

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 リリース 12.2(40)SE
改訂版 2007 年 9 月

Text Part Number: OL-8603-04-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。

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0708R)

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
© 2006-2007 Cisco Systems, Inc.
All rights reserved.

Copyright © 2006–2010, シスコシステムズ合同会社 .
All rights reserved.



CONTENTS

はじめに xxxi

対象読者 xxxi

目的 xxxi

表記法 xxxii

関連資料 xxxii

マニュアルの入手方法およびテクニカル サポート xxxiv

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 1-1

パフォーマンス向上機能 1-3

管理オプション 1-4

管理の簡易性に関する機能 1-4

アベイラビリティおよび冗長性に関する機能 1-6

VLAN 機能 1-6

セキュリティ機能 1-7

QoS および CoS 機能 1-9

モニタ機能 1-10

スイッチ初期設定後のデフォルト値 1-10

ネットワークの構成例 1-13

スイッチを使用する場合の設計概念 1-13

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 1-16

長距離広帯域トランスポートの構成 1-17

次の作業 1-18

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

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 2-10
コンソール接続または Telnet による CLI アクセス 2-10

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 3-1
起動プロセスの概要 3-1
スイッチ情報の割り当て 3-2
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 3-3
DHCP クライアントの要求プロセス 3-4
DHCP ベースの自動設定の設定 3-5
DHCP サーバ設定時の注意事項 3-5
TFTP サーバの設定 3-5
DNS の設定 3-6
リレー デバイスの設定 3-6
コンフィギュレーション ファイルの入手方法 3-7
構成例 3-8
手動でのスイッチ情報の割り当て 3-10
実行コンフィギュレーションの確認および保存 3-10
スタートアップ コンフィギュレーションの変更 3-11
起動のデフォルト設定 3-12
コンフィギュレーション ファイルの自動ダウンロード 3-12
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 3-12
手動で起動する場合 3-13
特定のソフトウェア イメージを起動する場合 3-14
環境変数の制御 3-14
ソフトウェア イメージ リロードのスケジュール設定 3-16
リロードのスケジュール設定 3-16
リロード スケジュール情報の表示 3-17

CHAPTER 4 Cisco IOS CNS エージェントの設定 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 4-3
DeviceID 4-4
ホスト名および DeviceID 4-4
ホスト名、DeviceID、ConfigID の使用方法 4-4
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 4-8
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 4-12
CNS 設定の表示 4-13

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 5-3
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 5-4
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 5-5
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 5-7
新しくインストールしたスイッチの検出 5-8
HSRP およびスタンバイ クラスタ コマンド スイッチ 5-9
仮想 IP アドレス 5-10
クラスタ スタンバイ グループに関する他の考慮事項 5-10
クラスタ設定の自動復旧 5-11
IP アドレス 5-12

ホスト名 5-12
パスワード 5-13
SNMP コミュニティ ストリング 5-13
TACACS+ および RADIUS 5-14
LRE プロファイル 5-14
CLI によるスイッチ クラスタの管理 5-14
Catalyst1900 および Catalyst2820 の CLI に関する考慮事項 5-14
SNMP によるスイッチ クラスタの管理 5-15

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 6-1
NTP の概要 6-2
NTP の設定 6-3
NTP のデフォルト設定 6-4
NTP 認証の設定 6-4
NTP アソシエーションの設定 6-5
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 6-10
NTP 設定の表示 6-11
手動での日時の設定 6-11
システム クロックの設定 6-12
日時設定の表示 6-12
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 6-15
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 6-16
DNS のデフォルト設定 6-17
DNS の設定 6-17
DNS の設定の表示 6-18
バナーの作成 6-18
バナーのデフォルト設定 6-18
MoTD ログイン バナーの設定 6-19
ログイン バナーの設定 6-20
MAC アドレス テーブルの管理 6-20
アドレス テーブルの作成 6-21

MAC アドレスおよび VLAN 6-21
MAC アドレス テーブルのデフォルト設定 6-22
アドレス エージング タイムの変更 6-22
ダイナミック アドレス エントリの削除 6-23
MAC アドレス通知トラップの設定 6-23
スタティック アドレス エントリの追加および削除 6-25
ユニキャスト MAC アドレス フィルタリングの設定 6-26
アドレス テーブル エントリの表示 6-27
ARP テーブルの管理 6-28

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 7-2
SDM テンプレートの設定 7-2
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 8-3
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
複数の権限レベルの設定 8-7
コマンドの権限レベルの設定 8-8
回線に対するデフォルトの権限レベルの変更 8-9
権限レベルへのログインおよび終了 8-9
TACACS+ によるスイッチ アクセスの制御 8-10
TACACS+ の概要 8-10
TACACS+ の動作 8-12
TACACS+ の設定 8-12
TACACS+ のデフォルト設定 8-13
TACACS+ サーバ ホストの特定および認証鍵の設定 8-13
TACACS+ ログイン認証の設定 8-14

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 8-16
TACACS+ アカウンティングの起動 8-17
TACACS+ 設定の表示 8-17
RADIUS によるスイッチ アクセスの制御 8-17
RADIUS の概要 8-18
RADIUS の動作 8-19
RADIUS の設定 8-19
RADIUS のデフォルト設定 8-20
RADIUS サーバ ホストの識別 8-20
RADIUS ログイン認証の設定 8-23
AAA サーバ グループの定義 8-25
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 8-27
RADIUS アカウンティングの起動 8-28
すべての RADIUS サーバの設定 8-29
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 8-29
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 8-31
RADIUS の設定の表示 8-32
スイッチのローカル認証および許可の設定 8-32
SSH のためのスイッチの設定 8-33
SSH の概要 8-33
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 8-34
制限事項 8-34
SSH の設定 8-34
設定時の注意事項 8-35
スイッチで SSH を実行するためのセットアップ 8-35
SSH サーバの設定 8-36
SSH の設定およびステータスの表示 8-37
SSL HTTP のためのスイッチの設定 8-37
セキュア HTTP サーバおよびクライアントの概要 8-38
CA の信頼点 8-38
CipherSuite 8-39
セキュア HTTP サーバおよびクライアントの設定 8-40
SSL のデフォルト設定 8-40
SSL の設定時の注意事項 8-40
CA の信頼点の設定 8-40
セキュア HTTP サーバの設定 8-41
セキュア HTTP クライアントの設定 8-43
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 8-44

SCP のためのスイッチの設定 8-44
Secure Copy に関する情報 8-44

CHAPTER 9 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 9-2
認証プロセス 9-3
認証の開始およびメッセージ交換 9-5
許可ステートおよび無許可ステートのポート 9-7
IEEE 802.1x のホスト モード 9-7
IEEE 802.1x アカウンティング 9-8
IEEE 802.1x アカウンティング アトリビュート値（AV）ペア 9-8
VLAN 割り当てを使用した IEEE 802.1x 認証の利用 9-9
ゲスト VLAN を使用した IEEE 802.1x 認証の利用 9-11
制限付き VLAN による IEEE 802.1x 認証の利用 9-12
アクセス不能認証バイパスによる IEEE 802.1x 認証の使用 9-13
音声 VLAN ポートを使用した IEEE 802.1x 認証の利用 9-14
ポート セキュリティを使用した IEEE 802.1x 認証の利用 9-14
WoL 機能を使用した IEEE 802.1x 認証の利用 9-15
MAC 認証バイパスを使用した IEEE 802.1x 認証の利用 9-16
NAC レイヤ 2 IEEE 802.1x 検証の利用 9-17
Web 認証の使用 9-17
自動 MAC チェックによる Web 認証 9-18
IEEE 802.1x 認証の設定 9-18
IEEE 802.1x 認証のデフォルト設定 9-19
IEEE 802.1x 認証設定時の注意事項 9-20
IEEE 802.1x 認証 9-20
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 9-21
MAC 認証バイパス 9-22
旧版のソフトウェア リリースからのアップグレード 9-22
IEEE 802.1x 認証の設定 9-22
スイッチおよび RADIUS サーバ間の通信の設定 9-23
ホスト モードの設定 9-25
定期的な再認証の設定 9-25
ポートに接続するクライアントの手動での再認証 9-26
待機時間の変更 9-26
スイッチからクライアントへの再送信時間の変更 9-27
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 9-28
再認証回数の設定 9-28

IEEE 802.1x アカウンティングの設定 9-29
ゲスト VLAN の設定 9-30
制限付き VLAN の設定 9-31
アクセス不能認証バイパス機能の設定 9-33
WoL を使用した IEEE 802.1x 認証の設定 9-35
MAC 認証バイパスの設定 9-36
NAC レイヤ 2 IEEE 802.1x 検証の設定 9-37
Web 認証の設定 9-38
ポート上での IEEE 802.1x 認証のディセーブル化 9-40
IEEE 802.1x 認証設定のデフォルト値へのリセット 9-41
IEEE 802.1x の統計情報およびステータスの表示 9-41

CHAPTER 10 インターフェイス特性の設定 10-1
インターフェイス タイプの概要 10-1
ポートベースの VLAN 10-2
スイッチ ポート 10-2
アクセス ポート 10-2
トランク ポート 10-3
EtherChannel ポート グループ 10-3
デュアルパーパス アップリンク ポート 10-4
インターフェイスの接続 10-5
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 10-5
インターフェイスの設定手順 10-6
インターフェイス範囲の設定 10-7
インターフェイス レンジ マクロの設定および使用方法 10-8
イーサネット インターフェイスの設定 10-10
イーサネット インターフェイスのデフォルト設定 10-11
デュアルパーパス アップリンク ポートのタイプの設定 10-12
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 10-13
速度とデュプレックス モードの設定時の注意事項 10-13
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 10-14
IEEE 802.3x フロー制御の設定 10-16
インターフェイスでの Auto-MDIX の設定 10-17
インターフェイスに関する記述の追加 10-18
システム MTU の設定 10-19
インターフェイスのモニタおよびメンテナンス 10-20
インターフェイス ステータスのモニタ 10-20
インターフェイスおよびカウンタのクリアとリセット 10-21
インターフェイスのシャットダウンおよび再起動 10-21

CHAPTER 11 SmartPort マクロの設定 11-1
SmartPort マクロの概要 11-1
SmartPort マクロの設定 11-2
SmartPort マクロのデフォルト設定 11-2
SmartPort マクロ設定時の注意事項 11-3
SmartPort マクロの作成 11-4
SmartPort マクロの適用 11-5
シスコのデフォルト SmartPort マクロの適用 11-6
SmartPort マクロの表示 11-8

CHAPTER 12 VLAN の設定 12-1
VLAN の概要 12-1
サポートされる VLAN 12-2
VLAN ポート メンバシップ モード 12-3
標準範囲 VLAN の設定 12-4
トークンリング VLAN 12-5
標準範囲 VLAN 設定時の注意事項 12-5
VLAN コンフィギュレーション モードのオプション 12-6
config-vlan モードでの VLAN 設定 12-6
VLAN データベース コンフィギュレーション モードでの VLAN 設定 12-6
VLAN 設定の保存 12-7
イーサネット VLAN のデフォルト設定 12-7
イーサネット VLAN の作成または変更 12-8
VLAN の削除 12-10
VLAN へのスタティック アクセス ポートの割り当て 12-11
拡張範囲 VLAN の設定 12-11
VLAN のデフォルト設定 12-12
拡張範囲 VLAN 設定時の注意事項 12-12
拡張範囲 VLAN の作成 12-13
VLAN の表示 12-14
VLAN トランクの設定 12-14
トランキングの概要 12-14
IEEE 802.1Q の設定に関する考慮事項 12-16
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 12-16
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 12-16
他の機能との相互作用 12-17
トランク ポートの設定 12-17
トランクでの許可 VLAN の定義 12-18
プルーニング適格リストの変更 12-20

タグなしトラフィック用ネイティブ VLAN の設定 12-20
トランク ポートの負荷分散の設定 12-21
STP ポート プライオリティによる負荷分散 12-21
STP パス コストによる負荷分散 12-23
VMPS の設定 12-24
VMPS の概要 12-25
ダイナミックアクセス ポート VLAN メンバシップ 12-25
VMPS クライアントのデフォルト設定 12-26
VMPS 設定時の注意事項 12-26
VMPS クライアントの設定 12-27
VMPS の IP アドレスの入力 12-27
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 12-27
VLAN メンバシップの再確認 12-28
再確認インターバルの変更 12-28
再試行回数の変更 12-29
VMPS のモニタ 12-29
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 12-30
VMPS の設定例 12-30

CHAPTER 13 **VTP の設定** 13-1
VTP の概要 13-1
VTP ドメイン 13-2
VTP モード 13-3
VTP アドバタイズ 13-3
VTP バージョン 2 13-4
VTP プルーニング 13-4
VTP の設定 13-7
VTP のデフォルト設定 13-7
VTP 設定オプション 13-7
グローバル コンフィギュレーション モードでの VTP 設定 13-7
VLAN データベース コンフィギュレーション モードでの VTP 設定 13-8
VTP 設定時の注意事項 13-8
ドメイン名 13-8
パスワード 13-9
VTP バージョン 13-9
設定要件 13-9
VTP サーバの設定 13-10
VTP クライアントの設定 13-11
VTP のディセーブル化（VTP トランスペアレント モード） 13-12

VTP バージョン 2 のイネーブル化 13-13
VTP プルーニングのイネーブル化 13-14
VTP ドメインへの VTP クライアント スイッチの追加 13-15
VTP のモニタ 13-16

CHAPTER 14 音声 VLAN の設定 14-1
音声 VLAN の概要 14-1
Cisco IP Phone の音声トラフィック 14-2
Cisco IP Phone のデータ トラフィック 14-2
音声 VLAN の設定 14-3
音声 VLAN のデフォルト設定 14-3
音声 VLAN 設定時の注意事項 14-3
Cisco7960 IP Phone に接続するポートの設定 14-4
Cisco IP Phone の音声トラフィックの設定 14-5
着信データ フレームのプライオリティ設定 14-6
音声 VLAN の表示 14-7

CHAPTER 15 STP の設定 15-1
スパニング ツリー機能の概要 15-1
STP の概要 15-2
スパニング ツリー トポロジと BPDU 15-3
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 15-4
スパニング ツリー インターフェイス ステート 15-4
ブロッキング ステート 15-6
リスニング ステート 15-6
ラーニング ステート 15-6
フォワーディング ステート 15-7
ディセーブル ステート 15-7
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 15-7
スパニング ツリーおよび冗長接続 15-8
スパニング ツリー アドレスの管理 15-8
接続を維持するためのエージング タイムの短縮 15-9
スパニング ツリー モードおよびプロトコル 15-9
サポートされるスパニング ツリー インスタンス 15-10
スパニング ツリーの相互運用性と下位互換性 15-10
STP および IEEE 802.1Q トランク 15-10
スパニング ツリー機能の設定 15-11
スパニング ツリー機能のデフォルト設定 15-11
スパニング ツリー設定時の注意事項 15-12

スパニング ツリー モードの変更 15-13
スパニング ツリーのディセーブル化 15-14
ルート スイッチの設定 15-15
セカンダリ ルート スイッチの設定 15-16
ポート プライオリティの設定 15-17
パス コストの設定 15-18
VLAN のスイッチ プライオリティの設定 15-20
スパニング ツリー タイマーの設定 15-20
Hello タイムの設定 15-21
VLAN の転送遅延時間の設定 15-22
VLAN の最大エージング タイムの設定 15-22
転送保留カウントの設定 15-23
スパニング ツリー ステータスの表示 15-23

CHAPTER 16 MSTP の設定 16-1
MSTP の概要 16-2
MST リージョン 16-2
IST、CIST、および CST 16-3
MST リージョン内の動作 16-3
MST リージョン間の動作 16-4
IEEE 802.1s の用語 16-5
ホップ カウント 16-6
境界ポート 16-6
IEEE 802.1s の実装 16-7
ポートの役割名の変更 16-7
レガシー スイッチと標準スイッチの相互運用 16-7
単一方向リンクの失敗の検出 16-8
IEEE 802.1D STP との相互運用性 16-9
RSTP の概要 16-9
ポートの役割およびアクティブ トポロジ 16-9
高速コンバージェンス 16-10
ポートの役割の同期化 16-12
BPDU のフォーマットおよびプロセス 16-13
優位 BPDU 情報の処理 16-13
下位 BPDU 情報の処理 16-14
トポロジの変更 16-14
MSTP 機能の設定 16-15
MSTP のデフォルト設定 16-15
MSTP 設定時の注意事項 16-16

MST リージョンの設定および MSTP のイネーブル化 16-16
ルート スイッチの設定 16-18
セカンダリ ルート スイッチの設定 16-19
ポート プライオリティの設定 16-20
パス コストの設定 16-21
スイッチ プライオリティの設定 16-22
Hello タイムの設定 16-23
転送遅延時間の設定 16-24
最大エージング タイムの設定 16-24
最大ホップ カウントの設定 16-25
リンク タイプの指定による高速移行の保証 16-25
ネイバ タイプの指定 16-26
プロトコル移行プロセスの再起動 16-26
MST コンフィギュレーションおよびステータスの表示 16-27

CHAPTER 17 **オプションのスパニング ツリー機能の設定 17-1**
オプションのスパニング ツリー機能の概要 17-1
PortFast の概要 17-2
BPDU ガードの概要 17-2
BPDU フィルタリングの概要 17-3
UplinkFast の概要 17-3
BackboneFast の概要 17-5
EtherChannel ガードの概要 17-7
ルート ガードの概要 17-8
ループ ガードの概要 17-9
オプションのスパニング ツリー機能の設定 17-9
オプションのスパニング ツリー機能のデフォルト設定 17-10
オプションのスパニング ツリー設定時の注意事項 17-10
PortFast のイネーブル化 17-10
BPDU ガードのイネーブル化 17-11
BPDU フィルタリングのイネーブル化 17-12
冗長リンク用 UplinkFast のイネーブル化 17-14
BackboneFast のイネーブル化 17-14
EtherChannel ガードのイネーブル化 17-15
ルート ガードのイネーブル化 17-16
ループ ガードのイネーブル化 17-16
スパニング ツリー ステータスの表示 17-17

