  IEEE 802.1Q トランキングの相互運用性
                               16-12
  サポートされているインスタンス
                           16-11
  説明
        16-10
```

Q

```
OoS
  DSCP 透過
             33-40
  IP Phone
     検出および信頼設定
                     33-20, 33-39
     自動分類およびキューイング
                           33-20
  MQC コマンド
               33-1
  QoS ラベル、定義
                  33-4
  暗黙の拒否
             33-8
  概要
         33-2
  書き換える
             33-20
  基本モデル
             33-4
  キュー
     SRR、説明
                33-14
     WTD、説明
                33-13
     特性の設定、出力
                    33-67
     特性の設定、入力
                    33-62
```

ハイ プライオリティ (緊急) 33-19, 33-73 場所 33-13 クラス マップ 設定 33-47 表示 33-75 グローバルなイネーブル化 33-35 サポート 1-13 自動 QoS イネーブル化、VoIP 用 33-27 実行コンフィギュレーションでの影響 33-26 出力キューのデフォルト 33-21 初期設定の表示 33-30 生成コマンドの一覧 33-22 生成コマンドの表示 33-27 設定時の注意事項 33-26 設定とデフォルトの表示 33-30 設定例 33-28 説明 33-20 ディセーブル化 33-27 トラフィックの分類 33-21 入力キューのデフォルト 33-21 出力インターフェイスの帯域幅の制限 33-74 出力キュー DSCP または CoS 値のマッピング 33-70 SRR 共有重みの設定 33-72 SRR シェーピング重みの設定 33-71 WTD しきい値の設定 33-68 WTD、説明 33-19 しきい値マップの表示 33-70 スケジューリング、説明 33-4 説明 33-4 バッファ スペースの割り当て 33-68 バッファ割り当て方式、説明 33-18 フローチャート 33-17 信頼状態 信頼性のあるデバイス 33-39 説明 33-5 ドメイン内 33-35 別のドメインとの境界 33-41

DSCP 透過 33-40 DSCP マップ 33-56 IP 拡張 ACL 33-44 IP 標準 ACL 33-43 MAC ACL 33-45 自動 OoS 33-20 集約ポリサー 33-54 出力キューの特性 33-67 信頼境界 33-39 デフォルトのポート CoS 値 33-38 ドメイン内のポートの信頼状態 33-35 入力キューの特性 33-62 別のドメインとの境界での DSCP 信頼状 33-41 能 設定時の注意事項 自動 QoS 33-26 標準 QoS 33-33 デフォルトの自動設定 33-21 デフォルトの標準設定 33-31 統計の表示 33-75 入力キュー DSCP または CoS 値のマッピング 33-62 SRR 共有重みの設定 33-65 WTD しきい値の設定 33-62 WTD、説明 33-16 しきい値マップの表示 33-63 スケジューリング、説明 33-4 説明 33-4 帯域幅の割り当て 33-65 バッファおよび帯域幅の割り当て、説明 33-16 バッファ スペースの割り当て 33-64 プライオリティ キュー、説明 33-16 プライオリティ キューの設定 33-66 フローチャート 33-15 パケットの変更 33-20 フローチャート 出力キューイングおよびスケジューリン 33-17

設定

入力キューイングおよびスケジューリン ガ 33-15 分類 33-7 ポリシングおよびマーキング 33-11 分類 DSCP 透過、説明 33-40 DSCP を信頼、説明 33-5 IP ACL、説明 33-6, 33-8 IP precedence を信頼、説明 33-5 IP トラフィックのオプション 33-6 MAC ACL、説明 33-5, 33-8 クラス マップ、説明 33-8 信頼性のある CoS、説明 33-5 定義 33-4 転送処理 33-3 非 IP トラフィックのオプション 33-5 フレームおよびパケット 33-3 フローチャート 33-7 ポリシー マップ、説明 33-9 ポリサー 数 33-34 設定 33-52, 33-54 説明 33-9 タイプ 33-10 表示 33-75 ポリシー、インターフェイスに結合 33-10 ポリシー マップ 特性 33-49 表示 33-75 物理ポートの非階層型 33-49 ポリシング 説明 33-4, 33-9 トークン バケット アルゴリズム 33-10 マーキング、説明 33-4, 33-9 マークダウン アクション 33-52 マッピング テーブル CoS/DSCP 33-56 DSCP/CoS 33-59 DSCP/DSCP 変換 33-60

```
IP precedence/DSCP
                        33-57
      タイプ
               33-12
      表示
             33-75
      ポリシング済み DSCP 33-58
OoS O CoS/DSCP \neg \gamma \gamma
                       33-56
QoS の CoS 出力キューしきい値マップ
                                 33-19
QoS の CoS 入力キューしきい値マップ
                                 33-16
QoS の DSCP/CoS マップ
                       33-59
QoS の DSCP/DSCP 変換マップ
                            33-60
QoS の DSCP 出力キューしきい値マップ
                                   33-19
QoS の DSCP 入力キューしきい値マップ
                                   33-16
QoS \mathcal{O} IP precedence/DSCP \forall \forall \forall \forall
                               33-57
OoS の緊急キュー
                 33-73
QoS のクラス マップ
   設定
          33-47
   説明
          33-8
   表示
          33-75
QoS の信頼境界
                33-39
OoS のポリシー マップ
   説明
          33-9
   特性
          33-49
   表示
          33-75
   物理ポートの非階層型
      説明
             33-10
QoS のポリシング済み DSCP マップ
                               33-58
QoS のマッピング テーブル
   設定
      CoS/DSCP 33-56
      DSCP 33-56
      DSCP/CoS
                33-59
      DSCP/DSCP 変換
                        33-60
      IP precedence/DSCP
                        33-57
      ポリシング済み DSCP
                         33-58
   説明
          33-12
Quality of Service
   「OoS」を参照
```

R

RADIUS AAA サーバ グループの定義 8-32 アトリビュート ベンダー固有 8-36 ベンダー独自 8-38 概要 8-19 クラスタ 5-15 サーバの識別 8-28 サーバ ロードバランシング 8-40 サポート 1-12 推奨されるネットワーク環境 8-19 設定 アカウンティング 8-35 許可 8-34 通信、グローバル 8-28, 8-36 通信、サーバ単位 8-28 認証 8-30 複数の UDP ポート 8-28 設定の表示 8-40 デフォルト設定 8-28 動作 8-21 方式リスト、定義 8-27 ユーザがアクセスできるサービスのトラッキン グ 8-35 ユーザが使用できるサービスの制限 8-34 RADIUS Change of Authorization 8-21 Rapid Per-VLAN Spanning-Tree Plus 「Rapid PVST+」を参照 Rapid PVST+ IEEE 802.1Q トランキングの相互運用性 16-12 サポートされているインスタンス 16-11 説明 16-11 Rapid Spanning Tree Protocol 「RSTP」を参照 rcommand コマンド 5-16 RCP イメージファイル