CHAPTER 18 **Flex Link および MAC アドレス テーブル移動更新機能の設定** 18-1
Flex Link および MAC アドレス テーブル移動更新機能の概要 18-1
Flex Link 18-1
VLAN Flex Link ロード バランシングおよびサポート 18-2
MAC アドレス テーブル移動更新 18-3
Flex Link および MAC アドレス テーブル移動更新機能の設定 18-4
デフォルト設定 18-4
設定時の注意事項 18-5
Flex Link の設定 18-6
Flex Link の VLAN ロード バランシングの設定 18-8
MAC アドレス テーブル移動更新機能の設定 18-9
Flex Link および MAC アドレス テーブル移動更新のモニタ 18-11

CHAPTER 19 **DHCP 機能の設定** 19-1
DHCP 機能の概要 19-1
DHCP サーバ 19-2
DHCP リレー エージェント 19-2
DHCP スヌーピング 19-2
Option 82 データ挿入 19-3
DHCP スヌーピング バインディング データベース 19-5
DHCP 機能の設定 19-7
DHCP のデフォルト設定 19-7
DHCP スヌーピング設定時の注意事項 19-7
DHCP リレー エージェントの設定 19-9
DHCP スヌーピングおよび Option 82 のイネーブル化 19-9
Cisco IOS DHCP サーバ データベースのイネーブル化 19-11
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 19-11
DHCP スヌーピング情報の表示 19-12

CHAPTER 20 **IGMP スヌーピングおよび MVR の設定** 20-1
IGMP スヌーピングの概要 20-1
IGMP バージョン 20-3
マルチキャスト グループへの加入 20-3
マルチキャスト グループからの脱退 20-5
即時脱退 20-6
IGMP 脱退タイマーの設定 20-6
IGMP レポート抑制 20-6
IGMP スヌーピングの設定 20-7
IGMP スヌーピングのデフォルト設定 20-7

IGMP スヌーピングのイネーブル化およびディセーブル化 20-7
スヌーピング方法の設定 20-8
マルチキャスト ルータ ポートの設定 20-9
グループに加入するホストの静的な設定 20-10
IGMP 即時脱退のイネーブル化 20-11
IGMP 脱退タイマーの設定 20-11
TCN 関連のコマンドの設定 20-12
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 20-12
フラッディング モードからの回復 20-13
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 20-13
IGMP スヌーピング クエリアの設定 20-14
IGMP レポート抑制のディセーブル化 20-16
IGMP スヌーピング情報の表示 20-16
MVR の概要 20-18
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 20-19
MVR の設定 20-20
MVR のデフォルト設定 20-20
MVR 設定時の注意事項および制限事項 20-21
MVR グローバル パラメータの設定 20-21
MVR インターフェイスの設定 20-23
MVR 情報の表示 20-24
IGMP フィルタリングおよびスロットリングの設定 20-24
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 20-25
IGMP プロファイルの設定 20-26
IGMP プロファイルの適用 20-27
IGMP グループの最大数の設定 20-27
IGMP スロットリング アクションの設定 20-28
IGMP フィルタリングおよび IGMP スロットリング設定の表示 20-29

CHAPTER 21 **ポート単位のトラフィック制御の設定** 21-1
ストーム制御の設定 21-1
ストーム制御の概要 21-1
ストーム制御のデフォルト設定 21-3
ストーム制御およびしきい値レベルの設定 21-3
保護ポートの設定 21-5
保護ポートのデフォルト設定 21-6
保護ポート設定時の注意事項 21-6
保護ポートの設定 21-6
ポート ブロッキングの設定 21-7

ポート ブロッキングのデフォルト設定 21-7
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 21-7
ポート セキュリティの設定 21-8
ポート セキュリティの概要 21-8
セキュア MAC アドレス 21-8
セキュリティ違反 21-9
ポート セキュリティのデフォルト設定 21-10
ポート セキュリティの設定時の注意事項 21-11
ポート セキュリティのイネーブル化および設定 21-12
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 21-16
ポート単位のトラフィック制御設定の表示 21-18

CHAPTER 22 **CDP の設定** 22-1
CDP の概要 22-1
CDP の設定 22-2
CDP のデフォルト設定 22-2
CDP の特性の設定 22-2
CDP のディセーブル化およびイネーブル化 22-3
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 22-4
CDP のモニタおよびメンテナンス 22-4

CHAPTER 23 **LLDP および LLDP-MED の設定** 23-1
LLDP および LLDP-MED の概要 23-1
LLDP の概要 23-1
LLDP-MED の概要 23-2
LLDP および LLDP-MED の設定 23-3
デフォルト LLDP 設定 23-3
LLDP 特性の設定 23-4
LLDP のグローバルなディセーブル化およびイネーブル化 23-4
インターフェイス上での LLDP のディセーブル化およびイネーブル化 23-5
LLDP-MED TLV の設定 23-6
LLDP および LLDP-MED のモニタリングおよびメンテナンス 23-7

CHAPTER 24 **UDLD の設定** 24-1
UDLD の概要 24-1
動作モード 24-1
単一方向の検出方法 24-2
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 24-4
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 24-5
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 24-6
UDLD ステータスの表示 24-7

CHAPTER 25 **SPAN および RSPAN の設定** 25-1
SPAN および RSPAN の概要 25-1
ローカル SPAN 25-2
リモート SPAN 25-2
SPAN と RSPAN の概念および用語 25-3
SPAN セッション 25-3
モニタ対象トラフィック 25-4
送信元ポート 25-5
送信元 VLAN 25-6
VLAN フィルタリング 25-6
宛先ポート 25-6
RSPAN VLAN 25-7
SPAN および RSPAN と他の機能の相互作用 25-8
SPAN および RSPAN の設定 25-9
SPAN および RSPAN のデフォルト設定 25-9
ローカル SPAN の設定 25-9
SPAN 設定時の注意事項 25-10
ローカル SPAN セッションの作成 25-10
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 25-13
フィルタリングする VLAN の指定 25-15
RSPAN の設定 25-16
RSPAN 設定時の注意事項 25-17
RSPAN VLAN としての VLAN の設定 25-17
RSPAN 送信元セッションの作成 25-18
RSPAN 宛先セッションの作成 25-20
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 25-21
フィルタリングする VLAN の指定 25-23
SPAN および RSPAN のステータス表示 25-24

CHAPTER 26 **RMON の設定** 26-1
RMON の概要 26-1
RMON の設定 26-2
RMON のデフォルト設定 26-3

RMON アラームおよびイベントの設定 26-3
インターフェイス上でのグループ履歴統計情報の収集 26-5
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 26-5
RMON ステータスの表示 26-6

CHAPTER 27 システム メッセージ ロギングの設定 27-1
システム メッセージ ロギングの概要 27-1
システム メッセージ ロギングの設定 27-2
システム ログ メッセージのフォーマット 27-2
システム メッセージ ロギングのデフォルト設定 27-3
メッセージ ロギングのディセーブル化 27-4
メッセージ表示宛先デバイスの設定 27-5
ログ メッセージの同期化 27-6
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 27-7
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 27-8
メッセージ重大度の定義 27-8
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 27-10
設定変更ロガーのイネーブル化 27-11
UNIX Syslog サーバの設定 27-12
UNIX Syslog デーモンへのログ メッセージ 27-12
UNIX システム ロギング ファシリティの設定 27-12
ロギング設定の表示 27-14

CHAPTER 28 SNMP の設定 28-1
SNMP の概要 28-1
SNMP バージョン 28-2
SNMP マネージャ機能 28-3
SNMP エージェント機能 28-4
SNMP コミュニティ ストリング 28-4
SNMP を使用して MIB 変数にアクセスする方法 28-4
SNMP 通知 28-5
SNMP ifIndex MIB オブジェクト値 28-6
SNMP の設定 28-6
SNMP のデフォルト設定 28-7
SNMP 設定時の注意事項 28-7
SNMP エージェントのディセーブル化 28-8
コミュニティ ストリングの設定 28-8
SNMP グループおよびユーザの設定 28-10
SNMP 通知の設定 28-12

エージェント コンタクトおよびロケーションの設定 28-16
SNMP を通して使用する TFTP サーバの制限 28-16
SNMP の例 28-17
SNMP ステータスの表示 28-18

CHAPTER 29 **ACL によるネットワーク セキュリティの設定 29-1**
ACL の概要 29-1
ポート ACL 29-2
フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理 29-3
IPv4 ACL の設定 29-4
標準 IPv4 ACL および拡張 IPv4 ACL の作成 29-5
アクセス リスト番号 29-6
番号付き標準 ACL の作成 29-7
番号付き拡張 ACL の作成 29-8
ACL 内の ACE の並べ替え 29-12
名前付き標準 ACL および名前付き拡張 ACL の作成 29-12
ACL での時間範囲の使用 29-14
ACL へのコメントの挿入 29-15
端末回線への IPv4 ACL の適用 29-16
インターフェイスへの IPv4 ACL の適用 29-17
ハードウェアおよびソフトウェアによる IP ACL の処理 29-17
IPv4 ACL の設定例 29-18
番号付き ACL 29-18
拡張 ACL 29-18
名前付き ACL 29-19
IP ACL に適用される時間範囲 29-19
コメント付きの IP ACL エントリ 29-19
名前付き MAC 拡張 ACL の作成 29-20
レイヤ 2 インターフェイスへの MAC ACL の適用 29-21
IPv4 ACL の設定の表示 29-22

CHAPTER 30 **Cisco IOS IP SLA 動作の設定 30-1**
Cisco IOS IP SLA の概要 30-1
Cisco IOS IP SLA によるネットワーク パフォーマンスの測定 30-2
IP SLA Responder と IP SLA コントロール プロトコル 30-3
IP SLA の応答時間の計算 30-4
IP SLA 動作の設定 30-5
デフォルト設定 30-5

設定時の注意事項 30-5
IP SLA Responder の設定 30-6
IP SLA 動作のモニタリング 30-7

CHAPTER 31 QoS の設定 31-1
QoS の概要 31-1
QoS の基本モデル 31-3
分類 31-5
QoS ACL に基づく分類 31-7
クラス マップおよびポリシー マップに基づく分類 31-8
ポリシングおよびマーキング 31-8
物理ポートのポリシング 31-9
マッピング テーブル 31-10
キューイングおよびスケジューリングの概要 31-11
WTD 31-12
SRR のシェーピングおよび共有 31-12
入力キューでのキューイングおよびスケジューリング 31-13
出力キューでのキューイングおよびスケジューリング 31-16
パケットの変更 31-19
自動 QoS の設定 31-19
生成される自動 QoS 設定 31-20
コンフィギュレーションにおける自動 QoS の影響 31-24
自動 QoS 設定時の注意事項 31-24
VoIP 用自動 QoS のイネーブル化 31-25
自動 QoS 設定例 31-27
自動 QoS 情報の表示 31-29
標準 QoS の設定 31-29
標準 QoS のデフォルト設定 31-29
入力キューのデフォルト設定 31-30
出力キューのデフォルト設定 31-31
マッピング テーブルのデフォルト設定 31-31
標準 QoS 設定時の注意事項 31-32
QoS ACL の注意事項 31-32
ポリシングの注意事項 31-32
一般的な QoS の注意事項 31-33
QoS のグローバルなイネーブル化 31-33
ポートの信頼状態による分類の設定 31-34
QoS ドメイン内のポートの信頼状態の設定 31-34
インターフェイスの CoS 値の設定 31-36

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 31-36
DSCP 透過モードのイネーブル化 31-38
別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定 31-38
QoS ポリシーの設定 31-40
ACL によるトラフィックの分類 31-41
クラス マップによるトラフィックの分類 31-44
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 31-46
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 31-50
DSCP マップの設定 31-53
CoS/DSCP マップの設定 31-53
IP precedence/DSCP マップの設定 31-54
ポリシング済み DSCP マップの設定 31-55
DSCP/CoS マップの設定 31-56
DSCP/DSCP 変換マップの設定 31-57
入力キューの特性の設定 31-58
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 31-59
入力キュー間のバッファ スペースの割り当て 31-60
入力キュー間の帯域幅の割り当て 31-61
入力プライオリティ キューの設定 31-61
出力キューの特性の設定 31-62
設定時の注意事項 31-63
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 31-63
出力キューおよび ID への DSCP または CoS 値のマッピング 31-65
出力キューでの SRR シェーピング重みの設定 31-66
出力キューでの SRR 共有重みの設定 31-67
出力緊急キューの設定 31-68
出力インターフェイスの帯域幅の制限 31-69
標準 QoS 情報の表示 31-70

CHAPTER 32 **IPv6 ホスト機能の設定** 32-1
IPv6 の概要 32-1
IPv6 アドレス 32-2
サポート対象の IPv6 ユニキャスト ルーティング機能 32-3
128 ビット幅のユニキャスト アドレス 32-3
IPv6 用 DNS 32-4
ICMPv6 32-4
近接ディスカバリ 32-4

IPv6 のステートレス自動設定および重複アドレス検出 32-5
IPv6 アプリケーション 32-5
デュアル IPv4/IPv6 プロトコル スタック 32-6
SDM テンプレート 32-6
デュアル IPv4/IPv6 SDM テンプレート 32-7
IPv6 の設定 32-8
IPv6 のデフォルト設定 32-8
IPv6 ICMP レート制限の設定 32-8
IPv6 のスタティック ルートの設定 32-9
IPv6 の表示 32-11

CHAPTER 33 **IPv6 MLD スヌーピングの設定** 33-1
MLD スヌーピングの概要 33-1
MLD メッセージ 33-2
MLD クエリー 33-3
マルチキャスト クライアント エージングの堅牢性 33-3
マルチキャスト ルータ検出 33-3
MLD レポート 33-4
MLD Done メッセージおよび即時脱退 33-4
TCN 処理 33-5
IPv6 MLD スヌーピングの設定 33-5
MLD スヌーピングのデフォルト設定 33-5
MLD スヌーピング設定時の注意事項 33-6
MLD スヌーピングのイネーブル化またはディセーブル化 33-6
スタティックなマルチキャスト グループの設定 33-8
マルチキャスト ルータ ポートの設定 33-8
MLD 即時脱退のイネーブル化 33-9
MLD スヌーピング クエリーの設定 33-10
MLD リスナー メッセージ抑制のディセーブル化 33-11
MLD スヌーピング情報の表示 33-11

CHAPTER 34 **EtherChannel およびリンクステート トラッキングの設定** 34-1
EtherChannel の概要 34-1
EtherChannel の概要 34-2
ポートチャネル インターフェイス 34-3
ポート集約プロトコル 34-4
PAgP モード 34-4
PAgP と他の機能との相互作用 34-5
LACP 34-5

LACP モード 34-5
LACP と他の機能との相互作用 34-6
EtherChannel の On モード 34-6
ロードバランシングおよび転送方式 34-6
EtherChannel の設定 34-8
EtherChannel のデフォルト設定 34-9
EtherChannel 設定時の注意事項 34-9
レイヤ 2 EtherChannel の設定 34-10
EtherChannel ロードバランシングの設定 34-13
PAgP 学習方式およびプライオリティの設定 34-14
LACP ホット スタンバイ ポートの設定 34-15
LACP システム プライオリティの設定 34-16
LACP ポート プライオリティの設定 34-16
EtherChannel、PAgP、および LACP ステータスの表示 34-17
リンクステート トラッキングの概要 34-18
リンクステート トラッキングの設定 34-20
デフォルトのリンクステート トラッキングの設定 34-21
リンクステート トラッキングの設定時の注意事項 34-21
リンクステート トラッキングの設定 34-21
リンクステート トラッキング ステータスの表示 34-22

CHAPTER 35 トラブルシューティング 35-1
ソフトウェアで障害が発生した場合の回復 35-2
パスワードを忘れた場合の回復 35-3
パスワード回復がイネーブルになっている場合の手順 35-4
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 35-6
コマンド スイッチで障害が発生した場合の回復 35-7
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 35-8
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 35-9
クラスタ メンバー スイッチとの接続の回復 35-11
自動ネゴシエーションの不一致の防止 35-11
SFP モジュールのセキュリティと識別 35-12
SFP モジュール ステータスのモニタリング 35-12
ping の使用 35-12
ping の概要 35-13
ping の実行 35-13
レイヤ 2 traceroute の使用 35-14
レイヤ 2 traceroute の概要 35-14

使用上のガイドライン 35-14
物理パスの表示 35-15
IP traceroute の使用 35-15
IP traceroute の概要 35-15
IP traceroute の実行 35-16
TDR の使用 35-17
TDR の概要 35-17
TDR の実行および結果の表示 35-18
debug コマンドの使用 35-18
特定機能に関するデバッグのイネーブル化 35-18
システム全体診断のイネーブル化 35-19
デバッグおよびエラー メッセージ出力のリダイレクト 35-19
show platform forward コマンドの使用 35-20
crashinfo ファイルの使用 35-21
基本 crashinfo ファイル 35-21
拡張 crashinfo ファイル 35-22

APPENDIX A サポート対象 MIB 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

APPENDIX 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 B-1
フラッシュ ファイル システムの操作 B-1
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 B-3
ディレクトリの変更および作業ディレクトリの表示 B-3
ディレクトリの作成および削除 B-4
ファイルのコピー B-4
ファイルの削除 B-5
tar ファイルの作成、表示、および抽出 B-5
tar ファイルの作成 B-6
tar ファイルの内容の表示 B-6
tar ファイルの抽出 B-7
ファイルの内容の表示 B-7
コンフィギュレーション ファイルの操作 B-8
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-9
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-9

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-10
TFTP によるコンフィギュレーション ファイルのコピー B-10
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 B-10
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-11
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-12
FTP によるコンフィギュレーション ファイルのコピー B-12
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備 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 B-13
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-15
RCP によるコンフィギュレーション ファイルのコピー B-16
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-16
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-17
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-18
設定情報の消去 B-19
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-19
格納されたコンフィギュレーション ファイルの削除 B-19
コンフィギュレーションの交換またはロール バック B-19
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-20
設定時の注意事項 B-21
コンフィギュレーション アーカイブの設定 B-21
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-22
ソフトウェア イメージの操作 B-23
スイッチ上のイメージの場所 B-24
サーバまたは Cisco.com 上のイメージの tar ファイル形式 B-25
TFTP によるイメージ ファイルのコピー B-25
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-26
TFTP によるイメージ ファイルのダウンロード B-27
TFTP によるイメージ ファイルのアップロード B-28
FTP によるイメージ ファイルのコピー B-29
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-29
FTP によるイメージ ファイルのダウンロード B-30
FTP によるイメージ ファイルのアップロード B-33
RCP によるイメージ ファイルのコピー B-34
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-34
RCP によるイメージ ファイルのダウンロード B-35
RCP によるイメージ ファイルのアップロード B-37

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-5

APPENDIX D Cisco IOS リリース 12.2(40)SE でサポートされていないコマンド D-1
ACL D-1
サポートされていない特権 EXEC コマンド D-1
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-1
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-1
ブート ローダ コマンド D-2
サポートされていないユーザ 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
組み込みイベントマネージャ 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
アプレット コンフィギュレーション モードでサポートされていないコマンド D-2
debug コマンド D-2
サポートされていない特権 EXEC コマンド D-2
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-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-4
その他 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
NAT 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
QoS D-5
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-5
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-5
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 D-5
RADIUS D-5
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-5

SNMP D-5
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-5
スパニング ツリー D-6
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-6
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-6
VLAN D-6
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-6
サポートされていない vlan-config コマンド D-6
サポートされていないユーザ EXEC コマンド D-6
VTP D-6
サポートされていない特権 EXEC コマンド D-6

INDEX



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 モジュール*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 QoS（Quality Of Service）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、Catalyst 2960 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。

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

関連資料

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

（注） 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。

印刷資料は、Cisco.com または電話で、DOC-xxxxxx= という番号を使用して発注できます。電話番号については、「マニュアルの入手方法およびテクニカル サポート」（P.xxxiv）を参照してください。

- 『*Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches*』（発注はできませんが、Cisco.com から入手できます）
- 『*Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide*』（発注はできませんが、Cisco.com から入手できます）
- 『*Catalyst 2960 Switch Software Configuration Guide*』（発注はできませんが、Cisco.com から入手できます）
- 『*Catalyst 2960 Switch Command Reference*』（発注はできませんが、Cisco.com から入手できます）
- 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*』（発注はできませんが、Cisco.com から入手できます）
- 『*Catalyst 2960 Switch Getting Started Guide*』（Customer Order Number DOC-7816879=）
- 『*Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*』（Customer Order Number DOC-7816880=）
- 『*Getting Started with Cisco Network Assistant*』（発注はできませんが、Cisco.com から入手できます）
- 『*Release Notes for Cisco Network Assistant*』（発注はできませんが、Cisco.com から入手できます）
- 『*Cisco Small Form-Factor Pluggable Modules Installation Notes*』（Customer Order Number DOC-7815160=）
- 『*Cisco RPS 300 Redundant Power System Hardware Installation Guide*』（Customer Order number DOC-7810372=）
- 『*Cisco RPS 675 Redundant Power System Hardware Installation Guide*』（Customer Order number DOC-7815201=）
- 『*Cisco Redundant Power System 2300 Hardware Installation Guide*』（Customer Order number DOC-7817647=）
- Network Admission Control（NAC）の詳細については、『*Network Admission Control Software Configuration Guide*』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）。
- 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*』（発注はできませんが、Cisco.com から入手できます）
  - 『*Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*』（発注はできませんが、Cisco.com から入手できます）
  - 『*Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*』（発注はできませんが、Cisco.com から入手できます）
  - 『*Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*』（発注はできませんが、Cisco.com から入手できます）

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



CHAPTER 1

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。内容は次の通りです。

- 「機能」（P.1-1）
- 「スイッチ初期設定後のデフォルト値」（P.1-10）
- 「ネットワークの構成例」（P.1-13）
- 「次の作業」（P.1-18）

このマニュアルでは、IP は IP Version 4（IPv4）を意味します。

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）バージョンのみに対応しています。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。

スイッチの機能は、次のとおりです。

- 「使用および導入を簡素化する機能」（P.1-1）
- 「パフォーマンス向上機能」（P.1-3）
- 「管理オプション」（P.1-4）
- 「管理の簡易性に関する機能」（P.1-4）（ソフトウェアの暗号化バージョンが必要な機能を含む）
- 「アベイラビリティおよび冗長性に関する機能」（P.1-6）
- 「VLAN 機能」（P.1-6）
- 「セキュリティ機能」（P.1-7）（ソフトウェアの暗号化バージョンが必要な機能を含む）
- 「QoS および CoS 機能」（P.1-9）
- 「モニタ機能」（P.1-10）

使用および導入を簡素化する機能

スイッチには、使用と導入を容易にするため、次の機能が搭載されています。

- 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。
  - 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。
- 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。
  - 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。

パフォーマンス向上機能

スイッチには、次の機能が搭載されています。

- 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。
- 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。
- 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。

- Cisco IOS IP Service Level Agreements （SLA）は、Cisco IOS ソフトウェアの一部で、アクティブなトラフィックをモニタリングしてネットワーク パフォーマンスを測定します。Cisco IOS IP SLA responder をサポートし、システムがネットワーク パフォーマンスをモニタリングするために Cisco IOS IP SLA の要求パケットを予期して応答することが可能になります。Responder の設定については、リリースノートを参照してください。

管理オプション

次のオプションは、スイッチの設定と管理を実行します。

- 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 28 章「SNMP の設定」を参照してください。
- CNS：Cisco Networking Services 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。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 CNS エージェントの設定」を参照してください。

管理の簡易性に関する機能

次に、管理の簡易性に関する機能を示します。

- 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。
- 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。
- 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 デバイスへロケーション情報を提供する LLDP メディア拡張（LLDP-MED）ロケーション TLV。
- 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。
- 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。
- これらの IP サービスをサポートし VRF 認識を行って、次のような複数のルーティング インスタンスを稼動できます。HSRP、GLBP、uRPF、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute および ping。
- 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（ソフトウェアの暗号化バージョンが必要）。
- 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）。
- 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。

アベイラビリティおよび冗長性に関する機能

アベイラビリティおよび冗長性に関する機能を次に示します。

- 拡張オブジェクト トラッキング機能は HSRP とトラッキング メカニズムを分離し、HSRP 以外のプロセスで使用可能な個別のスタンドアロン型トラッキング プロセスを作成します。
- Unidirectional Link Detection（UDLD; 単一方向リンク検出）およびアグレッシブ UDLD。光ファイバ ケーブルの配線ミスまたはポート障害に起因する光ファイバ インターフェイス上の単一方向リンクを検出し、ディセーブルにします。
- IEEE 802.1D Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）による冗長バックボーン接続およびループフリー ネットワーク。STP には次の機能があります。
  - 最大 128 のスパニング ツリー インスタンスをサポート。
  - Per-VLAN Spanning-Tree Plus（PVST+）による VLAN 間でのロードバランシング。
  - Rapid PVST+ による、VLAN 間でのロードバランシングおよびスパニング ツリー インスタンスの高速コンバージェンスの実現。
  - 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。
- 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。
- Cisco RPS 300 および Cisco RPS 675 による RPS サポート。電源の信頼性が向上します。

VLAN 機能

次に、VLANに関する機能を示します。

- 最大 255 個の VLAN をサポート。適切なネットワーク リソース、トラフィック パターン、および帯域幅を対応付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 規格で認められている 1 ～ 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。

セキュリティ機能

スイッチには、次のセキュリティ機能が搭載されています。

- 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。
- 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。
- 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 access control list（ACL; アクセス コントロール リスト）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。
- 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。
  - MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
  - VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
  - ポート セキュリティ。IEEE 802.1x ポートへのアクセスを制御します。
  - 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
  - IP Phone 検出機能拡張。Cisco IP Phone を検出し識別します。
  - ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
  - 制限付き VLAN。IEEE 802.1x に準拠はしているが、標準の IEEE 802.1x で認証するための証明書を持っていないユーザに制限付きのサービスを提供します。
  - IEEE 802.1x アカウンティング。ネットワーク使用をトラッキングします。
  - IEEE 802.1x と LAN のウェイクアップ機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
- MAC 認証バイパス。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します。
- 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 NAC レイヤ 2 IEEE 802.1x 検証。

  NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 IEEE 802.1x 検証の設定」（P.9-37）を参照してください。
- Terminal Access Controller Access Control System Plus（TACACS+）。TACACS サーバを介してネットワーク セキュリティを管理する独自の機能です。
- 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）。

QoS および CoS 機能

次に、QoS および CoS 機能を示します。

- auto-QoS（自動 QoS）。トラフィックの分類と出力キューの設定を自動化することで既存の QoS 機能の展開を簡略化します。
- 分類
  - IP Type of Service/Differentiated Services Code Point（IP ToS/DSCP）および IEEE 802.1p CoS のポート単位でのプライオリティ設定。ミッション クリティカルなアプリケーションのパフォーマンスを保護します。
  - IP ToS/DSCP および IEEE 802.1p CoS（サービス クラス）のフローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダーに含まれる情報に基づく）によるマーキング。ネットワーク エッジで高性能な QoS 機能を提供し、ネットワーク トラフィックのタイプ別に差別化されたサービス レベルを可能にするとともに、ネットワーク上のミッション クリティカルなトラフィックにプライオリティを設定します。
  - QoS ドメイン内および別の QoS ドメインとの境界ポートにおける、trusted（信頼性のある）ポート ステート（CoS、DSCP、および IP precedence）。
  - 信頼境界機能。Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを確保します。
- ポリシング
  - 特定のトラフィック フローに対してどの程度のポート帯域幅を割り当てるかを管理する、スイッチ ポート上のトラフィック ポリシング ポリシー。
  - Cisco IOS Release 12.2(25)SED 以降では、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。
  - 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）。
- 出力キューおよびスケジューリング
  - 1 ポートに 4 つの出力キュー。
  - 輻輳回避メカニズムとしての WTD。キュー長を管理し、トラフィックの分類ごとに異なる廃棄優先順位を設定します。
  - スケジューリング サービスとしての SRR。キューからパケットを出して出力インターフェイスに入れる速度を指定します（出力キューではシェーピングおよび共有がサポートされます）。シェーピング型出力キューは、ポート帯域幅の割り当てが保証されますが、割り当てられた

ポート帯域幅の使用に制限されています。共有型出力キューは、設定された帯域幅の割り当てが保証されるだけではなく、他のキューが空になり、その割り当て分の帯域幅が使用されない場合、保証された割り当てより多く使用できます。

モニタ機能

次に、モニタ機能を示します。

- 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 19 章「DHCP 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 19 章「DHCP 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 10 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 10 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 10 章「インターフェイス特性の設定」を参照してください。
- SmartPort マクロは定義されていません。詳細は、第 11 章「SmartPort マクロの設定」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 12 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 12 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 12 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 13 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 13 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 14 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 15 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 16 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 17 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 18 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。
- 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 19 章「DHCP 機能の設定」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 20 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 20 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 20 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 20 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 21 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 21 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 21 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 21 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 22 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 25 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルに設定されています。詳細は、第 26 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 27 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 28 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 29 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 31 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 34 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.1-13）
- 「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.1-16）
- 「長距離広帯域トランスポートの構成」（P.1-17）

スイッチを使用する場合の設計概念

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

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

表 1-1　ネットワーク パフォーマンスの向上

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

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

表 1-2　ネットワーク サービスの提供

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

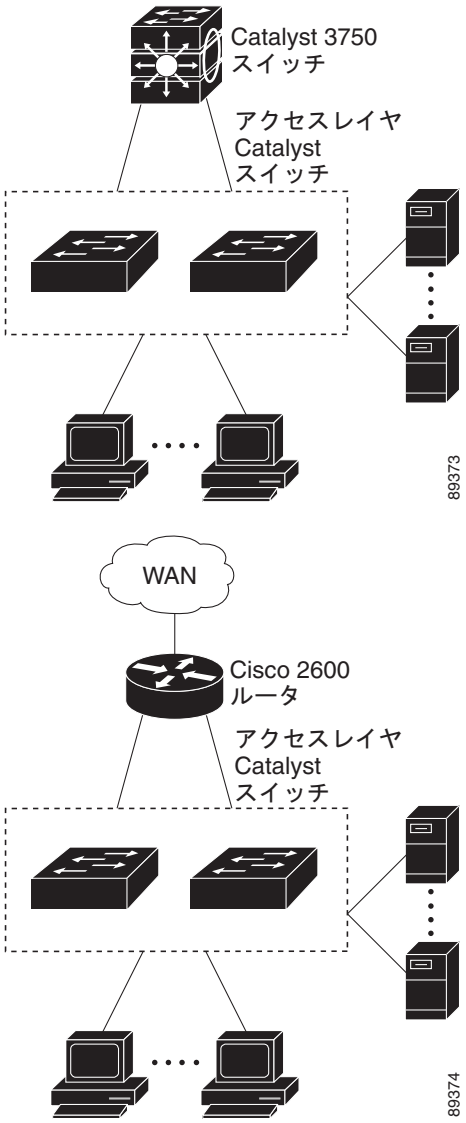
スイッチを使用して、以下を作成できます。

- 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 2960 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。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）



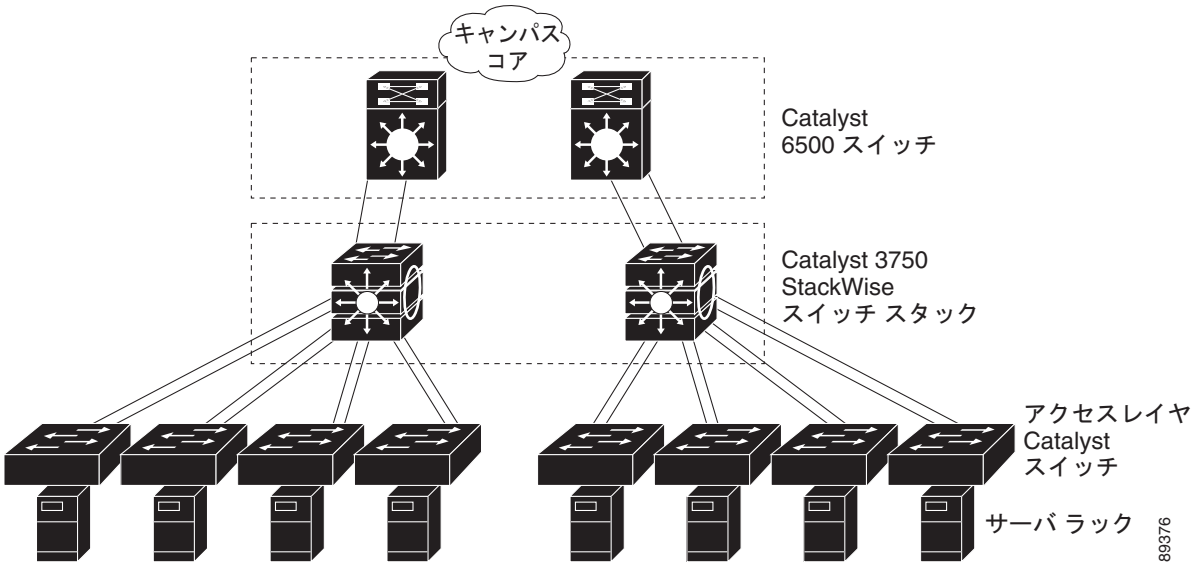
- サーバ集約（図 1-2）：スイッチを使用して、サーバ グループを相互接続し、ネットワークの物理的なセキュリティと管理を一元化できます。ディストリビューション レイヤで高速 IP 転送を実現するには、アクセス レイヤ スイッチを、ルーティング機能を備えたマルチレイヤ スイッチに接続します。ギガビットの相互接続によって、データ フローの遅延を最小限に抑えることができます。

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 を有する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。

図 1-2　サーバ集約



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 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2960 。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。