アップロード **B-42** サーバの準備 **B-39** ダウンロード **B-40** 古いイメージの削除 **B-42** コンフィギュレーション ファイル アップロード **B-22** 概要 **B-19** サーバの準備 **B-20** ダウンロード **B-21** Remote Authentication Dial-In User Service 「RADIUS」を参照 Remote Copy Protocol 「RCP」を参照 Remote Network Monitoring 「RMON」を参照 responder, IP SLA イネーブル化 32-6 説明 32-4 RFC 1112、IP マルチキャストおよび IGMP 22-2 1157, SNMPv1 30-2 1305、NTP 6-2 1757、RMON 28-2 1901, SNMPv2C **30-2** $1902 \sim 1907$, SNMPv2 **30-2** 2236、IP マルチキャストおよび IGMP 22-2 $2273 \sim 2275$, SNMPv3 30-2 RFC 5176 規定 8-22 RMON アラームおよびイベントのイネーブル化 28-3 概要 28-1 サポート 1-15 サポートされているグループ 28-2 ステータスの表示 28-7 デフォルト設定 28-3 統計 収集、イーサネット グループ 28-6 収集、グループ履歴 28-5 RSPAN

VLAN ベース 27-6 宛先ポート 27-7 概要 1-15, 27-1 受信トラフィック 27-5 ステータスの表示 27-24 セッション イネーブルに設定された入力トラフィッ 27-21 ク 27-18 作成 送信元トラフィックを特定の VLAN に制 27-23 限 27-4 定義 モニタ対象ポートの指定 27-18 設定時の注意事項 27-17 送信元ポート 27-6 他の機能との相互作用 27-9 定義 27-3 デフォルト設定 27-10 伝送トラフィック 27-5 特性 27-8 モニタ側ポート 27-7 モニタ対象ポート 27-6 RSTP BPDU 17-13 処理 フォーマット 17-13 IEEE 802.1D との相互運用性 移行プロセスの再起動 17-27 説明 17-9 トポロジの変更 17-14 アクティブ トポロジ 17-10 概要 17-9 高速コンバージェンス エッジ ポートおよび PortFast 17-10 17-10 説明 ポイントツーポイント リンク 17-11, 17-26 ルート ポート 17-10 指定スイッチ、定義 17-9 指定ポート、定義 17-9

提案 / 合意ハンドシェイク プロセス 17-11 ポートの役割 説明 17-9 同期 17-12 ルートポート、定義 17-9 「MSTP」も参照

S

SCP SSH 8-54 8-54 設定 「SCP」を参照 SC (スタンバイ コマンド スイッチ) 5-11 SDM テンプレート 数 7-1 設定 7-3 SDM テンプレート 設定 7-2 設定時の注意事項 7-2 タイプ 7-1 Secure Copy Protocol Secure Shell 「SSH」を参照 Secure Socket Layer 「SSL」を参照 set-request 動作 30-5 SFP ステータスのモニタ 11-32, 37-14 ステータス、表示 37-14 セキュリティと識別 37-14 Shaped Round Robin 「SRR」を参照 show access-lists hw-summary $\exists \forall \mathcal{V} \models$ 31-39 show cdp traffic $\neg \neg \checkmark ee$ 25-5 show cluster members $\exists \forall \vee ee$ 5-16 show configuration コマンド 11-29 show forward $\neg \neg \checkmark ee$ 37-23

show interfaces switchport 19-5 show interfaces $\neg \neg \checkmark \lor$ 11-21, 11-29 show lldp traffic $\exists \forall \vee \lor$ 26-13 show platform forward $\exists \forall \vee \lor$ 37-23 ACL の表示 31-38, 31-39 インターフェイスの記述 11-29 show および more コマンド出力、フィルタリング 2-10 Smartport マクロ グローバル パラメータ値の適用 12-19 シスコのデフォルト マクロの適用 12-19 設定時の注意事項 12-18 追跡 12-18 定義 12-2 デフォルト設定 12-18 表示 12-21 SNAP 25-1 **SNMP** CPU しきい値通知の設定 30-17 ifIndex 値 30-6 informs trap キーワード 30-13 イネーブル化 30-16 説明 30-5 ディセーブル化 30-16 トラップとの相違 30-5 IP SLA 32-2 MIB サポートされている A-1 場所 A-3 MIB 変数にアクセス 30-5 NMS に対するシステム ログ メッセージの制 限 29-11 TFTP サーバによるアクセスの制限 30-18 エージェント 説明 30-4 ディセーブル化 30-8 エンジン ID 30-7 帯域内管理 1-6

概要 30-1, 30-5 クラスタ 5-15 クラスタの管理 5-17 グループ 30-7, 30-10 コミュニティ ストリング 概要 30-4 クラスタ スイッチ 30-4 設定 30-9 サポートされているバージョン 30-2 システム コンタクトおよびロケーション 30-17 ステータス、表示 30-20 セキュリティ レベル 30-3 設定例 30-19 通知 30-5 デフォルト設定 30-7 トラップ informs との相違 30-5 MACアドレス通知のイネーブル化 6-25, 6-27, 6-28 イネーブル化 30-13 概要 30-1, 30-5 説明 30-3, 30-5 タイプ 30-13 ディセーブル化 30-16 トラップマネージャ、設定 30-14 認証レベル 30-11 ホスト 30-7 マネージャ機能 1-5, 30-3 ユーザ 30-7, 30-10 SNMPv1 30-2 SNMPv2C 30-2 SNMPv3 30-2 **SPAN** VLAN ベース 27-6 宛先ポート 27-7 概要 1-15, 27-1 受信トラフィック 27-5 ステータスの表示 27-24 セッション

宛先(モニタ側)ポートの削除 27-13 イネーブルに設定された入力トラフィッ カ 27-14 作成 27-11 送信元トラフィックを特定の VLAN に制 27-16 肦 定義 27-4 入力転送の設定 27-15, 27-22 モニタ対象ポートの指定 27-11 設定時の注意事項 27-10 送信元ポート 27-6 他の機能との相互作用 27-9 デフォルト設定 27-10 伝送トラフィック 27-5 ポート、制限 23-13 モニタ側ポート 27-7 モニタ対象ポート 27-6 Spanning Tree Protocol 「STP」を参照 27-5 SPAN トラフィック SRR 共有モード 33-14 サポート 1-14 シェーピング モード 33-14 設定 出力キューでの共有重み 33-72 33-71 出力キューでのシェーピング重み 入力キューでの共有重み 33-65 説明 33-14 SSH 暗号化ソフトウェア イメージ 8-42 暗号方式 8-42 設定 8-43 説明 1-6, 8-42 ユーザ認証方式、サポートされている 8-43 SSL 暗号化ソフトウェア イメージ 8-46 セキュア HTTP クライアントの設定 8-53 セキュア HTTP サーバの設定 8-51

設定時の注意事項 8-49 説明 8-46 モニタ 8-53 STP BackboneFast イネーブル化 18-16 説明 18-6 ディセーブル化 18-16 BPDU ガード イネーブル化 18-12 説明 18-3 ディセーブル化 18-13 BPDU フィルタリング イネーブル化 18-14 説明 18-3 ディセーブル化 18-14 BPDU メッセージ交換 16-3 EtherChannel ガード イネーブル化 18-16 説明 18-8 ディセーブル化 18-17 IEEE 802.1D およびブリッジ ID 16-4 IEEE 802.1D およびマルチキャスト アドレ ス 16-10 IEEE 802.10 トランクの制限 16-12 IEEE 802.1t および VLAN Identifier 16-4 PortFast イネーブル化 18-11 説明 18-2 PortFast 対応ポートのシャットダウン 18-3 UplinkFast イネーブル化 18-15 説明 18-4 インターフェイス ステート 概要 16-5 ディセーブル 16-8 フォワーディング 16-6, 16-8 ブロッキング 16-7 ラーニング 16-7