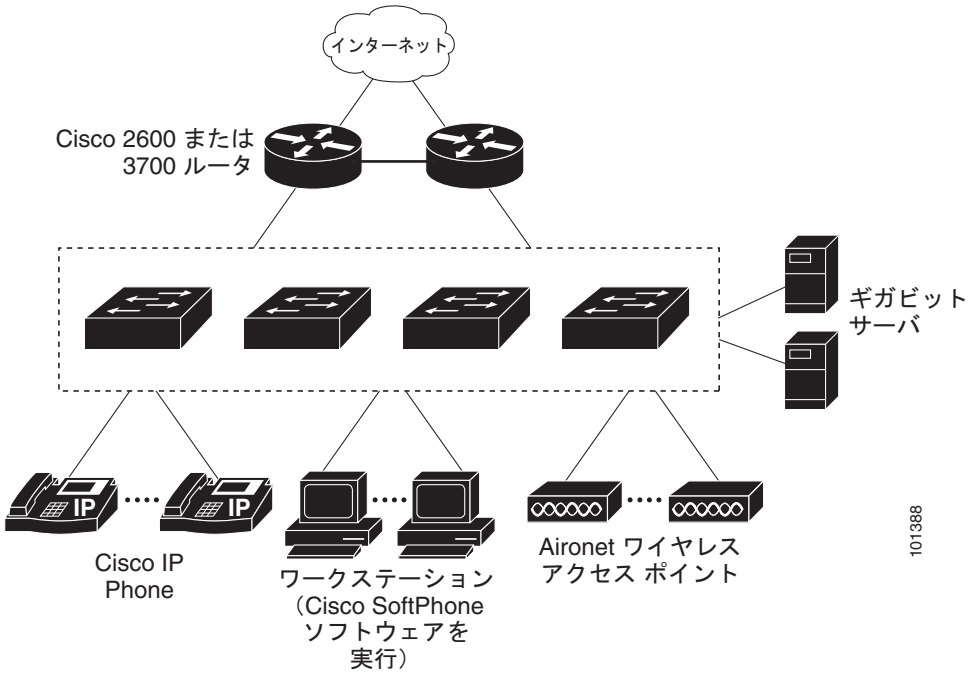
ある VLAN のエンド ステーションが別の VLAN にあるエンド ステーションと通信する必要がある場合、ルータが宛先 VLAN にトラフィックをルーティングします。このネットワークでは、ルータが VLAN 間ルーティングを行います。スイッチ上の VLAN ACL（VLAN マップ）が VLAN 内セキュリティを設定し、不正ユーザがネットワークの重要な領域にアクセスしないようにします。

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　　Catalyst 2960 スイッチ（コラプスト バックボーン設定）



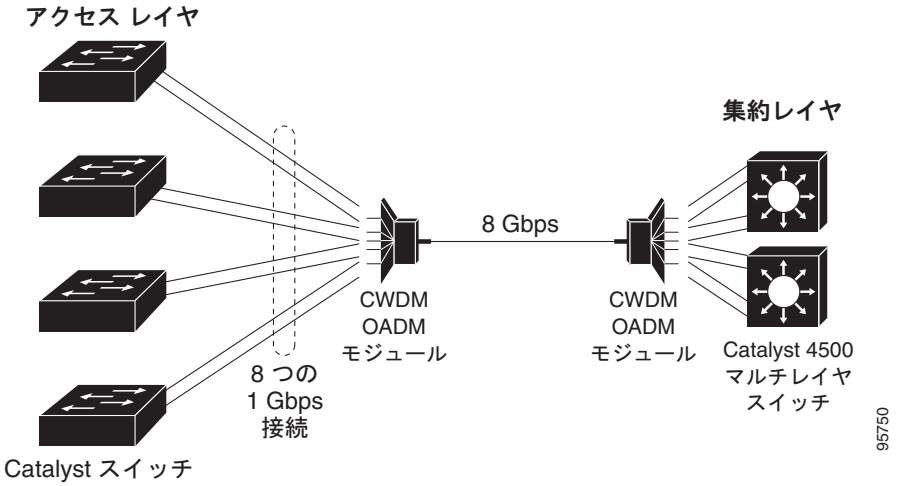
長距離広帯域トランスポートの構成

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。

図 1-4　　長距離広帯域トランスポートの構成



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 2960 スイッチを設定するための Cisco IOS 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。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.2-10）

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始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、**Ctrl+Z** を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
config-vlan	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	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.10-5）を参照してください。 同じパラメータを指定して複数のインターフェイスを設定する場合は、「インターフェイス範囲の設定」（P.10-7）を参照してください。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**linevty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

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

ヘルプ システムの概要

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

表 2-2　ヘルプの概要 （続き）

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

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

コマンドの省略形

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

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

```
Switch# show conf
```

コマンドの no 形式および default 形式の概要

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。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギングの使用方法

Cisco IOS Release 12.2(25)SED 以降では、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/switches/lan/catalyst2960/software/release/12.2_40_se/configuration/guide/swlog.html

（注） 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 10 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。 （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。	**Return** キーを押します。	1 行下へスクロールします。
	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 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わったあと、**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グ

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

この機能を使用するには、**show** または **more** コマンドを入力したあと、*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.8-33）を参照してください。スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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



CHAPTER 3

スイッチの 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.3-1）
- 「スイッチ情報の割り当て」（P.3-2）
- 「実行コンフィギュレーションの確認および保存」（P.3-10）
- 「スタートアップ コンフィギュレーションの変更」（P.3-11）
- 「ソフトウェア イメージ リロードのスケジュール設定」（P.3-16）

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）を行う必要があります。

通常の起動プロセスにはブートローダ ソフトウェアの動作が含まれます。ブート ローダは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。
- システム ボード上のフラッシュ ファイル システムを初期化します。
- デフォルトの OS（オペレーティング システム）ソフトウェアをメモリにロードし、スイッチを起動します。

ブート ローダによってフラッシュ ファイル システムにアクセスしてから、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.35-2）および「パスワードを忘れた場合の回復」（P.35-3）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。

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

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

スイッチ情報の割り当て

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。

ここでは、次の設定情報について説明します。

- 「デフォルトのスイッチ情報」（P.3-3）
- 「DHCP ベースの自動設定の概要」（P.3-3）
- 「手動でのスイッチ情報の割り当て」（P.3-10）

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。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。

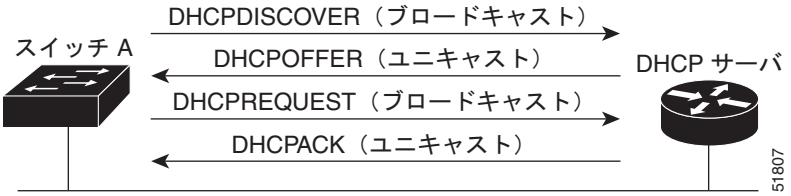
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

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/サーバ間のメッセージ交換



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

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

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。スイッチ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.3-5）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（DHCP サーバがパラメータを別のクライアントに割り当てた）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 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クライアント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 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.3-5）
- 「TFTP サーバの設定」（P.3-5）
- 「DNS の設定」（P.3-6）
- 「リレー デバイスの設定」（P.3-6）
- 「コンフィギュレーション ファイルの入手方法」（P.3-7）
- 「構成例」（P.3-8）

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。

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）
- DNS サーバの IP アドレス（任意）
- 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）

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。

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.3-6）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。

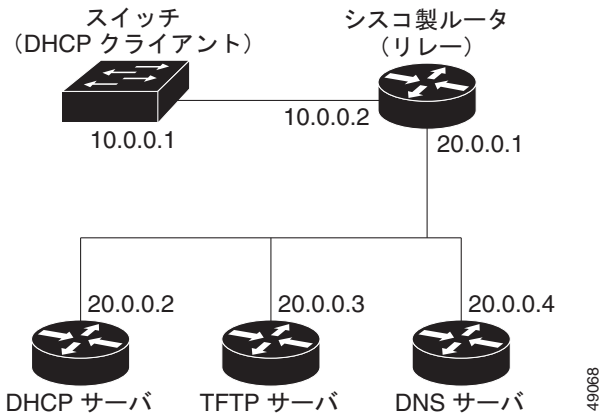
インターフェイス 10.0.0.2 の場合

```
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
```

図 3-2　自動設定でのリレー デバイスの使用



コンフィギュレーション ファイルの入手方法

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

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

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

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

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

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

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

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

  デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手したあと、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。

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

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。

図 3-3　DHCP ベースの自動設定を使用するネットワークの構成例

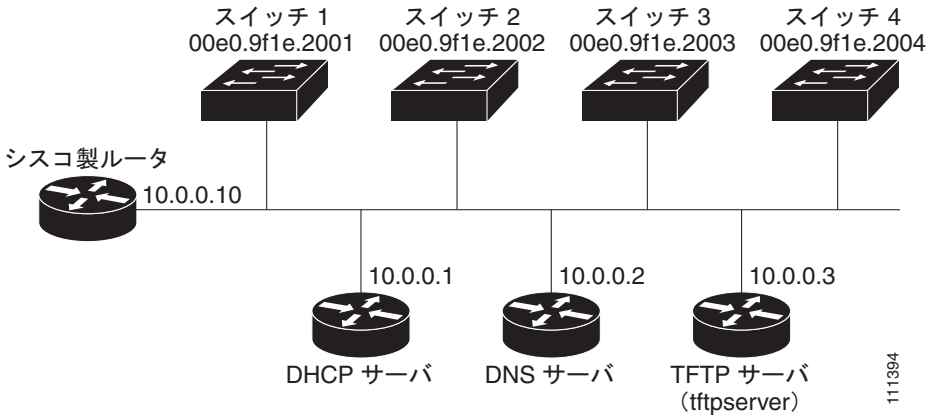


表 3-2 は、DHCP サーバ上の予約リースの設定例です。

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	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*	*tftpserver* または *10.0.0.3*
ブート ファイル名（コンフィギュレーション ファイル）（任意）	switcha-confg	switchb-confg	switchc-confg	switchd-confg
ホスト名（任意）	switcha	switchb	switchc	switchd

DNS サーバ 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。

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** *ip-address*	スイッチに直接接続しているネクスト ホップのルータ インターフェイスの IP アドレスを入力します。このスイッチにはデフォルト ゲートウェイが設定されています。デフォルト ゲートウェイは、スイッチから宛先 IP アドレスを取得していない IP パケットを受信します。 デフォルト ゲートウェイが設定されると、スイッチは、ホストが接続する必要のあるリモート ネットワークに接続できます。 **（注）** IP でルーティングするようにスイッチを設定した場合、デフォルト ゲートウェイの設定は不要です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces vlan** *vlan-id*	設定された IP アドレスを確認します。
ステップ 8	**show ip redirects**	設定されたデフォルト ゲートウェイを確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチの 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 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Switch A
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet0/1
ip address 172.20.137.50 255.255.255.0
!
interface gigabitethernet0/2
mvr type source

<output truncated>

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

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

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

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

コンフィギュレーション ファイルの他のコピー元については、付録 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.3-12）
- 「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.3-12）
- 「手動で起動する場合」（P.3-13）
- 「特定のソフトウェア イメージを起動する場合」（P.3-14）
- 「環境変数の制御」（P.3-14）

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 *config.text* ファイルを使用します。 新しいスイッチの場合、コンフィギュレーション ファイルはありません。

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.3-3）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。 *file-url* に、パス（ディレクトリ）およびコンフィギュレーション ファイル名を指定します。 ファイル名およびディレクトリ名は、大文字と小文字が区別されます。
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 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。
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***:**/*file-url* ブート ローダ コマンドを使用します。 • *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字が区別されます。
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** *filesystem***:**/*file-url*	次回の起動時に、フラッシュ メモリ内の特定のイメージを起動するようにスイッチを設定します。 • *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。 • *file-url* には、パス（ディレクトリ）および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字が区別されます。
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 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。

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

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 ...* 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。	**boot system** f*ilesystem:/file-url ...* 次回の起動時に読み込む Cisco IOS イメージを指定します。このコマンドによって、BOOT 環境変数の設定が変更されます。
MANUAL_BOOT	**set MANUAL_BOOT yes** 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。	**boot manual** 次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。 次回のシステム再起動時には、スイッチはブート ローダ モードになります。システムを起動するには、**boot flash:***filesystem:/file-url* ブート ローダ コマンドを使用し、起動可能イメージの名前を指定します。
CONFIG_FILE	**set CONFIG_FILE flash:***/file-url* Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。	**boot config-file flash:***/file-url* Cisco IOS がシステム 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。

  （注）　**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。



CHAPTER 4

Cisco IOS CNS エージェントの設定

この章では、Catalyst 2960 スイッチにプライベート VLAN 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、Cisco.com で次の 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

この章で説明する内容は、次のとおりです。

- 「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.4-13）

Cisco Configuration Engine ソフトウェアの概要

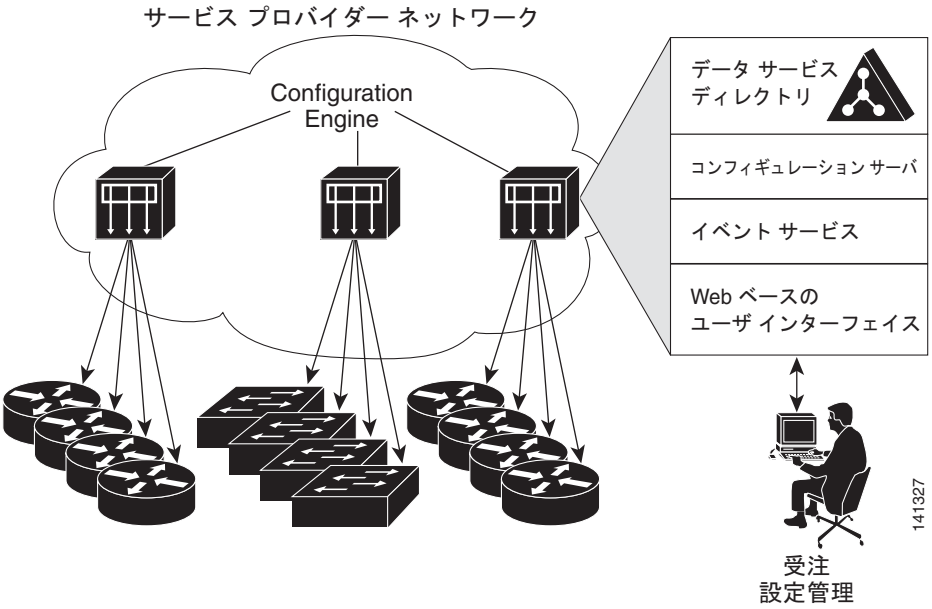
Cisco Configuration Engine は、ネットワーク管理ソフトウェアで、ネットワーク デバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーション サービスとして機能します（図 4-1 を参照）。各 Configuration Engine は、シスコ デバイス（スイッチとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Configuration Engine はデバイス固有の設定変更を生成してデバイスに送信し、設定変更を実行してその結果をロギングすることで、初期設定および設定の更新を自動化します。

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



ここでは、次の概要について説明します。

- 「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

Cisco 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、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*あと*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は、Cisco.com で次の 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/products_installation_and_configuration_guide_book09186a00803b59db.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

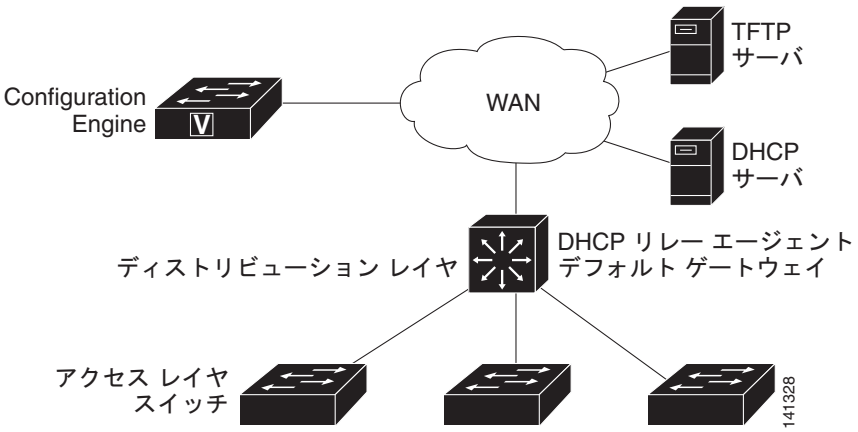
スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol（DHCP）要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューション スイッチは DHCP リレー エージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバの IP アドレス、ブートストラップ コンフ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

図 4-2　初期設定の概要



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.4-8）
- 「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

（注）　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	**cns event** {*ip-address* | *hostname*} [*port-number*] [**backup**] [**init-retry** *retry-count*] [**keepalive** *seconds retry-count*] [**source** *ip-address*]	イベント エージェントをイネーブルにして、ゲートウェイ パラメータを入力します。 • {*ip-address* | *hostname*} に、イベント ゲートウェイの IP アドレスまたはホスト名を入力します。 • （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）**init-retry** *retry-count* に、バックアップに切り替えるまでの最初の再試行回数を入力します。デフォルト値は 3 です。 • （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 0 です。 • （任意）**source** *ip-address* 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 **force-fmt1** 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 config connect-intf** *interface-prefix* [**ping-interval** *seconds*] [**retries** *num*]	connect-interface-config サブモードを開始して、Configuration Engine に接続するためのインターフェイスを指定します。 • 接続するインターフェイスの *interface-prefix* を入力します。インターフェイス タイプを指定する必要がありますが、インターフェイス番号を指定する必要はありません。 • （任意）**ping-interval** *seconds* に、連続する ping の試行間隔を入力します。指定できる範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。 • （任意）**retries** *num* に、ping の再試行回数を入力します。指定できる範囲は 1 ～ 30 です。デフォルト値は 5 です。

	コマンド	目的
ステップ 3	**config-cli** または **line-cli**	**cns config connect-intf** で定義されたインターフェイスを介して Configuration Engine に接続するには、**config-cli** を入力します。モデム ダイアルアップ回線を介して Configuration Engine に接続するには、**line-cli** を入力します。 （注）　**config-cli** 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、インターフェイス名のプレースホルダとして機能する特殊な文字 **&** を使用します。設定が適用されると、**&** はインターフェイス名に置き換えられます。たとえば、FastEthernet0/1 を介して接続する場合、コマンド **config-cli ip route 0.0.0.0 0.0.0.0&** は、コマンド **ip route 0.0.0.0 0.0.0.0 FastEthernet0/1** を生成します。
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	**hostname** *name*	スイッチのホスト名を入力します。
ステップ 6	**ip route** *network-number*	IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。
ステップ 7	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] または **cns id** {**hardware-serial** | **hostname** | **string** *string*} [**event**]	Configuration Engine が使用する一意の EventID または ConfigID を設定します。 • *interface num* 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 UID として割り当てるには **dns-reverse** を、IP アドレスを使用するには **ipaddress** を、MAC アドレスを一意の ID として使用するには **mac-address** を使用します。 • （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。 • {**hardware-serial** | **hostname** | **string** *string*} 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、または **string** *string* に任意のテキストストリングを一意の ID として入力します。