リスニング 16-7 インターフェイス ステート、ブロッキングからフォ ワーディングへ 18-2 下位 BPDU 16-4 概要 16-2 カウンタ、クリア 16-25 拡張システム ID 概要 16-4 セカンダリ ルート スイッチの影響 16-18 予期しない動作 16-17 ルート スイッチでの影響 16-16 間接リンク障害の検出 18-6 サポートされているインスタンス 16-11 サポートされているオプション機能 1-8 サポートされている機能 1-8 サポートされているプロトコル 16-10 サポートされているモード 16-10 指定スイッチ、定義 16-4 指定ポート、定義 16-4 冗長接続 16-9 ステータスの表示 16-25 ステータス、表示 16-25 設定 Hello タイム 16-22 最大エージング タイム 16-23 スイッチ プライオリティ 16-21 スパニング ツリー モード 16-15 セカンダリ ルート スイッチ 16-18 転送遅延時間 16-23 転送保留カウント 16-24 パス コスト 16-20 ポート プライオリティ 16-19 ルート スイッチ 16-16 設定時の注意事項 16-14, 18-11 タイマー、説明 16-22 ディセーブル化 16-16 デフォルト設定 16-13 デフォルトのオプション機能の設定 18-11 パス コスト 13-23

負荷分散 概要 13-21 パス コストを使用 13-23 ポート プライオリティを使用 13-21 ポート プライオリティ 13-22 マルチキャストアドレス、影響 16-10 モード間の相互運用性と下位互換性 16-12 優位 BPDU 16-3 ルート ガード イネーブル化 18-17 説明 18-8 ルート スイッチ 拡張システム ID の影響 16-4, 16-16 設定 16-16 選択 16-4 予期しない動作 16-17 ルート スイッチの選択の防止 18-8 ルート ポートを短時間で選択する 18-4 ループ ガード イネーブル化 18-18 説明 18-10 SunNet Manager 1-5 Smartport マクロ 「Auto SmartPort マクロ」も参照 Switch Database Management 「SDM」を参照 Switched Port Analyzer 「SPAN」を参照 switchport backup interface **19-4**, **19-6** switchport block multicast $\neg \neg \checkmark ee$ 23-9 switchport block unicast $\exists \forall \mathcal{V} \vdash$ 23-9 switchport protected コマンド 23-7 syslog 「システム メッセージ ロギング」を参照

Т

TACACS+

アカウンティング、定義 8-12

概要 8-11 許可、定義 8-12 クラスタ 5-15 サーバの識別 8-14 サポート 1-12 設定 アカウンティング 8-18 許可 8-17 認証鍵 8-14 ログイン認証 8-15 設定の表示 8-19 デフォルト設定 8-14 動作 8-13 認証、定義 8-12 ユーザがアクセスできるサービスのトラッキン グ 8-18 ユーザが使用できるサービスの制限 8-17 tar ファイル イメージ ファイル形式 **B-29** 作成 **B-8** 抽出 **B-9** 内容の表示 **B-8** TDR 1-15 Telnet 管理インターフェイスへのアクセス 2-11 接続数 1-6 パスワードの設定 8-6 Terminal Access Controller Access Control System Plus 「TACACS+」を参照 TFTP イメージ ファイル アップロード **B-33** サーバの準備 **B-31** 削除 **B-33** ダウンロード **B-31** コンフィギュレーション ファイル アップロード **B-14** サーバの準備 **B-12** ダウンロード **B-13**

サーバによるアクセスの制限 30-18 自動設定の設定 3-8 ベース ディレクトリのコンフィギュレーション ファ イル 3-8 TFTP サーバ 1-5 Time Domain Reflector 「TDR」を参照 time-range コマンド 31-35 TLV LLDP 26-2 LLDP-MED 26-3 定義 26-2 ToS 1-13 traceroute コマンド 37-19 「IP traceroute」も参照 traceroute, $\nu \uparrow \neq 2$ ARP 37-17 CDP 37-17 IP アドレスおよびサブネット 37-17 MAC アドレスおよび VLAN 37-17 使用上のガイドライン 37-17 説明 37-16 ブロードキャスト トラフィック 37-16 ポート上の複数のデバイス 37-17 マルチキャスト トラフィック 37-17 ユニキャスト トラフィック 37-16 trusted (信頼性のある) ポート ステート IP Phone のポート セキュリティを確保 33-39 OoS ドメイン間 33-41 QoS ドメイン内 33-35 サポート 1-13 分類オプション 33-5 Type of Service 「ToS」を参照

U

UDLD イネーブル化

インターフェイス単位 24-6 グローバル 24-5 インターフェイスのリセット 24-7 概要 24-1 検出メカニズムとしてエコーを利用 24-3 サポート 1-8 ステータス、表示 24-7 設定時の注意事項 24-5 ディセーブル化 インターフェイス単位 24-6 グローバル 24-6 光ファイバ インターフェイス上 24-6 デフォルト設定 24-4 ネイバデータベース 24-3 リンク検出のメカニズム 24-1 UDLD shutdown インターフェイスのリセット 24-7 unicast storm control コマンド 23-4 UniDirectional Link Detection プロトコル 「UDLD」を参照 UNIX Syslog サーバ サポートされているファシリティ 29-14 デーモンの設定 29-13 メッセージ ロギングの設定 29-14 UplinkFast イネーブル化 18-15 サポート 1-8 説明 18-4 ディセーブル化 18-15

V

VLAN RSPAN 送信元トラフィックを制限 27-23 SPAN 送信元トラフィックを制限 27-16 STP および IEEE 802.1Q トランク 16-12 VLAN データベースへの追加 13-8 VTP モード 14-3 間のトラフィック 13-2 エージング、ダイナミック アドレス 16-10

拡張範囲 13-1, 13-11 機能 1-9 削除 13-10 作成 13-9 サポートされている 13-3 サポートされている数 1-9 図 13-2 スタティック アクセス ポート 13-10 スパニングツリーインスタンス 13-3, 13-7, 13-12 設定 13-1 設定、ID 1006 ~ 4094 13-12 設定時の注意事項、拡張範囲 VLAN 13-12 設定時の注意事項、標準範囲 VLAN 13-6 説明 11-2, 13-2 追加 13-8 デフォルト設定 13-8 トークンリング 13-6 トランク上で許可される 13-18 ネイティブ、設定 13-20 パラメータ 13-5 表示 13-14 標準範囲 13-1, 13-5 13-8 変更 ポート メンバシップ モード 13-4 マルチキャスト 22-19 vlan.dat ファイル 13-5 VLAN 1 最小化 13-18 VLAN 1、トランク ポート上でディセーブル 13-18 VLAN ID、検出 6-34 VLAN Management Policy Server 「VMPS」を参照 VLAN Query Protocol 「VOP」を参照 VLAN Trunking Protocol 「VTP」を参照 VLAN 管理ドメイン 14-2 vlan グローバル コンフィギュレーション コマン ド 13-7 VLAN コンフィギュレーション