	コマンド	目的
ステップ 8	**cns config initial** {*ip-address* | *hostname*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]	Cisco IOS をイネーブルにし、初期設定を開始します。 • {*ip-address* | *hostname*} 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）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 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**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 11	**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、リモート スイッチで初期設定を実施する例を示します。スイッチのホスト名は一意の ID です。Cisco Configuration Engine の IP アドレスは 172.28.129.22 です。

```
Switch(config)# cns config connect-intf serial ping-interval 1 retries 1
Switch(config-cns-conn-if)# config-cli ip address negotiated
Switch(config-cns-conn-if)# config-cli encapsulation ppp
Switch(config-cns-conn-if)# config-cli ip directed-broadcast
Switch(config-cns-conn-if)# config-cli no keepalive
Switch(config-cns-conn-if)# config-cli no shutdown
Switch(config-cns-conn-if)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 10.1.1.1 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id Ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 10.1.1.1 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。 • {*ip-address* | *hostname*} 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** *ip-address* 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** または **show cns config outstanding**	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 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 に記載された特権 EXEC コマンドを使用すると、CNS 設定情報を表示できます。

表 4-2　CNS 設定の表示

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



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ています。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.5-4）
- 「CLI によるスイッチ クラスタの管理」（P.5-14）
- 「SNMP によるスイッチ クラスタの管理」（P.5-15）

（注） 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 29 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ヤ 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。

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 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 2970	12.1(11)AX 以降	メンバーまたはコマンド スイッチ
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

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）

スイッチ	Cisco IOS リリース	クラスタへの対応性
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

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 スイッチの場合、スタンバイ クラスタ コマンド スイッチも Catalyst 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.5-12）および「パスワード」（P.5-13）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。

（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。

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。

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.5-9）
- 「IP アドレス」（P.5-12）
- 「ホスト名」（P.5-12）
- 「パスワード」（P.5-13）
- 「SNMP コミュニティ ストリング」（P.5-13）
- 「TACACS+ および RADIUS」（P.5-14）

- 「LRE プロファイル」（P.5-14）

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 22 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。

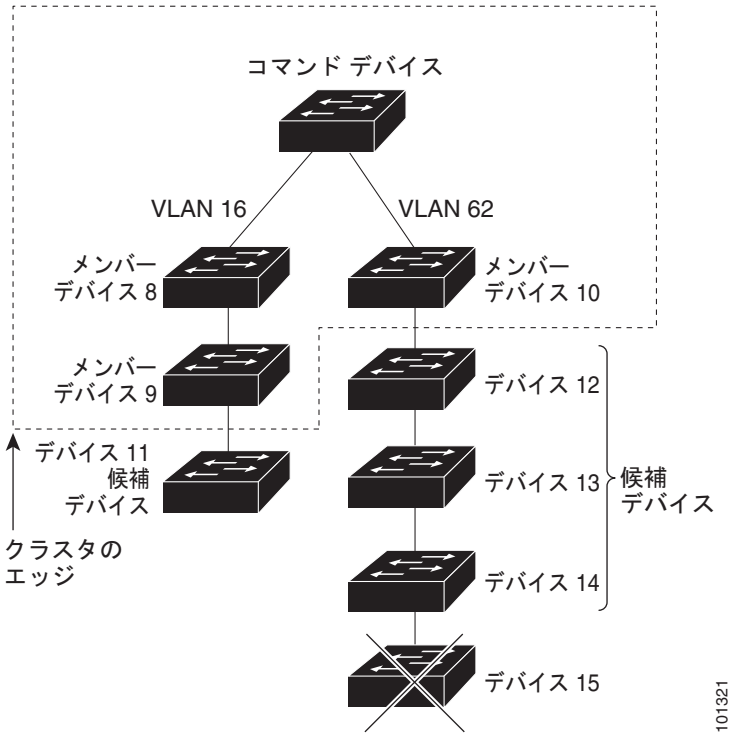
- 「CDP ホップを使用しての検出」（P.5-5）
- 「CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出」（P.5-6）
- 「異なる VLAN からの検出」（P.5-7）
- 「異なる管理 VLAN からの検出」（P.5-7）
- 「新しくインストールしたスイッチの検出」（P.5-8）

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。

図 5-1　CDP ホップを使用しての検出

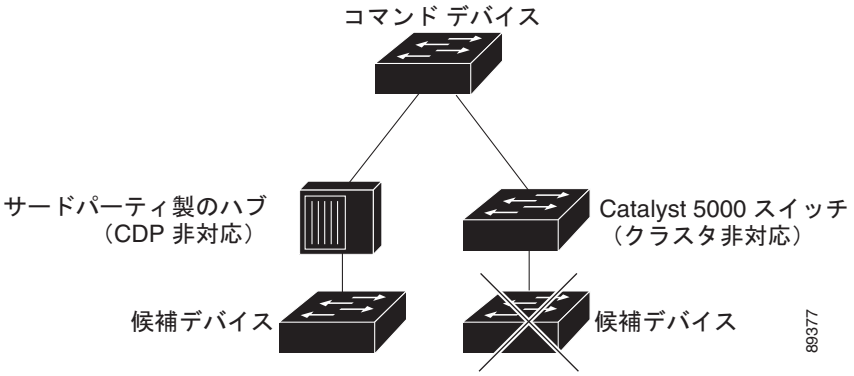


CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

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

図 5-2　CDP 非対応デバイスおよびクラスタ非対応デバイスからの検出

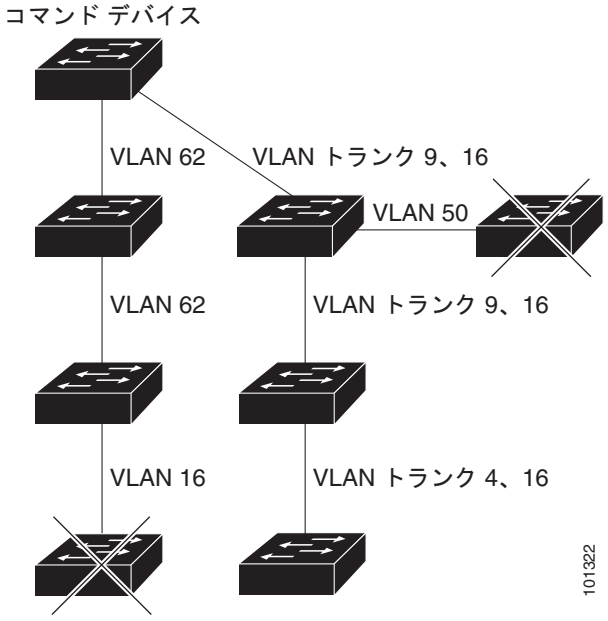


異なる VLAN からの検出

クラスタ コマンド スイッチが Catalyst 2970、Catalyst 3550、Catalyst 3560、または Catalyst 3750 の場合、異なる VLAN のクラスタ メンバー 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.5-7）を参照してください。VLAN の詳細については、第 12 章「VLAN の設定」を参照してください。

図 5-3　　異なる VLAN からの検出



異なる管理 VLAN からの検出

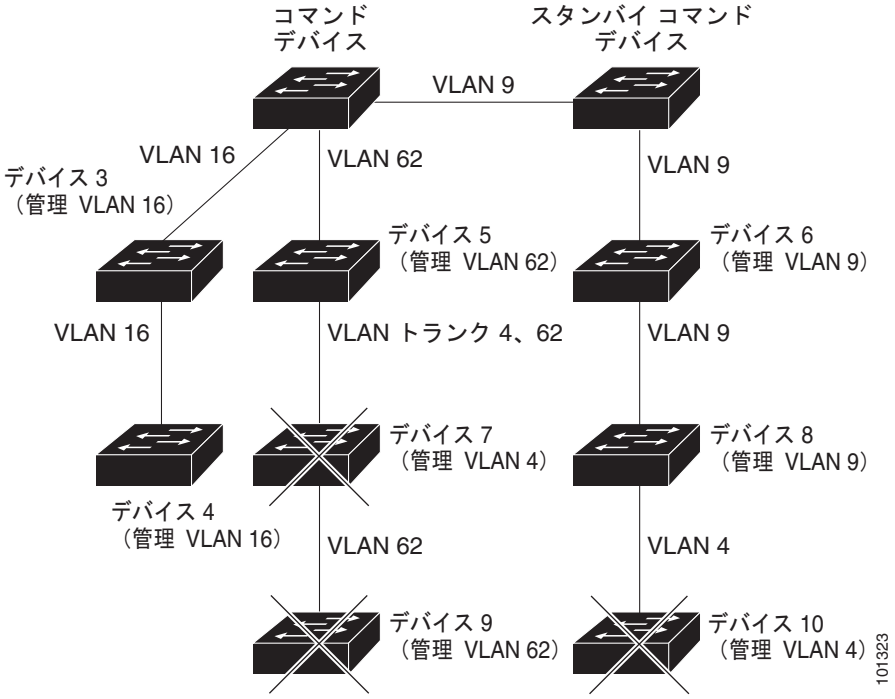
Catalyst 2970、Catalyst 3550、Catalyst 3560、Catalyst 3750 クラスタ コマンド スイッチは、異なる VLAN や管理 VLAN のクラスタ メンバー スイッチを検出して管理できます。クラスタ メンバー スイッチとして、Catalyst スイッチもクラスタ コマンド スイッチと共通の VLAN に少なくとも 1 つは接続している必要があります。ただし、管理 VLAN を介してクラスタ コマンド スイッチに接続する必要はありません。デフォルトの管理 VLAN は VLAN 1 です。

（注）　スイッチ クラスタに Catalyst 3750 スイッチまたはスイッチ スタックがある場合は、Catalyst 3750 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 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 VLAN 4 のスイッチ）。クラスタ コマンド スイッチと共通の VLAN（VLAN 62 および VLAN 9）に接続していないため検出されません。
- スイッチ 9。自動検出は非候補デバイス（スイッチ 7）より先は検出できないため、検出されません。

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

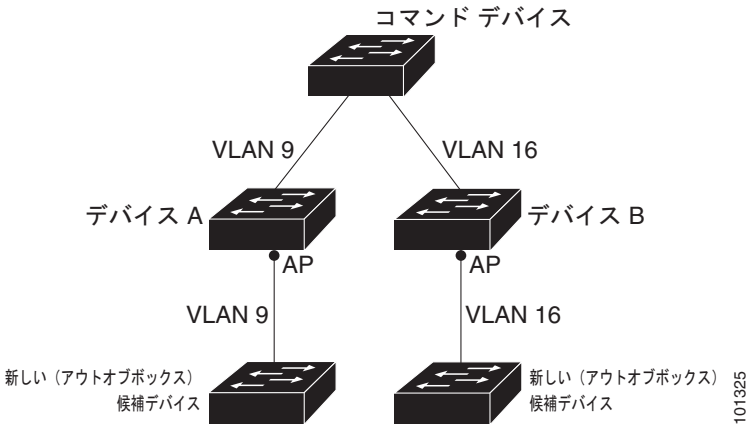
新しいアウトオブボックス スイッチをクラスタに加入させるには、アクセスポートの 1 つにクラスタを接続する必要があります。Access Port（AP; アクセス ポート）は 1 つの VLAN にのみ属し、そのトラフィックを転送します。デフォルトでは、新しいスイッチとそのアクセス ポートに対して VLAN 1 が割り当てられます。

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.5-3）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.5-11）を参照してください。

（注）　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.5-10）
- 「クラスタ スタンバイ グループに関する他の考慮事項」（P.5-10）
- 「クラスタ設定の自動復旧」（P.5-11）

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.5-12）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、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。

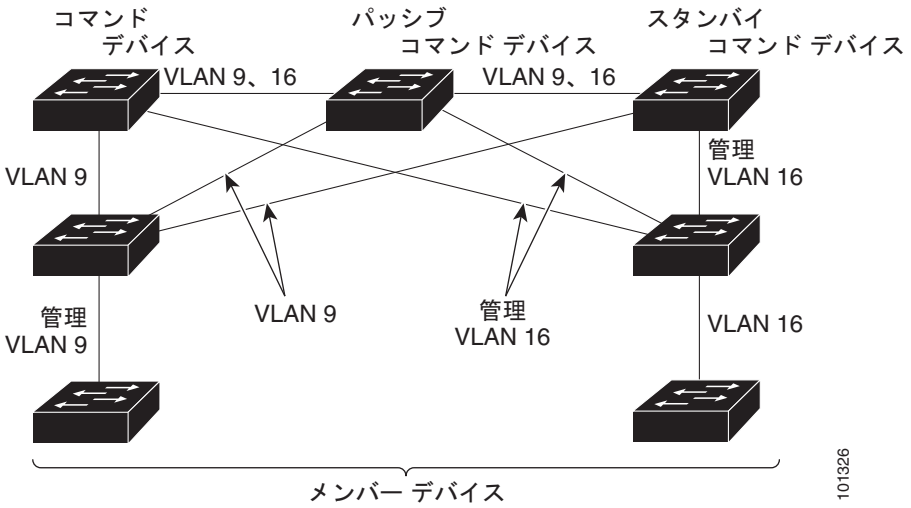
（注）　スタンバイ クラスタ コマンド スイッチとして割り当てることができるスイッチ数に制限はありません。ただし、クラスタのスイッチの総数（アクティブ クラスタ コマンド スイッチ、スタンバイ グループ メンバー、およびクラスタ メンバー スイッチを含む）は 16 以内にする必要があります。

- 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.5-7）

図 5-6　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。

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 *@esN* を追加した形でコミュニティ ストリングを継承します。

- *command-switch-readonly-community-string@esN* : *N* にはメンバ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 28 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.8-10）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.8-17）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。

（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.28-6）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。

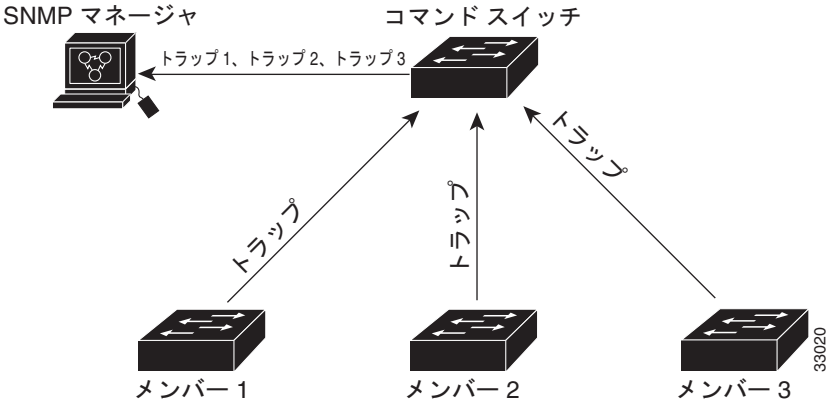
クラスタを作成すると、クラスタ コマンド スイッチがクラスタ メンバー スイッチと SNMP アプリケーション間のメッセージ交換を管理します。クラスタ コマンド スイッチ上のクラスタ ソフトウェアは、クラスタ コマンド スイッチ上で最初に設定された Read-Write および Read-Only コミュニティ ストリングにクラスタ メンバー スイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをクラスタ メンバー スイッチに伝播します。クラスタ コマンド スイッチは、このコミュニティ ストリングを使用して、SNMP 管理ステーションとクラスタ メンバー スイッチ間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

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

クラスタ メンバー 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 28 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





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.6-15）
- 「バナーの作成」（P.6-18）
- 「MAC アドレス テーブルの管理」（P.6-20）
- 「ARP テーブルの管理」（P.6-28）

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.6-1）
- 「NTP の概要」（P.6-2）
- 「NTP の設定」（P.6-3）
- 「手動での日時の設定」（P.6-11）

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.6-11）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。

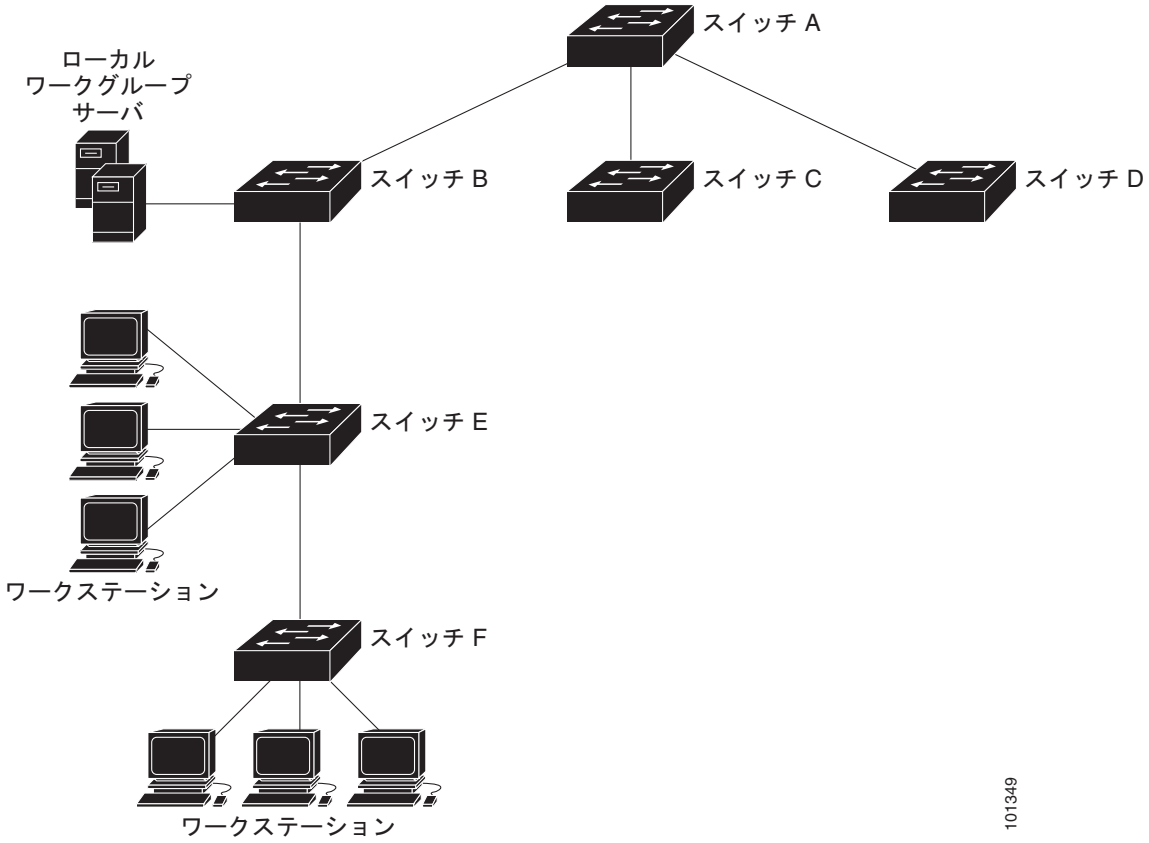
NTP が稼動するデバイス間の通信（*アソシエーション*）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャスト メッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャスト メッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、この場合は、情報の流れは一方向に限られます。

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.6-4）
- 「NTP アソシエーションの設定」（P.6-5）
- 「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.6-10）
- 「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

機能	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。

	コマンド	目的
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** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**] 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 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 *ip-address* 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）*number* 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）*interface* 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** *number*] [**key** *keyid*] [*destination-address*]	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）*number* 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。 キーワードの意味は次のとおりです。 • **query-only**：NTP 制御クエリーに限り許可します。 • **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。 *access-list-number* 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
ステップ 1	**configure terminal**	グローバル コ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、ディセーブルにするインターフェイスを指定します。
ステップ 3	**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。
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。

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
ステップ 1	**configure terminal**	グローバル コ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 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。
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。

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.6-5）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**

（注）　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.6-12）
- 「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* または **clock set** *hh*:*mm*:*ss month day 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す。 • *hh*:*mm*:*ss* 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。 • *day* には、当月の日付で日を指定します。 • *month* 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

日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 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。 • *hours-offset* には、UTC からの時差を入力します。 • （任意）*minutes-offset* 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。

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	**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）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* 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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* 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）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* 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.6-16）

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.6-17）
- 「DNS の設定の表示」（P.6-18）

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

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 ... server-address6*]	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。 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。

	コマンド	目的
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。

（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, 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.6-18）
- 「MoTD ログイン バナーの設定」（P.6-19）
- 「ログイン バナーの設定」（P.6-20）

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。 *message* 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。 *message* 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。

（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。

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.6-21）
- 「MAC アドレスおよび VLAN」（P.6-21）
- 「MAC アドレス テーブルのデフォルト設定」（P.6-22）
- 「アドレス エージング タイムの変更」（P.6-22）
- 「ダイナミック アドレス エントリの削除」（P.6-23）
- 「MAC アドレス通知トラップの設定」（P.6-23）
- 「スタティック アドレス エントリの追加および削除」（P.6-25）
- 「ユニキャスト MAC アドレス フィルタリングの設定」（P.6-26）
- 「アドレス テーブル エントリの表示」（P.6-27）

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	自動学習
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。 *vlan-id* 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 アドレス通知トラップの設定

MAC アドレス通知は、スイッチに MAC アドレス 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常に、SNMP（簡易ネットワーク管理プロトコル）通知を生成して Network Management System（NMS; ネットワーク管理システム）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、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、動的でセキュアな MAC アドレスについて生成されます。自己アドレス、マルチキャスト アドレス、またはその他のスタティック アドレスについては、イベントは生成されません。

NMS ホストに MAC アドレス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	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* 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。

	コマンド	目的
ステップ 3	**snmp-server enable traps mac-notification**	スイッチが MAC アドレス 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 アドレス通知機能をイネーブルにします。
ステップ 5	**mac address-table notification** [**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	**snmp trap mac-notification** {**added** | **removed**}	MAC アドレス通知トラップをイネーブルにします。 • **added** を指定すると、このインターフェイスに MAC アドレスが追加された場合には常に、MAC アドレス通知トラップをイネーブルにします。 • **removed** を指定すると、このインターフェイスから MAC アドレスが削除された場合には常に、MAC アドレス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 interface** **show running-config**	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。

スイッチによる MAC アドレス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** グローバル 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 アドレス通知トラップをディセーブルにするには、**no snmp trap mac-notification** {**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 アドレス通知機能をディセーブルにするには、**no mac address-table notification** グローバル 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 アドレス通知機能をイネーブルにし、インターバルを 60 秒、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
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

これまでのコマンドを確認するには、**show mac address-table notification interface** および **show mac address-table notification** 特権 EXEC コマンドを入力します。

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* **vlan** *vlan-id* **interface** *interface-id*	MAC アドレス テーブルにスタティック アドレスを追加します。 • *mac-addr* 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。 • *vlan-id* 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。

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

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

  % 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。 • *vlan-id* 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
```

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 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。

（注） 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 7

SDM テンプレートの設定

この章では、Catalyst 2960 スイッチで Switch Database Management（SDM）テンプレート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。

- 「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。

- 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。
- 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 およびデュアル IPv6 SDM テンプレートでは、デュアル スタック環境が可能です。

表 7-1 に、各テンプレートでサポートされる各リソースの概数を示します。

表 7-1　各テンプレートが許容する機能リソースの概数

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

表 7-1　各テンプレートが許容する機能リソースの概数 （続き）

リソース	デフォルト	QoS	デュアル
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
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

表内の各行は、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.7-2）

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。

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。

	コマンド	目的
ステップ 2	**sdm prefer** {**default** | **dual-ipv4-and-ipv6 default** | **qos**}	スイッチで使用する SDM テンプレートを指定します。 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。



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.8-10）
- 「RADIUS によるスイッチ アクセスの制御」（P.8-17）
- 「スイッチのローカル認証および許可の設定」（P.8-32）
- 「SSH のためのスイッチの設定」（P.8-33）
- 「SSL HTTP のためのスイッチの設定」（P.8-37）
- 「SCP のためのスイッチの設定」（P.8-44）

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.8-10）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。

（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。

- 「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.8-3）
- 「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.8-7）

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。 *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。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 *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モード アクセス）。

```
Switch(config)# enable password l1u2c3k4y5
```

暗号化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} または **enable secret** [**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 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）*level* 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。
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.8-7）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 *1FaD0$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。

（注）　パスワード回復をディセーブルにする場合は、エンド ユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP（VLAN トランキング プロトコル）トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」（P.35-3）を参照してください。

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。
ステップ 5	**password** ***password***	1 つまたは複数の回線に対応する Telnet パスワードを入力します。 *password* 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。 コマンド **line vty 0 15** の下にパスワードが表示されます。
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。 • *encryption-type* 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** または **line vty 0 15**	ライン コンフィギュレーション モードを開始し、コンソール ポート（回線 0）または VTY 回線（回線 0 ～ 15）を設定します。
ステップ 4	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
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.8-9）
- 「権限レベルへのログインおよび終了」（P.8-9）

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。 • *level* 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。
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。 • *level* 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** または **show privilege**	設定を確認します。 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。

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。 *level* 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。
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** または **show privilege**	設定を確認します。 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。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable***level*	指定した権限レベルを終了します。 *level* 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.8-10）
- 「TACACS+ の動作」（P.8-12）
- 「TACACS+ の設定」（P.8-12）
- 「TACACS+ 設定の表示」（P.8-17）

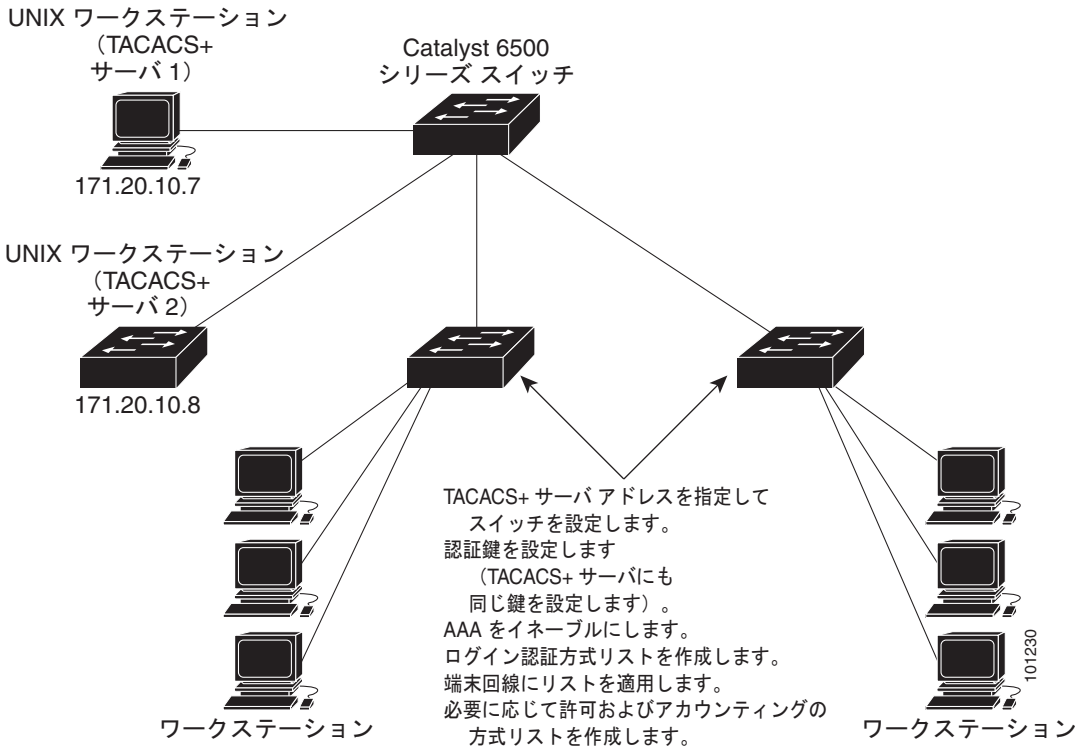
TACACS+ の概要

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）。

図 8-1　一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力されたあと、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。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての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.8-13）
- 「TACACS+ サーバ ホストの特定および認証鍵の設定」（P.8-13）
- 「TACACS+ ログイン認証の設定」（P.8-14）

- 「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.8-16）
- 「TACACS+ アカウンティングの起動」（P.8-17）

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。

	コマンド	目的
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* 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。 • *method1...* 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.8-13）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。
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** | *list-name*}	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。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* 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。

（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 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.8-18）

- 「RADIUS の動作」（P.8-19）
- 「RADIUS の設定」（P.8-19）
- 「RADIUS の設定の表示」（P.8-32）

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。

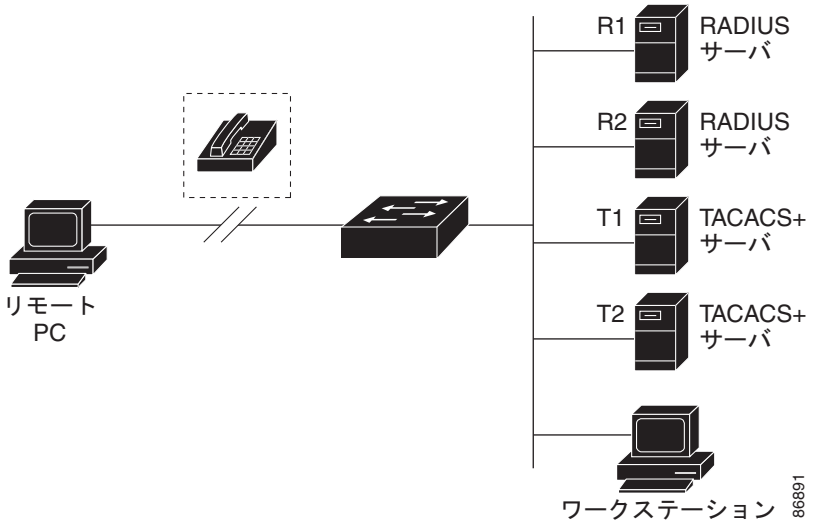
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- 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.8-19）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 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、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。

ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」（P.8-20）
- 「RADIUS サーバ ホストの識別」（P.8-20）（必須）
- 「RADIUS ログイン認証の設定」（P.8-23）（必須）
- 「AAA サーバ グループの定義」（P.8-25）（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.8-27）（任意）
- 「RADIUS アカウンティングの起動」（P.8-28）（任意）
- 「すべての RADIUS サーバの設定」（P.8-29）（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.8-29）（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.8-31）（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、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示して、そのあと同じデバイス上で 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。

（注）　スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、および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.8-29）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.8-25）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** *port-number* 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	**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、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```

（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。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* 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。 • *method1...* 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.8-20）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** | *list-name*}	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。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* 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	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* 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** *group-name*	AAA サーバ グループを、特定のグループ名で定義します。 このコマンドを使用すると、スイッチはサーバ グループ コンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。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。 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。

	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.8-23）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-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

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**} *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。

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す。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コ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アトリビュート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アトリビュート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アトリビュート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。

（注） 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
```

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。
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。 • *encryption-type* 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.8-33）
- 「SSH の設定」（P.8-34）
- 「SSH の設定およびステータスの表示」（P.8-37）

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/fsecur_c.html

（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_book09186a0080087e33.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.8-34）
- 「制限事項」（P.8-34）

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.8-10）を参照）
- RADIUS（詳細については、「RADIUS によるスイッチ アクセスの制御」（P.8-17）を参照）
- 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.8-32）を参照）

（注）　このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。
- スイッチは、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.8-35）
- 「スイッチで SSH を実行するためのセットアップ」（P.8-35）（必須）
- 「SSH サーバの設定」（P.8-36）（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.8-35）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.8-32）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。

	コマンド	目的
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。
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。

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**：SSHv1 を実行するようにスイッチを設定します。 • **2**：SSHv2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートしている場合、SSH サーバは SSHv2 を選択します。
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 4	**line vty** *line_number* [*ending_line_number*] **transport input ssh**	（任意）仮想端末回線設定を設定します。 • ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* に対して、1 回線ペアを指定します。指定できる範囲は 0 ～ 15 です。 • スイッチで非 SSH Telnet 接続を回避するように設定します。これにより、ルータは SSH 接続に限定されます。
ステップ 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 ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバの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。

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 8-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 8-2　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/fsecur_r.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.8-38）
- 「セキュア HTTP サーバおよびクライアントの設定」（P.8-40）
- 「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.8-44）

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/products/sw/iosswrel/ps1839/products_feature_guide09186a008015a4c6.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。

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
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D

<output truncated>
```

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。

（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）
2. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化、およびメッセージ ダイジェストに MD5 を使用した RSA の鍵交換

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.8-40）
- 「SSL の設定時の注意事項」（P.8-40）
- 「CA の信頼点の設定」（P.8-40）
- 「セキュア HTTP サーバの設定」（P.8-41）
- 「セキュア HTTP クライアントの設定」（P.8-43）

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。

	コマンド	目的
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** *url*	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** *url*	ピアの証明書が取り消されていないかを確認するために、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** *path-name*	（任意）HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバ ファイルの場所を指定します（通常、システムのフラッシュ メモリを指定します）。
ステップ 9	**ip http access-class** *access-list-number*	（任意）HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	**ip http max-connections** *value*	（任意）HTTP サーバへの同時最大接続数を指定します。指定できる範囲は 1 ～ 16 です。デフォルトは 5 です。
ステップ 11	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*	（任意）指定の状況下における、HTTP サーバへの接続最大時間を指定します。 • **idle**：データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は 180 秒です（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 8-3 に記載された特権 EXEC コマンドを使用します。

表 8-3　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ンド

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 SSH が必要です（Berkeley の 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



CHAPTER 9

IEEE 802.1x ポートベース認証の設定

この章では、Catalyst 2960 スイッチ上で IEEE 802.1x ポートベース認証を設定する方法について説明します。IEEE 802.1x 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。

（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 Security Command Reference, Release 12.2*』の「RADIUS 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。

- 「IEEE 802.1x ポートベース認証の概要」（P.9-1）
- 「IEEE 802.1x 認証の設定」（P.9-18）
- 「IEEE 802.1x の統計情報およびステータスの表示」（P.9-41）

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（認証されている場合を除く）、クライアント/サーバ型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 が提供する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。

ここでは、IEEE 802.1x ポートベース認証について説明します。

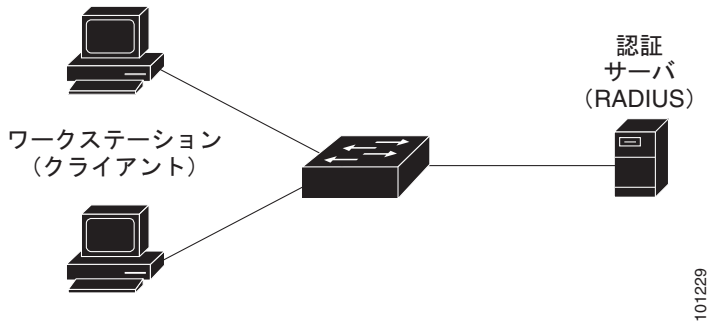
- 「デバイスの役割」（P.9-2）
- 「認証プロセス」（P.9-3）
- 「認証の開始およびメッセージ交換」（P.9-5）
- 「許可ステートおよび無許可ステートのポート」（P.9-7）
- 「IEEE 802.1x のホスト モード」（P.9-7）
- 「IEEE 802.1x アカウンティング」（P.9-8）