起動時 13-7 保存 13-7 VLAN コンフィギュレーション モード 2-2 VLAN データベース VLAN コンフィギュレーション、保存 13-7 VLAN、保存 13-5 VTP **14-1** スタートアップ コンフィギュレーション ファイ 13-7 ル VLAN トランク 13-14 VLAN の削除 13-10 VLAN フィルタリングおよび SPAN 27-7 VLAN メンバシップ 確認 13-28 モード 13-4 VLAN 割り当て応答、VMPS 13-25 VMPS MAC アドレスの VLAN へのマッピング 13-25 管理 13-30 サーバ アドレスの入力 13-27 再確認インターバル、変更 13-29 再試行の回数、変更 13-29 設定時の注意事項 13-26 設定例 13-31 説明 **13-24** ダイナミック ポート メンバシップ 再確認 13-29 説明 13-25 トラブルシューティング 13-30 デフォルト設定 13-26 メンバシップの再確認 13-28 モニタ 13-30 Voice over IP 15-1 VQP 1-9, 13-24 VTP アドバタイズ 13-16, 14-4 拡張範囲 VLAN 13-3, 14-2 クライアントモード、設定 14-13 クライアントをドメインに追加 14-17

コンフィギュレーション リビジョン番号 注意事項 14-17 リセット 14-17 サーバモード、設定 14-11, 14-14 サポート 1-9 使用 14-1 整合性検査 14-5 設定 注意事項 14-8 保存 14-9 要件 14-11 設定要件 14-11 説明 14-1 デフォルト設定 14-8 統計 14-18 トークンリングのサポート 14-4 ドメイン 14-2 ドメイン名 14-9 トランスペアレントモード、設定 14-11 バージョン イネーブル化 14-14 バージョン1 14-4 バージョン2 概要 14-4 設定時の注意事項 14-10 バージョン3 概要 14-5 バージョン、注意事項 14-10 パスワード 14-9 標準範囲 VLAN 13-3, 14-2 プルーニング イネーブル化 14-16 概要 14-6 サポート 1-9 ディセーブル化 14-16 14-6 例 プルーニング適格リスト、変更 13-19 モード 移行 14-3

オフ 14-3 クライアント 14-3 サーバ 14-3 トランスペアレント 14-3 モニタ 14-18 VTP バージョン 2 での整合性検査 14-5

W

Web 認証 9-17 設定 10-17 説明 1-10 Web ベース認証 カスタマイズ可能な Web ページ 10-6 説明 10-1 Web ベース認証、他の機能との相互作用 10-7 Weighted Tail Drop 「WTD」を参照 WTD サポート 1-14 しきい値の設定 出力キューセット 33-68 入力キュー 33-62 説明 33-13

Х

Xmodem プロトコル 37-2

あ

```
アカウンティング
802.1x 9-51
IEEE 802.1x 9-15
RADIUS 8-35
TACACS+ 8-12, 8-18
アクセス
クラスタ、スイッチ 5-14
```

コマンド スイッチ 5-12 スイッチ クラスタ 5-14 メンバー スイッチ 5-14 アクセス拒否応答、VMPS **13-25** アクセス グループ、インターフェイスへの IPv4 ACL の 適用 31-38 アクセス制御エントリ 「ACE」を参照 アクセスの制限 NTP サービス 6-8 RADIUS 8-19 TACACS+ 8-11 概要 8-1 パスワードと権限レベル 8-2 アクセス不能認証バイパス 9-24 複数認証ポートのサポート 9-24 アクセス ポート スイッチ クラスタ 5-10 アクセス ポート、定義 11-3 アクセス リスト 「ACL」を参照 アクティブ トラフィック モニタリング、IP SLA 32-1 アクティブ リンク **19-2**, **19-4**, **19-5**, **19-6** アップロード イメージファイル FTP を使用 **B-37** RCP を使用 **B-42** TFTP を使用 **B-33** B-31, B-34, B-39 進備 理由 **B-28** コンフィギュレーション ファイル FTP を使用 **B-18** RCP を使用 **B-22** TFTP を使用 **B-14** 準備 B-12, B-16, B-20 理由 **B-10** 宛先 IP アドレスベース転送、EtherChannel 36-7 宛先 MAC アドレス転送、EtherChannel 36-7 宛先アドレス

IPv4 ACL 31-30 アドバタイズ CDP **25-1** LLDP 26-2 VTP 13-16, 14-3, 14-4 アトリビュート、RADIUS ベンダー固有 8-36 ベンダー独自 8-38 アトリビュート値ペア 9-13, 9-15, 9-20, 9-21 アドレス IPv6 34-2 MAC アドレス テーブルの表示 6-33 MAC、検出 6-34 スタティック 追加と削除 6-30 定義 6-22 ダイナミック エージング タイムの変更 6-24 削除 6-24 短縮、エージング 16-10 定義 6-22 デフォルト、エージング 16-10 ラーニング **6-23** マルチキャスト、STP アドレスの管理 16-10 アドレス エイリアス 22-2 アドレスの解決 6-34 アベイラビリティ、機能 1-8 アラーム、RMON 28-4 暗号化、CipherSuite 8-48 暗号化ソフトウェア イメージ SSH 8-42 SSL 8-46 安全なリモート接続 8-42

い

イーサネット VLAN 追加 **13-8** デフォルト値および範囲 **13-8**

変更 13-8 一時的な自己署名証明書 8-47 一致、IPv4 ACL 31-26 一般クエリー 19-5 イネーブル シークレット パスワード 8-4 イネーブル パスワード 8-4 イベント、RMON 28-4 インターネット プロトコル バージョン6 「IPv6」を参照 インターフェイス Auto-MDIX、設定 11-23 カウンタ、クリア 11-32 管理 1-5 記述、追加 11-29 11-33 再起動 サポートされている 11-11 シャットダウン 11-33 情報の表示 11-31 ステータス 11-31 設定 手順 11-11 設定時の注意事項 デュプレックスおよび速度 11-19 説明 11-29 タイプ 11-1 デフォルト設定 11-16 デュプレックスおよび速度、設定 11-20 名前付け 11-29 範囲 11-12 番号 11-11 物理、識別 11-11 フロー制御 11-22 モニタ 11-31 レンジマクロ 11-14 インターフェイス コマンド 11-11 インターフェイス コンフィギュレーション モード 2-3 インターフェイス上の shutdown コマンド 11-33 インターフェイス タイプ 11-11 インターフェイスのクリア 11-32

う

ウィザード **1-2**

え

永続的な自己署名証明書 8-47 エージング タイム MAC アドレス テーブル 6-24 最大 MSTP **17-25** STP 用 16-23, 16-24 短縮 17-24 MSTP STP 用 16-10, 16-23 エージング、短縮 16-10

お

応答時間、測定、IP SLA を使用 32-4 オプション、管理 1-5 オフモード、VTP 14-3 音声 VLAN Cisco 7960 Phone、ポート接続 15-1 IP Phone の音声トラフィック、説明 15-2 IP Phone のデータ トラフィック、説明 15-3 IP Phone への接続 15-5 音声トラフィックのポートの設定 802.1p プライオリティ タグ フレーム 15-6 802.1Q フレーム 15-6 設定時の注意事項 15-4 説明 15-1 データ トラフィック用に IP Phone を設定 着信フレームの CoS の上書き 15-7 着信フレームの CoS プライオリティを信頼す ろ 15-7 デフォルト設定 15-3 表示 15-8 音声認識 802.1x セキュリティ

ポートベース認証 設定 9-39 説明 9-31, 9-39

か

解析のためのトラフィックのミラーリング 27-1 ガイドモード 1-2 37-1 回復手順 カウンタ、インターフェイスのクリア 11-32 拡張 crashinfo ファイル 37-24 拡張システム ID MSTP **17-18** STP 16-4, 16-16 拡張範囲 VLAN 作成 13-12 設定 13-11 設定時の注意事項 13-12 定義 13-1 カスタマイズ可能な Web ページ、Web ベース認 証 10-6 仮想 IP アドレス クラスタ スタンバイ グループ 5-12 コマンド スイッチ 5-12 仮想スイッチおよび PAgP 36-5 簡易ネットワーク管理プロトコル 「SNMP」を参照 環境変数、機能 3-22 間接リンク障害の検出、STP 18-6 管理 VLAN 異なる管理 VLAN からの検出 5-9 スイッチ クラスタに関する考慮事項 5-9 管理アクセス 帯域外コンソール ポート接続 1-6 帯域内 CLIセッション 1-6 SNMP **1-6** デバイス マネージャ 1-6 ブラウザ セッション 1-6