- 「IEEE 802.1x アカウンティング アトリビュート値（AV）ペア」（P.9-8）
- 「VLAN 割り当てを使用した IEEE 802.1x 認証の利用」（P.9-9）
- 「ゲスト VLAN を使用した IEEE 802.1x 認証の利用」（P.9-11）
- 「制限付き VLAN による IEEE 802.1x 認証の利用」（P.9-12）
- 「アクセス不能認証バイパスによる IEEE 802.1x 認証の使用」（P.9-13）
- 「音声 VLAN ポートを使用した IEEE 802.1x 認証の利用」（P.9-14）
- 「ポート セキュリティを使用した IEEE 802.1x 認証の利用」（P.9-14）
- 「WoL 機能を使用した IEEE 802.1x 認証の利用」（P.9-15）
- 「MAC 認証バイパスを使用した IEEE 802.1x 認証の利用」（P.9-16）
- 「NAC レイヤ 2 IEEE 802.1x 検証の利用」（P.9-17）
- 「Web 認証の使用」（P.9-17）

デバイスの役割

IEEE 802.1x ポートベース認証では、ネットワーク上のデバイスにそれぞれ固有の役割があります（図 9-1 を参照）。

図 9-1　IEEE 802.1x におけるデバイスの役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP OS（オペレーティング システム）に付属しているような IEEE 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、IEEE 802.1x 標準では*サプリカント*といいます）。

（注）　Windows XP のネットワーク接続および IEEE 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、IEEE 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 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 IEEE 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

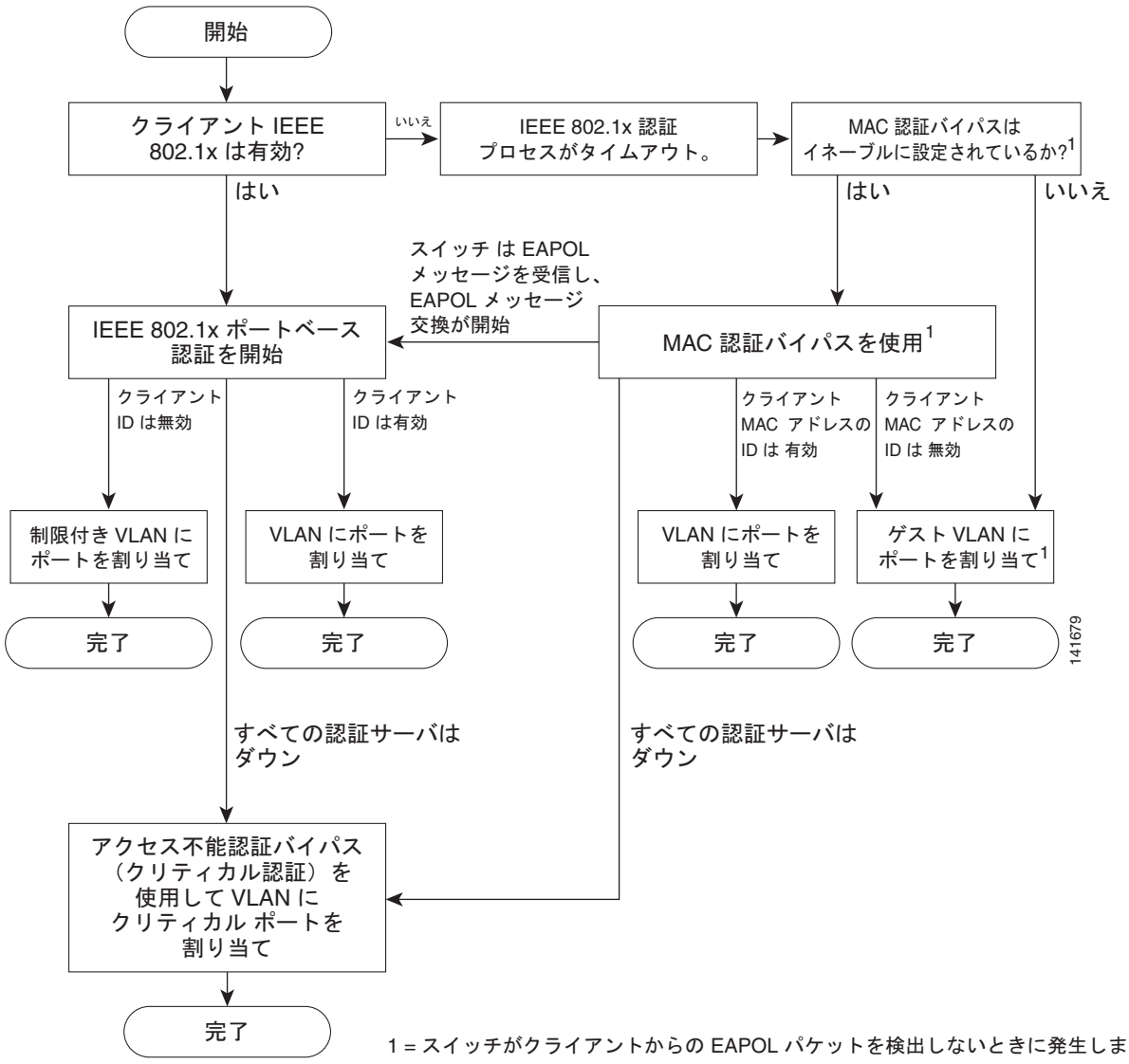
IEEE 802.1x ポートベース認証がイネーブルであり、クライアントが IEEE 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で IEEE 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 IEEE 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 IEEE 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。

図 9-2　認証フローチャート



1 = スイッチがクライアントからの EAPOL パケットを検出しないときに発生します。

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 IEEE 802.1x 認証を設定したあと、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*）、IEEE 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。

認証の開始およびメッセージ交換

IEEE 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。**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。

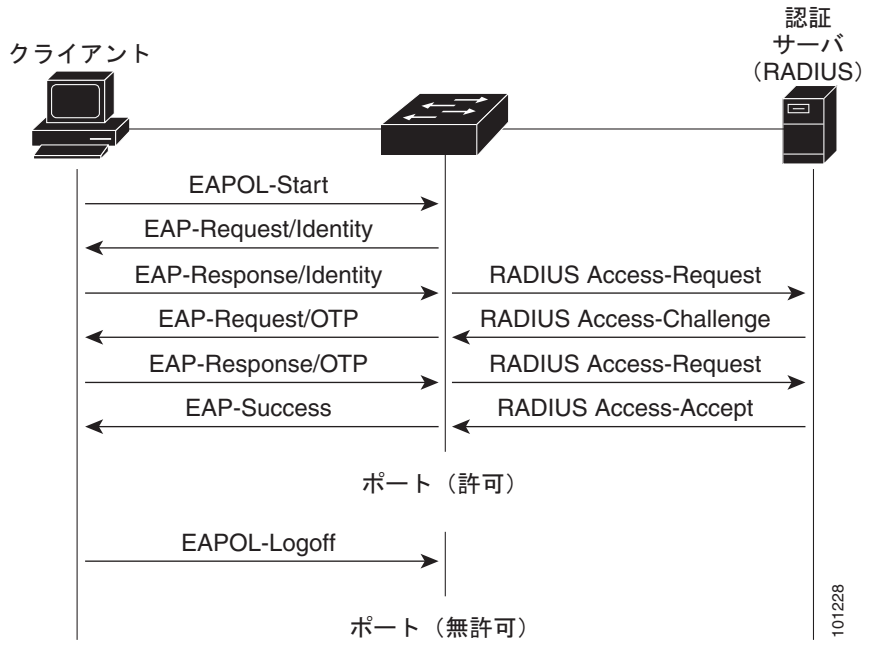
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス デバイスで IEEE 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.9-7）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.9-7）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。

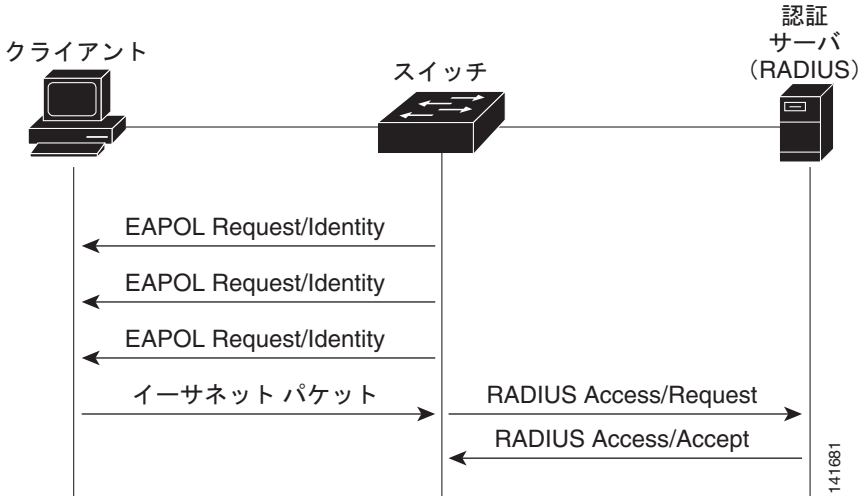
図 9-3　メッセージ交換



EAPOL メッセージ交換の待機中に IEEE 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、IEEE 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



許可ステートおよび無許可ステートのポート

IEEE 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 IEEE 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 として設定されている場合、VoIP トラフィックおよび IEEE 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。

IEEE 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 IEEE 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、IEEE 802.1x 対応のクライアントが、IEEE 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。

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**：IEEE 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の IEEE 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**：IEEE 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。

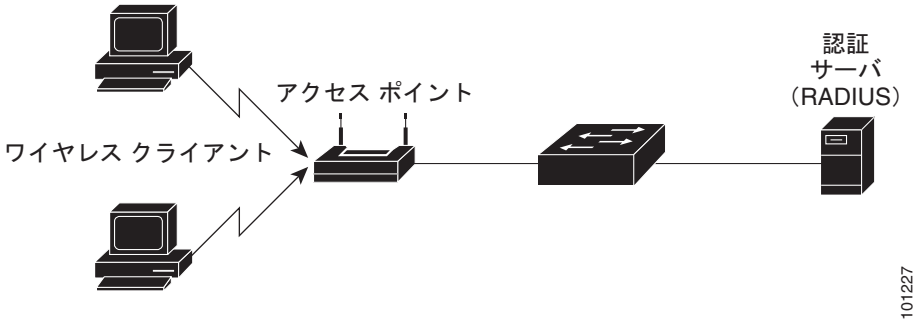
IEEE 802.1x のホスト モード

IEEE 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.9-2）を参照）では、IEEE 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 つのみです。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 IEEE 802.1x 対応ポートに接続できます。図 9-5 (P.9-8) に、ワイヤレス LAN における IEEE 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、IEEE 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。

図 9-5　マルチ ホスト モードの例



IEEE 802.1x アカウンティング

IEEE 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。IEEE 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。IEEE 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 IEEE 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 IEEE 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。

IEEE 802.1x アカウンティング アトリビュート値（AV）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、IEEE 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 9-1 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 9-1　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	非送信	常時送信
アトリビュート [43]	Acct-Output-Octets	非送信	非送信	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	非送信	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 『IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

VLAN 割り当てを使用した IEEE 802.1x 認証の利用

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。

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 IEEE 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 IEEE 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。
- IEEE 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、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、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。
- IEEE 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。
- IEEE 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。
- IEEE 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。
- IEEE 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 IEEE 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。
- IEEE 802.1x 認証をイネーブルにします （アクセス ポートで IEEE 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 名または VLAN ID

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、IEEE 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.8-29）を参照してください。

ゲスト VLAN を使用した IEEE 802.1x 認証の利用

スイッチ上の各 IEEE 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（IEEE 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 IEEE 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 IEEE 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、IEEE 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 パケット履歴を維持します。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 IEEE 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。

Cisco IOS Release 12.2(25)SEE 以降では、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。

（注）　インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、IEEE 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 IEEE 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、IEEE 802.1x ポート上でシングル ホスト モードまたはマルチ ホスト モードでサポートされています。

RSPAN VLAN または音声 VLAN を除くあらゆるアクティブ VLAN を、IEEE 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。

Cisco IOS Release 12.2(25)SEE 以降のリリースでは、スイッチが、*MAC 認証バイパス*をサポートしています。MAC 認証バイパスが IEEE 802.1x ポートでイネーブルの場合、スイッチは、IEEE 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。IEEE 802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、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。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 認証バイパスを使用した IEEE 802.1x 認証の利用」（P.9-16）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.9-30）を参照してください。

制限付き VLAN による IEEE 802.1x 認証の利用

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 IEEE 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 IEEE 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 IEEE 802.1x ポート上でシングル ホスト モードの場合のみサポートされます。

RSPAN VLAN または音声 VLAN を除くあらゆるアクティブ VLAN を、IEEE 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.9-31）を参照してください。

アクセス不能認証バイパスによる IEEE 802.1x 認証の使用

Cisco IOS Release 12.2(25)SEE以降では、スイッチが設定された RADIUS サーバに到達できず、ホストが認証されない場合、*クリティカル* ポートに接続されたホストにネットワーク アクセスできるようスイッチを設定できます。クリティカル ポートは、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）に対してイネーブルになっています。

この機能がイネーブルの場合、スイッチはクリティカル ポートに接続されたホストの認証を行う際に、RADIUS サーバのステータスを確認します。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。

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。

ホストを認証できる RADIUS サーバが利用可能な場合、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。

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 IEEE 802.1x 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。
- IEEE 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 IEEE 802.1x 認証の利用

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 IEEE 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 IEEE 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。

IEEE 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 IEEE 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 14 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 IEEE 802.1x 認証の利用

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 IEEE 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 IEEE 802.1x 認証をイネーブルに設定すると、IEEE 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、IEEE 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 IEEE 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 error-disabled 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.21-9）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 IEEE 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、IEEE 802.1x クライアントを再認証する必要があります。
- IEEE 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、IEEE 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。

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.21-8）を参照してください。

WoL 機能を使用した IEEE 802.1x 認証の利用

IEEE 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 IEEE 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、IEEE 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 IEEE 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 IEEE 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。

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。

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 認証バイパスを使用した IEEE 802.1x 認証の利用

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.9-4）を参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 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 IEEE 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 IEEE 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。IEEE 802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、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。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。

リンクの存続時間中にインターフェイスで EAPOL パケットが検出された場合、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 IEEE 802.1x 対応サプリカントであると判断し、インターフェイスを許可するために（MAC 認証バイパスではなく）IEEE 802.1x 認証を使用します。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、IEEE 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 IEEE 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、IEEE 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 IEEE 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『IEEE 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。

- IEEE 802.1x 認証：IEEE 802.1x 認証がポートでイネーブルの場合にのみ 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：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した IEEE 802.1x 認証の利用」（P.9-14）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した IEEE 802.1x 認証の利用」（P.9-14）を参照してください。
- VLAN Menbership Policy Server（VMPS; VLAN メンバシップ ポリシー サーバ）：IEEE 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。

NAC レイヤ 2 IEEE 802.1x 検証の利用

Cisco IOS Release 12.2(25)SED 以降では、スイッチは NAC レイヤ 2 IEEE 802.1x 検証をサポートします。これは、デバイス ネットワーク アクセスを許可する前に、エンドポイント システムやクライアントのウイルス対策の状態やポスチャをチェックします。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下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。
- **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 IEEE 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、IEEE 802.1x ポートベース認証と似ています。NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 IEEE 802.1x 検証の設定」（P.9-37）および「定期的な再認証の設定」（P.9-25）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。

Web 認証の使用

Web ブラウザを使用して、IEEE 802.1x 機能をサポートしないクライアントを認証することができます。この機能は、同一共有ポート内で最大 8 ユーザを認証することが可能で、適切なポリシーを共有ポート上の各エンド ホストに適用することができます。

Web 認証のみを使用してポートを設定することが可能です。また、まず IEEE 802.1x 認証を試行してみて、クライアントが IEEE 802.1x 認証をサポートしていない場合は Web 認証を使用するようにポート設定することも可能です。

Web 認証には、2 種類の Cisco AV のペア アトリビュートが必要です。

- 最初のアトリビュート `priv-lvl=15` は、常に *15* に設定しておく必要があります。これにより、スイッチにログインするユーザの権限レベルが設定されます。
- 次のアトリビュートが、Web 認証ホストに対して適用されるアクセス リストです。構文は、IEEE 802.1x ユーザ単位 ACL と似ています。ただし、`ip:inacl` の代わりに、このアトリビュートは `proxyacl` で開始され、各エントリの `source` フィールドは `any` でなければなりません　（認証後、ACL が適用された時にクライアント IP アドレスが `any` フィールドを置き換えます）。

  次に例を示します。

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

（注）　*proxyacl* エントリは、すべての許可済ネットワーク アクセスのタイプを決定します。

詳細については、「Web 認証の設定」（P.9-38）を参照してください。

自動 MAC チェックによる Web 認証

自動 MAC チェックによる Web 認証を使用して、IEEE 802.1x 機能または Web ブラウザ機能をサポートしていないクライアントを認証することができます。これにより、プリンタなどのエンド ホストを MAC アドレスだけで自動的に認証することが可能になります。他に必要な設定はありません。