管理アドレス TLV 26-2
管理オプション
CLI 2-1
CNS 4-1
Network Assistant 1-2
概要 1-5
クラスタ化 1-3
管理の簡易性に関する機能 1-5

き

起動 起動プロセス 3-2 手動で 3-19 特定のイメージ 3-20 ブート ローダ、機能 3-2 機能、互換性のない 23-13 競合、設定 37-12 許可 RADIUS 8-34 TACACS+ 8-12, 8-17 許可 VLAN リスト 13-18 許可ポート、IEEE 802.1x 9-11 近接ディスカバリ、IPv6 34-4

<

クエリー、IGMP 22-4 クエリー送信要求、IGMP 22-14 クライアントモード、VTP 14-3 クラスタ 5-16 クラスタ、スイッチ LRE プロファイルに関する考慮事項 5-16 アクセス 5-14 管理 CLI を通じて 5-16 SNMP を通して 5-17 互換性 5-5 自動検出 5-5

自動復旧 5-11 説明 5-1 プラン 5-5 プランニングに関する考慮事項 CLI 5-16 IPアドレス 5-14 LRE プロファイル 5-16 RADIUS 5-15 SNMP 5-15, 5-17 TACACS+ 5-15 自動検出 5-5 自動復旧 5-11 パスワード 5-15 ホスト名 5-14 利点 1-2 クラスタ スタンバイ グループ 仮想 IP アドレス 5-12 考慮事項 5-12 自動復旧 5-13 定義 5-2 要件 5-4 「HSRP」も参照 クラスタ、スイッチ 「候補スイッチ」、「コマンドスイッチ」、「クラスタス タンバイ グループ |、「メンバー スイッチ」および 「スタンバイ コマンド スイッチ」も参照 クリティカル VLAN 9-24 クリティカル認証、IEEE 802.1x 9-55 グローバル Leave、IGMP 22-14 グローバル コンフィギュレーション モード 2-2 クロック 「システム クロック」を参照

け

ケーブル、単一方向リンクのモニタリング 24-1 ゲスト VLAN と 802.1x 9-22 権限レベル 回線に対するデフォルトの変更 8-10

概要 8-2, 8-8 コマンドスイッチ 5-16 コマンドの設定 8-8 終了 8-10 メンバー スイッチのマッピング 5-16 ログイン 8-10 検出、クラスタ 「自動検出」を参照

J

構成例、ネットワーク 1-19 高速コンバージェンス 17-10, 19-3 候補スイッチ 自動検出 5-5 定義 5-4 要件 5-4 「コマンドスイッチ」、「クラスタスタンバイグルー プ」および「メンバー スイッチ」も参照 互換性、機能 23-13 コマンド no および default 2-4 2-4 省略 コマンド エントリ中のエラー メッセージ 2-5 コマンド、権限レベルの設定 8-8 コマンド スイッチ アクセス 5-12 アクティブ (AC) 5-11 交換 クラスタ メンバー 37-9 他のスイッチと 37-11 冗長 5-11 スタンバイ (SC) 5-11 設定の競合 37-12 定義 5-2 パスワード、権限レベル 5-16 パッシブ (PC) 5-11 復旧

コマンドスイッチで障害が発生した場合 5-11. 37-8 メンバー スイッチとの接続の回復 37-12 プライオリティ 5-11 要件 5-3 「候補スイッチ」、「クラスタ スタンバイ グループ」、 「メンバースイッチ」および「スタンバイコマンドス イッチ」も参照 コマンドの省略 2-4 コマンド モード 2-1 コマンドライン インターフェイス 「CLI」を参照 コミュニティ ストリング SNMP **5-15** 概要 30-4 クラスタ 5-15 クラスタ スイッチ 30-4 設定 5-15, 30-9 コンソール ポート、接続 2-11 コントロール プロトコル、IP SLA 32-4 コンフィギュレーション交換 **B-23** コンフィギュレーション ファイル TFTP サーバ アクセスの制限 30-18 アーカイブ **B-24** アップロード FTP を使用 **B-18** RCP を使用 **B-22** TFTP を使用 **B-14** 準備 B-12, B-16, B-20 理由 **B-10** 交換、実行コンフィギュレーション B-23, B-24 交換またはロール バックの注意事項 **B-25** コピー時の無効な組み合わせ **B-6** 削除、格納されたコンフィギュレーション **B-23** 作成および使用上の注意事項 **B-11** 作成、テキストエディタを使用 **B-12** システム コンタクトおよびロケーション情 30-17 報 消去、スタートアップ コンフィギュレーショ \geq **B-23**

説明 **B-10** タイプおよび場所 **B-11** ダウンロード FTP を使用 **B-16** RCP を使用 **B-21** TFTP を使用 **B-13** 自動 3-18 準備 B-12, B-16, B-20 理由 **B-10** デフォルトの名前 3-18 入手、DHCP を使用 3-10 パスワード回復のディセーブル化に関する考慮事 項 8-5 ファイル名の指定 3-19 ロール バック、実行コンフィギュレーショ B-23, B-25 ン コンフィギュレーション ロールバック B-23, B-24 コンフィギュレーション ロギング 2-5 コンポーネント管理 TLV 26-3, 26-9

さ

サーバモード、VTP 14-3
サービス プロバイダー ネットワーク、MSTP および RSTP 17-1
再確認インターバル、VMPS、変更 13-29
再試行の回数、VMPS、変更 13-29
最大エージング タイム MSTP 17-25
STP 16-23
最大ホップ カウント、MSTP 17-25
サポートされているポートベース認証方法 9-8
サマータイム(夏時間) 6-14

し

シェル関数 「Auto SmartPort マクロ」を参照 シェル トリガー

「Auto SmartPort マクロ」を参照 しきい値、トラフィック レベル 23-2 システム記述 TLV 26-2 システム機能 TLV 26-2 システム クロック 概要 6-2 設定 手動で 6-12 タイム ゾーン 6-13 夏時間 6-14 夏時間(サマータイム) 6-14 日時の表示 6-13 「NTP」も参照 システム プロンプト、デフォルト設定 6-16 システム名 手動設定 6-16 デフォルト設定 6-16 「DNS」も参照 システム名 TLV 26-2 システム メッセージ ロギング facility キーワード、説明 29-14 level キーワード、説明 29-10 syslog ファシリティ 1-15 UNIX Syslog サーバ サポートされているファシリティ 29-14 デーモンの設定 29-13 ロギング ファシリティの設定 29-14 イネーブル化 29-5 概要 29-2 シーケンス番号、イネーブル化およびディセーブル 29-8 化 設定の表示 29-15 タイム スタンプ、イネーブル化およびディセーブル 化 29-8 ディセーブル化 29-4 デフォルト設定 29-4 表示宛先デバイスの設定 29-5 メッセージ重大度の定義 29-9 メッセージの制限 29-11

メッセージ フォーマット 29-3 ログ メッセージの同期化 29-6 システム リソース、最適化 7-1 システム リソースの最適化 7-1 実行コンフィギュレーション B-23, B-24 交換 ロール バック **B-23, B-25** 実行コンフィギュレーション、保存 3-17 自動 OoS 「OoS」を参照 自動イネーブル化 9-31 自動検出 考慮事項 CDP 非対応デバイス 5-6 新しいスイッチ 5-10 管理 VLAN 5-9 クラスタ非対応デバイス 5-6 異なる VLAN 5-7 接続 5-5 非候補デバイスより先 5-9 スイッチ クラスタ 5-5 「CDP」も参照 自動検知、ポートの速度 1-3 自動設定 3-4 自動ネゴシエーション インターフェイス コンフィギュレーションに関する 考慮事項 11-20 デュプレックス モード 1-3 不一致 37-13 自動復旧、クラスタ 5-11 「HSRP」も参照 重大度、システム メッセージでの定義 29-9 柔軟な認証の順序設定 概要 9-30 設定 9-66 集約可能なグローバル ユニキャスト アドレス 34-3 集約ポート 「EtherChannel」を参照 集約ポリサー 33-54

集約ポリシング 1-14 準備状態チェック ポートベース認証 設定 9-38 説明 9-17, 9-38 冗長性 EtherChannel **36-3** STP パス コスト 13-23 バックボーン 16-9 ポート プライオリティ 13-21 冗長リンクと UplinkFast 18-15 初期設定 Express Setup 1-2 デフォルト 1-16 信頼できるタイム ソース、説明 6-2 信頼点、CA 8-47

す

スイッチ ソフトウェア機能 1-1 スイッチドポート 11-2 スイッチのクラスタ化テクノロジー 5-1 「クラスタ、スイッチ」も参照 スイッチのコンソール ポート 1-6 スイッチ プライオリティ MSTP 17-23 STP 16-21 スタートアップ コンフィギュレーション 記動 手動で 3-19 特定のイメージ 3-20 起動のデフォルト設定 3-18 コンフィギュレーション ファイル 自動ダウンロード 3-18 ファイル名の指定 3-19 消去 **B-23** スタティック MAC アドレッシング 1-10 スタティック VLAN メンバシップ 13-2

スタティック アクセス ポート VLAN への割り当て 13-10 定義 11-3, 13-4 スタティック アドレス 「アドレス」を参照 スタティック ホスト用 IP ポート セキュリティ レイヤ2アクセス ポート上での 20-20 スタティック ルート 概要 34-6 設定、IPv6用 34-11 スタンバイ グループ、クラスタ 「クラスタ スタンバイ グループ」および「HSRP」を 参照 スタンバイ コマンド スイッチ 仮想 IP アドレス 5-12 考慮事項 5-12 設定 定義 5-2 プライオリティ 5-11 要件 5-4 「クラスタ スタンバイ グループ」および「HSRP」も 参照 スタンバイ リンク 19-2 スティッキー ラーニング 23-10 ストーム制御 サポート 1-4 しきい値 23-1 設定 23-3 説明 23-1 ディセーブル化 23-5 23-20 表示 ストラタム、NTP 6-2 スヌーピング、IGMP 22-2 スパニング ツリーおよびネイティブ VLAN 13-16

せ

制限付き VLAN IEEE 802.1x で使用 **9-23**

設定 9-53 説明 9-23 成功応答、VMPS **13-25** セキュア HTTP クライアント 設定 8-53 表示 8-53 セキュア HTTP サーバ 8-47 設定 8-51 表示 8-53 セキュア MAC アドレス 最大数 23-10 削除 23-17 タイプ 23-10 セキュアポート、設定 23-9 セキュリティ機能 1-10 セキュリティ、ポート 23-9 接続、安全なリモート 8-42 接続の問題 37-15, 37-16, 37-18 設定、初期 Express Setup 1-2 デフォルト 1-16 設定、小さいフレームの着信レートの 23-6 設定値、保存 3-17 設定の競合、メンバー スイッチとの接続の回復 37-12 設定の変更、ロギング 29-11 設定ロガー 29-11 セットアップ プログラム 交換、故障したコマンドスイッチ 37-9 故障したコマンド スイッチの交換 37-11

そ

送信元 IP アドレスベース転送、EtherChannel 36-7 送信元 MAC アドレス転送、EtherChannel 36-7 送信元 / 宛先 IP アドレスベース転送、 EtherChannel 36-8 送信元アドレス IPv4 ACL 31-30 送信元および宛先 MAC アドレス転送、 EtherChannel **36-7** 即時脱退、IGMP 22-6 イネーブル化 35-10 ソフト 30-5 ソフトウェア イメージ tar ファイル形式、説明 **B-29** 回復手順 37-2 場所、フラッシュ **B-29** リロードのスケジュール 3-23 「ダウンロード」および「アップロード」も参照 ソフトウェア イメージのアップグレード 「ダウンロード」を参照 ソフトウェアのリロード 3-23

た

ダイナミック ARP インスペクション ARP ACL および DHCP スヌーピング エントリの優 先順位 21-5 ARP キャッシュ ポイズニング 21-2 ARP スプーフィング攻撃 21-2 ARP パケットのレート制限 errdisable ステート 21-5 設定 21-12 説明 21-5 ARP 要求、説明 21-2 DHCP スヌーピング バインディング データベー ス 21-3 DoS 攻撃、防止 21-12 man-in-the middle 攻撃、説明 21-2 インターフェイス信頼状態 21-3 確認検査、実行 21-14 機能 21-2 クリア 統計 21-17 ログバッファ 21-17 設定 **DHCP** 環境での 21-8 着信 ARP パケットのレート制限 21-5, 21-12

非 DHCP 環境の ACL 21-10 ログバッファ 21-15 設定時の注意事項 21-7 説明 21-2 超過したレート制限の errdisable ステート 21-5 デフォルト設定 21-6 統計 クリア 21-17 21-17 表示 ネットワーク セキュリティ問題およびインターフェ イス信頼状態 21-3 廃棄されたパケットのロギング、説明 21-5 表示 ARP ACL 21-17 信頼状態およびレート制限 21-17 設定および動作ステート 21-17 統計 21-17 ログ バッファ 21-17 ログ バッファ クリア 21-17 設定 21-15 表示 21-17 ダイナミック VLAN メンバシップの再確認 13-28 ダイナミック アクセス ポート 設定 13-28 定義 11-3 特性 13-4 ダイナミック アドレス 「アドレス」を参照 ダイナミック ポート VLAN メンバシップ 再確認 13-28, 13-29 接続のタイプ 13-28 説明 13-25 トラブルシューティング 13-30 タイム 「NTP」および「システム クロック」を参照 タイム ゾーン 6-13 ダウンロード イメージ ファイル

CMS を使用 1-2 FTP を使用 **B-35** HTTP を使用 1-2, B-28 RCP を使用 **B-40** TFTP を使用 **B-31** 準備 B-31, B-34, B-39 デバイス マネージャまたは Network Assistant の 使用 **B-28** 古いイメージの削除 **B-33** 理由 **B-28** コンフィギュレーション ファイル FTP を使用 **B-16** RCP を使用 **B-21** TFTP を使用 **B-13** 準備 B-12, B-16, B-20 理由 **B-10** ダウンロード可能 ACL 9-20, 9-21, 9-63 脱退タイマーの設定、IGMP 22-6 端末回線、パスワードの設定 8-6

ち

小さいフレームの着信レート、設定 23-6

つ

ツイストペア イーサネット、単一方向リンクの検出 24-1

τ

ディレクトリ
作成と削除 B-5
表示、作業 B-4
変更 B-4
です 6-24
デバイス B-28
デバイス検出プロトコル 25-1, 26-2
デバイス マネージャ

帯域内管理 1-6 スイッチのアップグレード **B-28** 説明 1-2, 1-5 利点 1-2 デバッグ イネーブル化、特定機能に関する 37-21 エラー メッセージ出力のリダイレクト 37-22 コマンドを使用 37-21 システム全体診断のイネーブル化 37-22 デフォルト ゲートウェイ 3-16 デフォルト設定 802.1x 9-34 CDP 25-2 DHCP 20-9 DHCP Option 82 20-9 DHCP スヌーピング 20-9 DHCP スヌーピング バインディング データベー 20-9 ス DNS 6-17 EtherChannel 36-9 Flex Link **19-9** IGMP スヌーピング 22-7, 35-6 IGMP スロットリング 22-28 IGMP フィルタリング 22-28 IP SLA 32-5 IPv6 34-7 IP 送信元ガード 20-18 LLDP **26-6** MAC アドレス テーブル 6-23 MAC アドレス テーブル移動更新 19-9 MSTP 17-15 MVR 22-22 NTP 6-4 RADIUS 8-28 RMON 28-3 RSPAN 27-10 SDM テンプレート 7-2 SNMP 30-7 SPAN 27-10

SSL 8-49 STP 16-13 TACACS+ 8-14 UDLD 24-4 VLAN 13-8 VLAN、レイヤ2イーサネットインターフェイ ス 13-16 VMPS 13-26 VTP **14-8** イーサネット インターフェイス 11-16 オプションのスパニング ツリー機能 18-11 音声 VLAN 15-3 起動 3-18 システム名とプロンプト 6-16 システム メッセージ ロギング 29-4 自動 QoS 33-21 スイッチの初期情報 3-3 ダイナミック ARP インスペクション 21-6 パスワードと権限レベル 8-2 バナー 6-19 標準 OoS 33-31 レイヤ2インターフェイス 11-16 デフォルトの Web ベース認証の設定 802.1x **10-9** デュアル IPv4/IPv6 テンプレート 34-5 デュアルアクティブ検出 36-5 デュアルパーパス アップリンク LED **11-4** タイプの設定 11-17 11-4 定義 リンクの選択 11-4, 11-17 デュアル プロトコル スタック IPv4 および IPv6 34-5 SDM テンプレート、サポート 34-5 電源管理 TLV 26-3, 26-9 転送遅延時間 MSTP 17-24 STP 16-23 転送保留カウント

「STP」を参照

ح

統計 802.1x 9-68, 10-18 CDP **25-5** LLDP 26-13 LLDP-MED 26-13 NMSP 26-13 QoS 入力および出力 33-75 RMON イーサネット グループ 28-6 RMON グループ履歴 28-5 SNMP 入出力 30-20 VTP **14-18** インターフェイス 11-31 トークンリング VLAN VTP サポート 14-4 サポート 13-6 都市ロケーション 26-4 特権 EXEC モード 2-2 ドメイン名 DNS 6-17 VTP 14-9 トラップ MAC アドレス通知の設定 6-25, 6-27, 6-28 イネーブル化 6-25, 6-27, 6-28, 30-13 概要 30-1, 30-5 通知タイプ 30-13 定義 30-3 マネージャの設定 30-13 トラップドア メカニズム 3-2 トラフィック フラグメント化された 31-24 フラグメント化されていない 31-24 ブロッキング、フラッディング 23-8 トラフィックの優先処理 「QoS」を参照 トラフィックの抑制 23-1

トラフィック ポリシング 1-14 トラブルシューティング CiscoWorks **30-5** CPU 使用率 37-25 debug コマンド 37-21 ping を使用 37-15 SFP セキュリティと識別 37-14 show forward $\neg \neg \checkmark ee$ 37-23 traceroute **37-18** クラッシュ情報の表示 37-24 システム メッセージ ロギング 29-2 接続の問題 37-15, 37-16, 37-18 単一方向リンクの検出 24-1 パケット転送の設定 37-23 トランキング カプセル化 1-9 トランク DTP をサポートしないデバイス 13-14 許可 VLAN リスト 13-18 タグなしトラフィック用ネイティブ VLAN 13-20 パラレル 13-23 負荷分散 STP パス コストの設定 13-23 STP ポート プライオリティを使用 13-21, 13-22 プルーニング適格リスト 13-19 トランク フェールオーバー 「リンクステート トラッキング」を参照 トランク ポート 設定 13-17 11-3, 13-4 定義 トランスペアレントモード、VTP 14-3

な

夏時間 **6-14** 名前付き IPv4 ACL **31-33**

に

認識不能な Type-Length-Value (TLV) のサポー \mathbb{P} 14-4 認証 NTP アソシエーション 6-5 Open1x 9-30 RADIUS 鍵 8-28 ログイン 8-30 TACACS+ 鍵 8-14 定義 8-12 ログイン 8-15 ローカルモード、AAA 8-40 「ポートベース認証」も参照 認証失敗 VLAN 「制限付き VLAN」を参照 認証マネージャ CLIコマンド 9-10 概要 9-8 旧 802.1x CLI コマンドとの互換性 9-10

ね

ネイティブ VLAN 13-20 設定 デフォルト 13-20 ネットワーク管理 CDP 25-1 RMON 28-1 SNMP 30-1 ネットワーク設計 サービス 1-19 パフォーマンス 1-19 ネットワークの構成例 中小規模のネットワーク 1-22 長距離広帯域トランスポート 1-24 ネットワーク サービスの提供 1-19 ネットワーク パフォーマンスの向上 1-19 ネットワークの設計、例 1-19 ネットワーク パフォーマンス、測定、IP SLA を使 用 32-3 ネットワーク ポリシー TLV 26-3, 26-9

は

バージョン依存型トランスペアレント モード 14-4 バインディング DHCP スヌーピング データベース 20-7 IP 送信元ガード 20-15 バインディング データベース DHCP スヌーピング 「DHCP スヌーピング バインディング データベー ス」を参照 バインディング テーブル、DHCP スヌーピング 「DHCP スヌーピング バインディング データベース」 を参照 パケット 20-6 パケットの変更、QoS を使用 33-20 パスコスト MSTP 17-22 STP 16-20 パスワード VTP ドメイン 14-9 暗号化 8-4 回復 37-4 回復のディセーブル化 8-5 概要 8-1 クラスタ 5-15 セキュリティ 1-10 設定 Telnet 8-6 イネーブル 8-3 イネーブル シークレット 8-4 ユーザ名 8-7 デフォルト設定 8-2 パスワードの暗号化 8-4

破損したソフトウェア、Xmodem を使用した回復手 順 37-2 バックアップ インターフェイス 「Flex Link」を参照 バックアップ リンク 19-2 バナー 設定 Message-of-The-Day (MoTD) ログイン 6-20 ログイン 6-21 デフォルト設定 6-19 表示されるとき 6-19 パフォーマンス向上機能 1-3 パフォーマンス、ネットワーク設計 1-19 範囲 インターフェイス 11-12 マクロ 11-14

ひ

非 IP トラフィックのフィルタリング 31-43 非階層型のポリシーマップ 説明 33-10 光ファイバ、単一方向リンクの検出 24-1 非トランキング モード 13-15 標準範囲 VLAN 13-5 設定 13-5 設定時の注意事項 13-6 定義 13-1

ふ

ファイル crashinfo、説明 **37-24** tar イメージファイル形式 **B-29** 作成 **B-8** 抽出 **B-9** 内容の表示 **B-8** 拡張 crashinfo

説明 37-25 ロケーション 37-25 基本 crashinfo 説明 37-25 ロケーション 37-25 コピー **B-6** 削除 **B-7** 内容の表示 **B-10** ファイル システム 使用可能なファイル システムの表示 **B-2** デフォルトの設定 **B-3** ネットワーク ファイル システム名 **B-6** 表示、ファイル情報 **B-4** ローカル ファイル システム名 **B-2** 不一致、自動ネゴシエーション 37-13 フィルタ、IP 「ACL」と「IP」を参照 フィルタリング show および more コマンド出力 2-10 非 IP トラフィック **31-43** フィルタリング、show および more コマンド出力 2-10 ブート ローダ アクセス 3-21 3-21 環境変数 説明 3-2 トラップドア メカニズム 3-2 プロンプト 3-21 複数認証 9-14 複数認証モード 設定 9-44 不正アクセスの防止 8-1 物理ポート 11-2 不適合マークダウン 1-14 プライオリティ CoS の上書き 15-7 CoS を信頼する 15-7 プライベート VLAN エッジ ポート 「保護ポート」を参照 プライマリ リンク 19-2

フラッシュデバイス、数 **B-2** フラッディング トラフィック、ブロッキング 23-8 プリエンプト遅延、デフォルト設定 19-9 プリエンプト、デフォルト設定 19-9 プルーニング、VTP イネーブル化 VTP ドメイン内 14-16 ポート上 13-19 概要 14-6 ディセーブル化 VTP ドメイン内 14-16 ポート上 13-20 例 14-6 プルーニング適格リスト VLAN 14-16 VTP プルーニング用 14-6 変更 13-19 フローチャート QoS 出力キューイングおよびスケジューリン 33-17 OoS 入力キューイングおよびスケジューリン ガ 33-15 OoS 分類 33-7 OoS ポリシングおよびマーキング 33-11 ブロードキャスト ストーム 23-1 フローベースのパケット分類 1-13 プロキシレポート 19-4 ブロッキング、パケット 23-8

ゝ

ヘルプ、コマンドライン 2-3
 編集機能
 イネーブル化およびディセーブル化 2-7
 使用するキーストローク 2-7
 ラップアラウンド機能で折り返された行 2-9

ほ

```
ポート
  VLAN 割り当て
              13-10
  アクセス
          11-3
  スイッチ
          11-2
  スタティック アクセス
                   13-4, 13-10
  セキュア
          23-9
  ダイナミック アクセス
                  13-4
  デュアルパーパス アップリンク
                        11-4
  トランク 13-4, 13-14
  ブロッキング
             23-8
  保護
        23-7
   11-3
ポート ACL、説明
              31-23
ポート VLAN ID TLV 26-2
ポートあたりのデバイスの最大数、ポートベース認
証
    9-37
ポート記述 TLV 26-2
ポートシャットダウン応答、VMPS 13-25
ポート集約プロトコル
  「EtherChannel」を参照
ポートセキュリティ
  QoS 信頼境界
              33-39
  違反
       23-11
  エージング 23-18
  スティッキー ラーニング
                    23-10
  設定
        23-13
  説明
        23-9
  他の機能との
             23-12
  デフォルト設定
               23-12
  トランク ポート上
                23-15
  表示
       23-20
ポートチャネル
  「EtherChannel」を参照
ポート プライオリティ
  MSTP 17-21
  STP 16-19
ポート ブロッキング
              1-4, 23-8
```

ポートベース認証 ACL および RADIUS Filter-Id アトリビュー 9-33 Ь EAPOL-Start フレーム 9-6 EAP-Request/Identity フレーム 9-6 EAP-Response/Identity フレーム 9-6 VLAN 割り当て AAA 許可 9-41 設定作業 **9-18** 説明 9-17 特性 9-17 Wake-on-LAN、説明 9-27 アカウンティング 9-15 アクセス不能認証バイパス 設定 9-55 説明 9-24 注意事項 9-37 イネーブル化 802.1x 認証 10-12 音声 VLAN PVID 9-25 VVID 9-25 説明 9-25 音声認識 802.1x セキュリティ 設定 9-39 説明 9-31, 9-39 開始およびメッセージ交換 9-6 カプセル化 9-3 クライアント、定義 9-3, 10-2 ゲスト VLAN 設定時の注意事項 9-22. 9-23 説明 9-22 柔軟な認証の順序設定 概要 9-30 設定 9-66 準備状態チェック 設定 9-38 説明 9-17, 9-38 スイッチ

RADIUS クライアント 9-3 プロキシとして 9-3, 10-2 スイッチ サプリカント 概要 9-31 設定 9-61 設定 802.1x 認証 9-41 RADIUS サーバ 9-44, 10-13 アクセス不能認証バイパス 9-55 違反モード 9-40 ~ 9-41 クライアントの手動での再認証 9-46 ゲスト VLAN 9-52 スイッチからクライアントへの再送信時 間 9-48 スイッチからクライアントへのフレーム再送信回 9-49, 9-50 数 スイッチ上の RADIUS サーバ パラメー 9-43, 10-12 タ 制限付き VLAN 9-53 待機時間 9-47 定期的な再認証 9-45 ホスト モード 9-44 設定時の注意事項 9-35, 10-9 説明 9-1 ダウンロード可能 ACL およびリダイレクト URL 概要 9-20 ~ 9-21 設定 9-63 ~ 9-65 デバイスの役割 9-3, 10-2 デフォルト設定 9-34, 10-9 デフォルト値へのリセット 9-68 統計の表示 9-68, 10-18 統計、表示 9-68 認証サーバ RADIUS サーバ 9-3 定義 9-3, 10-2 複数認証 9-14 方式リスト 9-41 ポート 音声 VLAN 9-25 許可および無許可 9-11

許可ステートおよび dot1x port-control コマン ĸ 9-11 ポートあたりのデバイスの最大数 9-37 ポート セキュリティ 音声 VLAN 9-27 説明 9-26 相互作用 9-26 マルチ ホスト モード 9-12 ホストモード **9-12** マジック パケット 9-27 ユーザ単位 ACL RADIUS サーバ アトリビュート 9-19 設定作業 9-19 説明 9-19 ユーザ ディストリビューション 概要 9-29 注意事項 9-29 ポートベース認証違反モードの設定 9-40 ~ 9-41 ポートベース認証方法、サポートされている 9-8 ポート メンバシップ モード、VLAN 13-4 保護ポート 1-10. 23-7 補助 VLAN 「音声 VLAN」を参照 ホスト、ダイナミック ポート上の制限 13-30 ホスト名、クラスタ 5-14 ポリサー 33-34 数 設定 一致したトラフィック クラスごと 33-49 複数のトラフィック クラス 33-54 説明 33-4 タイプ 33-10 表示 33-75 ポリシング 説明 33-4 トークン バケット アルゴリズム 33-10

ま

マーキング 集約ポリサーを使用するアクション 33-54 説明 33-4, 33-9 マクロ 「Auto SmartPort マクロ」を参照 「Smartport マクロ」を参照 マジック パケット 9-27 マルチキャスト TV アプリケーション 22-20 マルチキャスト VLAN 22-19 マルチキャスト グループ 加入 22-3 静的な加入 22-11, 35-8 即時脱退 22-6 脱退 22-5 マルチキャストストーム 23-1 マルチキャスト ルータ インターフェイス、モニ タ 22-18, 35-13 マルチキャスト ルータ ポート、追加 22-10, 35-9 マルチドメイン認証 「MDA」を参照

む

無許可ポート、IEEE 802.1x 9-11

め

メッセージ、ユーザへの、バナー経由 **6-19** メンバー スイッチ

管理 5-16自動検出 5-5

接続の回復 37-12

定義 5-2

パスワード **5-14**

要件 5-4

「候補スイッチ」、「クラスタ スタンバイ グループ」お よび「スタンバイ コマンド スイッチ」も参照 メンバシップ モード、VLAN ポート 13-4

ŧ

モジュール番号 11-11 モニタ CDP **25-5** Flex Link 19-16 IGMP スヌーピング 22-18, 35-13 フィルタ 22-32 IP SLA 動作 32-7 IPv4 ACL の設定 31-46 IPv6 **34-13** MAC アドレス テーブル移動更新 19-16 MVR 22-26 SFP ステータス 11-32, 37-14 VLAN 13-14 VMPS 13-30 VTP 14-18 アクセス グループ 31-46 インターフェイス 11-31 解析のためのネットワーク トラフィック (プローブ あり) 27-2 1-15 機能 スイッチ間で流れるトラフィック 28-1 速度およびデュプレックス モード 11-21 単一方向リンク用のケーブル 24-1 トラフィックの抑制 23-20 ポート ブロッキング 23-20 保護 23-20 マルチキャスト ルータ インターフェイス 22-18. 35-13

ゆ

ユーザ EXEC モード **2-2** ユーザ単位 ACL および Filter-Ids **9-9**

ユーザ名ベースの認証 8-7 ユニキャスト MAC アドレス フィルタリング 1-6 CPU パケット 6-31 スタティック アドレスの追加 6-31 設定時の注意事項 6-31 説明 6-31 マルチキャスト MAC アドレス 6-31 マルチキャストアドレス 6-31 ルータ MAC アドレス 6-31 ユニキャストストーム 23-1 ユニキャスト トラフィック、ブロッキング 23-8 ユニキャスト要求の転送 1-5

6

ライン コンフィギュレーション モード 2-3

り

る

```
ルート ガード
イネーブル化 18-17
サポート 1-8
説明 18-8
ルート スイッチ
MSTP 17-18
STP 16-16
STP
ルート ポート、定義 16-4
ループ ガード
イネーブル化 18-18
サポート 1-8
説明 18-10
```

れ

例	
ネットワークの構成 1-19	
レイヤ 2 traceroute	
ARP 37-17	
CDP 37-17	
IP アドレスおよびサブネット 37-17	
MAC アドレスおよび VLAN 37-17	
使用上のガイドライン 37-17	
説明 37-16	
ブロードキャスト トラフィック 37-16	
ポート上の複数のデバイス 37-17	
マルチキャストトラフィック 37-17	
ユニキャスト トラフィック 37-16	
レイヤ2インターフェイス、デフォルト設定	11-16
レイヤ2フレーム、CoSで分類 33-2	
レイヤ3インターフェイス	
IPv6 アドレスの割り当て 34-8	
レイヤ3機能 1-15	
レイヤ 3 パケット、分類方法 33-2	
レポート抑制、IGMP	
説明 22-6	

ろ

ディセーブル化 22-17, 35-12

ローカル SPAN 27-2 ログイン認証 RADIUS 8-30 TACACS+ 8-15 ログイン バナー 6-19 ログ メッセージ 「システム メッセージ ロギング」を参照 ログ メッセージのシーケンス番号 29-8 ログ メッセージのタイム スタンプ 29-8 ロケーション TLV 26-4, 26-9

わ

ワイヤード ロケーション サービス

概要 26-4 設定 26-11 表示 26-13 ロケーション TLV 26-4 I