自動 MAC チェックによる Web 認証は、Web 認証のスタンドアロン モードでのみ動作します。Web 認証を IEEE 802.1x 認証のフォールバックとして設定している場合、この方法は使用できません。

自動 MAC チェックを正しく実行するには、デバイスの MAC アドレスを Access Control Server（ACS）に設定する必要があります。プリンタなどの管理対象デバイスは、自動 MAC チェックを使用することで Web 認証を省略できます。

（注）　同一スイッチの異なるポートに設定された（自動 MAC チェックによる）Web 認証と IEEE 802.1x MAC 認証の相互運用性はサポートされません。

IEEE 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。

- 「IEEE 802.1x 認証のデフォルト設定」（P.9-19）
- 「IEEE 802.1x 認証設定時の注意事項」（P.9-20）
- 「IEEE 802.1x 認証の設定」（P.9-22）（必須）
- 「スイッチおよび RADIUS サーバ間の通信の設定」（P.9-23）（必須）
- 「ホスト モードの設定」（P.9-25）（任意）
- 「定期的な再認証の設定」（P.9-25）（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.9-26）（任意）

- 「待機時間の変更」（P.9-26）（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.9-27）（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.9-28）（任意）
- 「再認証回数の設定」（P.9-28）（任意）
- 「IEEE 802.1x アカウンティングの設定」（P.9-29）（任意）
- 「ゲスト VLAN の設定」（P.9-30）（任意）
- 「制限付き VLAN の設定」（P.9-31）（任意）
- 「アクセス不能認証バイパス機能の設定」（P.9-33）（任意）
- 「WoL を使用した IEEE 802.1x 認証の設定」（P.9-35）（任意）
- 「MAC 認証バイパスの設定」（P.9-36）（任意）
- 「NAC レイヤ 2 IEEE 802.1x 検証の設定」（P.9-37）（任意）
- 「Web 認証の設定」（P.9-38）（任意）
- 「ポート上での IEEE 802.1x 認証のディセーブル化」（P.9-40）（任意）
- 「IEEE 802.1x 認証設定のデフォルト値へのリセット」（P.9-41）（任意）

IEEE 802.1x 認証のデフォルト設定

表 9-2 に、IEEE 802.1x 認証のデフォルト設定を示します。

表 9-2　IEEE 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 IEEE 802.1x イネーブル ステート	ディセーブル
ポート単位の IEEE 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の IEEE 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（AAA; 認証、許可、アカウンティング）	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし • 1812. • 指定なし
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
再認証回数	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 9-2　IEEE 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。この値は設定変更ができません。）
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

IEEE 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。

- 「IEEE 802.1x 認証」（P.9-20）
- 「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.9-21）
- 「MAC 認証バイパス」（P.9-22）

IEEE 802.1x 認証

IEEE 802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 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。
- IEEE 802.1x 対応ポートを（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。
- IEEE 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。

  IEEE 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 IEEE 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、IEEE 802.1x 認証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、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 IEEE 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、IEEE 802.1x 認証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、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 IEEE 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、IEEE 802.1x 認証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。
  - EtherChannel ポート：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 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、IEEE 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 RSPAN 宛先ポート：SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにできます。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、IEEE 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、IEEE 802.1x 認証をイネーブルにできます。

- 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 IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 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

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- IEEE 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 IEEE 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、IEEE 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。
- Dynamic Host Configuration Protocol（DHCP）クライアントが接続する IEEE 802.1x ポートにゲスト VLAN を設定したあとは、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の IEEE 802.1x 認証プロセスを再開するための設定を変更することもできます。IEEE 802.1x 認証プロセスの設定を減らしてください（**dot1x timeout quiet-period** および **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）。設定を減らす量は、接続している IEEE 802.1x クライアント 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 IEEE 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。
  - IEEE 802.1x ポート上では、アクセス不能認証バイパス機能および制限付き VLAN を設定できます。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、IEEE 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

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は IEEE 802.1x 認証のものと同じです。詳細については、「IEEE 802.1x 認証」（P.9-20）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。

旧版のソフトウェア リリースからのアップグレード

Cisco IOS Release 12.2(25)SEE では、IEEE 802.1x 認証の実装が旧リリースから変更されています。IEEE 802.1x 認証がイネーブルの場合、PortFast に関する情報は設定には追加されず、この情報は実行コンフィギュレーションに表示されます。

```
dot1x pae authenticator
```

IEEE 802.1x 認証の設定

IEEE 802.1x ポートベース認証を設定するには、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、IEEE 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。

IEEE 802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	IEEE 802.1x 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが**指定されていない**場合に使用するデフォルトのリストを作成するには、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。 **（注）** **group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**dot1x system-auth-control**	スイッチ上で IEEE 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*	IEEE 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	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。 機能の相互作用については、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）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 dot1x**	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。

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。 *hostname* | *ip-address* 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** *port-number* 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、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.8-29）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 IEEE 802.1x 許可ポート上で、単一のホスト（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。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	**dot1x host-mode** {**single-host** | **multi-host**}	キーワードの意味は次のとおりです。 • **single-host**：IEEE 802.1x 許可ポートで単一のホスト（クライアント）の接続を許可します。 • **multi-host**：単一のホストの認証後に IEEE 802.1x 許可ポートで複数のホストの接続を許可します。 指定するインターフェイスで、**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。
ステップ 7	**show dot1x interface** *interface-id*	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。

ポート上で複数のホストをディセーブルにするには、**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、IEEE 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 gigabitethernet/0/1

Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

定期的な再認証の設定

IEEE 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。

	コマンド	目的
ステップ 3	**dot1x reauthentication**	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）をイネーブルにします。
ステップ 4	**dot1x timeout reauth-period** {*seconds* | **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 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show dot1x interface** *interface-id*	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。

定期的な再認証をディセーブルにするには、**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 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.9-25）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。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あと、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 dot1x 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。

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 dot1x 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。

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

スイッチからクライアントへの再送信時間を変更できるだけでなく、（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 ～ 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 dot1x 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。

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 dot1x 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。

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
```

IEEE 802.1x アカウンティングの設定

IEEE 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 IEEE 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになったあと、IEEE 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、IEEE 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、IEEE 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、IEEE 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。IEEE 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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）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。
	または	または
	switchport mode private-vlan host	ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。

	コマンド	目的
ステップ 5	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を IEEE 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、IEEE 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 dot1x interface** *interface-id*	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。

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 IEEE 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、IEEE 802.1x ポートの DHCP クライアント接続時に、VLAN 2 を IEEE 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)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x 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、IEEE 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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードにします。 または ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブな VLAN を、IEEE 802.1x 制限付き VLAN に指定します。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、IEEE 802.1x 制限付き VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show dot1x interface** *interface-id*	（任意）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。

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。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードにします。 または ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブな VLAN を、IEEE 802.1x 制限付き VLAN に指定します。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、IEEE 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 dot1x interface** *interface-id*	（任意）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。

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 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
ステップ 3	**radius-server deadtime** *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分です（24 時間）。デフォルト値は 0 分です。

	コマンド	目的
ステップ 4	**radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	（任意）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。 • **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** *udp-port*：RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 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。
ステップ 5	**dot1x critical** {**eapol** | **recovery delay** ***milliseconds***}	（任意）アクセス不能認証バイパスのパラメータを設定します。 **eapol**：スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 **recovery delay** *milliseconds*：使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポート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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）を参照してください。

	コマンド	目的
ステップ 7	**dot1x critical** [**recovery action reinitialize** | **vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。 • **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 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show dot1x** [**interface** *interface-id*]	（任意）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。

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 abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 0/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した IEEE 802.1x 認証の設定

WoL を使用した IEEE 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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）を参照してください。
ステップ 3	**dot1x control-direction** {**both** | **in**}	ポートで WoL を使用して IEEE 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。 • **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。

	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 dot1x 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。

スイッチで WoL を使用した IEEE 802.1x 認証をディセーブルにするには、**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 IEEE 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)# 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、「IEEE 802.1x 認証設定時の注意事項」（P.9-20）を参照してください。
ステップ 3	**dot1x port-control auto**	ポート上で IEEE 802.1x 認証をイネーブルにします。
ステップ 4	**dot1x mac-auth-bypass** [**eap**]	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。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show dot1x interface** *interface-id*	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。

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
```

NAC レイヤ 2 IEEE 802.1x 検証の設定

Cisco IOS Release 12.2(25)SED 以降では、NAC レイヤ 2 IEEE 802.1x 検証を設定できます。これは、RADIUS サーバを使用した IEEE 802.1x 認証とも呼ばれます。

NAC レイヤ 2 IEEE 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 IEEE 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、IEEE 802.1x ゲスト VLAN として設定できます。
ステップ 4	**dot1x reauthentication**	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）をイネーブルにします。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **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 dot1x interface** ***interface-id***	IEEE 802.1x 認証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。

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
```

Web 認証の設定

Web 認証の設定後に AAA および RADIUS を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。このステップにより、RADIUS 認証を使用して AAA がイネーブルになり、デバイス トラッキング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	**aaa new-model**	AAA をイネーブルにします。

ステップ 3	**aaa authentication login default 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。
		コンソールで、**aaa authentication login** コマンドを入力後にスイッチ コンソールにアクセスするために、ユーザ名とパスワードが要求されます。ユーザ名とパスワードを要求されたくない場合は、2 番めのログイン認証一覧を設定します。
		`Switch# config t`
		`Switch(config)# aaa authentication login line-console none`
		`Switch(config)# line console 0`
		`Switch(config-line)# login authentication line-console`
		`Switch(config-line)# end`

ステップ 4	**aaa authorization auth-proxy default group radius**	認証プロキシ（auth-proxy）認証に RADIUS を使用します。
ステップ 5	**radius-server host key *radius-key***	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。
ステップ 6	**radius-server attribute 8 include-in-access-req**	アクセス要求またはアカウント要求パケットで Framed-IP-Address RADIUS アトリビュート（アトリビュート [8]）を送信するようにスイッチを設定します。
ステップ 7	**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 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	**end**	特権 EXEC モードに戻ります。

次に、AAA をイネーブルにし、RADIUS 認証を使用し、デバイス トラッキングをイネーブルにする例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# radius-server host1.1.1.2 key key1
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# radius-server vsa send authentication
Switch(config)# ip device tracking
Switch(config) end
```

ポートで Web 認証を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す。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コ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 name *rule* proxy http**	Web 認証ルールを定義します。 **（注）** Web 認証と NAC レイヤ 2 IP 検証に同じルールを使用することはできません。NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
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**	ポートをアクセス モードにします。
ステップ 5	**ip access-group** *access-list* **in**	Web 認証前にネットワーク トラフィックに適用するデフォルトの Access Control List（ACL; アクセス コントロール リスト）を指定します。
ステップ 6	**ip admission** *rule*	IP 管理ルールをインターフェイスに適用します。
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 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。

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# ip access-group policy1 in
Switch(config-if)# ip admission rule1
Switch(config-if)# end
```

フォールバック メソッドとしての Web 認証のある IEEE 802.1x 認証をスイッチ ポートに設定するには、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	**ip admission name *rule* proxy http**	Web 認証ルールを定義します。
ステップ 3	**fallback profile *fallback-profile***	Web 認証を使用して IEEE 802.1x ポートでクライアントを認証することができるように、フォールバック プロファイルを定義します。
ステップ 4	**ip access-group *policy* in**	Web 認証前にネットワーク トラフィックに適用するデフォルトの ACL を指定します。
ステップ 5	**ip admission** *rule*	IP 管理ルールをプロファイルと関連付けして、Web 認証で接続するクライアントがこのルールを使用するように指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport mode access**	ポートをアクセス モードにします。

	コマンド	目的
ステップ 9	**dot1x port-control auto**	インターフェイス上で IEEE 802.1x 認証をイネーブルにします。
ステップ 10	**dot1x fallback** *fallback-profile*	IEEE 802.1x サプリカントがポートで検出されてない場合に、Web 認証を使用してクライアントを認証するようにポートを設定します。次回 IEEE 802.1x フォールバックがインターフェイスで呼び出される際に、フォールバック プロファイルのグローバル コンフィギュレーションへの変更が有効になります。 **（注）** ポートがマルチドメイン認証に設定されている場合、Web 認証を IEEE 802.1x のフォールバック メソッドとして使用することができません。
ステップ 11	**exit**	特権 EXEC モードに戻ります。
ステップ 12	**show dot1x interface** *interface-id*	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。

次に、フォールバック メソッドとしての Web 認証のある IEEE 802.1x 認証を設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback fallback1
Switch(config-if)# end
```

dot1x fallback 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。**ip admission name** および **ip access-group** コマンドの詳細については、Cisco.com の『*Network Admission Control Software Configuration Guide*』を参照してください。

ポート上での IEEE 802.1x 認証のディセーブル化

IEEE 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 IEEE 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 IEEE 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 dot1x 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。

IEEE 802.1x Port Access Entity（PAE; ポート アクセス エンティティ）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 IEEE 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。

次に、IEEE 802.1x 認証をポートでディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no dot1x pae authenticator
```

IEEE 802.1x 認証設定のデフォルト値へのリセット

IEEE 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**	IEEE 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 dot1x 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。

IEEE 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 IEEE 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 IEEE 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 IEEE 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 IEEE 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

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.10-1）
- 「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.10-5）
- 「イーサネット インターフェイスの設定」（P.10-10）
- 「システム MTU の設定」（P.10-19）
- 「インターフェイスのモニタおよびメンテナンス」（P.10-20）

（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。また、インターフェイスの物理特性に応じた設定手順についても説明します。

ここでは、次のようなインターフェイス タイプについて説明します。

- 「ポートベースの VLAN」（P.10-2）
- 「スイッチ ポート」（P.10-2）
- 「EtherChannel ポート グループ」（P.10-3）
- 「デュアルパーパス アップリンク ポート」（P.10-4）
- 「インターフェイスの接続」（P.10-5）

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 12 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。

通常範囲の VLAN（VLAN ID が 1 ～ 1005）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 config-vlan モードを開始するか、**vlan database** 特権 EXEC コマンドを使用して VLAN データベース コンフィギュレーション モードを開始します。VLAN ID 1 ～ 1005 の VLAN 設定は、VLAN データベースに保存されます。拡張範囲 VLAN（VLAN ID が 1006 ～ 4094）を設定するには、config-vlan モードを使用し、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。拡張範囲 VLAN は、VLAN データベースに追加されません。VTP モードがトランスペアレントである場合は、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に保存されるので、**copy running-config startup-config** 特権 EXEC コマンドを実行して、これをスイッチのスタートアップ コンフィギュレーション ファイルに保存できます。

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、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 ポートは、物理インターフェイスおよび対応するレイヤ 2 プロトコルの管理に使用されます。

スイッチ ポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。

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 12 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 ポートがタグ付きパケット（タグ付き IEEE 802.1Q）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 IEEE 802.1x 認証の利用」（P.9-9）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 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 14 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。IEEE 802.1Q トランク ポートのみサポートされます。

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 12 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 34 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 Catalyst 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 SFP 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。

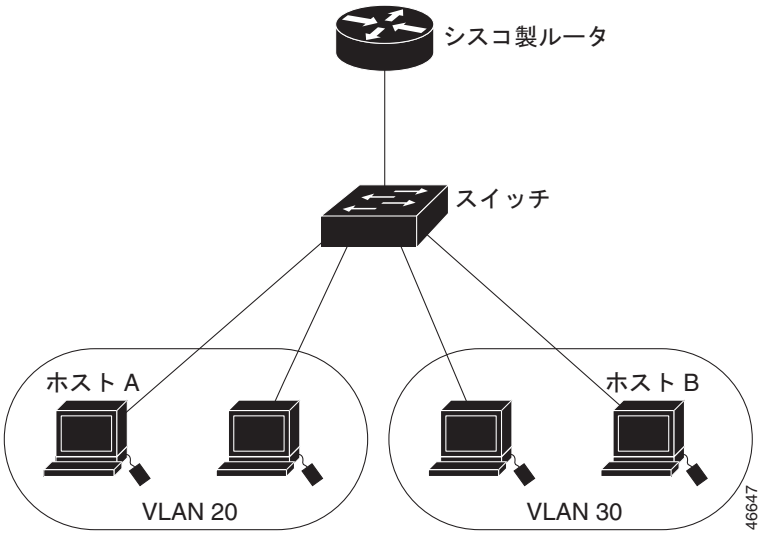
デフォルトでは、スイッチは最初にリンクするインターフェイス タイプを動的に選択します。ただし、**media-type** インターフェイス コンフィギュレーション コマンドを使用して、手動で RJ-45 コネクタまたは SFP モジュール コネクタを選択できます。デュアルパーパス アップリンクのデュプレックス設定および速度設定については、「インターフェイス速度およびデュプレックス パラメータの設定」（P.10-14）を参照してください。

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。

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 10-1 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 10-1　　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.10-7）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：10/100 Mb/s イーサネット対応のファスト イーサネット（fastethernet または fa）、10/100/1000 Mb/s イーサネット ポート対応のイーサネット（gigabitethernet または gi）、または SFP モジュール ギガビット イーサネット インターフェイス。
- 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（Catalyst 2960 スイッチでは常に 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、fastethernet0/1 または gigabitethernet0/1 のように、常に 1 で始まります。スイッチに向かって左のポートから順に番号付けされています。0/1.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。0/1. 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。

スイッチ上のインターフェイスの位置を物理的に確認することで、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。インターフェイスのタイプおよびコネクタ番号を特定します。次の例では、ギガビット イーサネット ポート 1 が選択されています。

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

（注）　インターフェイス タイプとインターフェイス番号の間にスペースを入れる必要はありません。たとえば、前出の行の場合は、**gigabitethernet 0/1**、**gigabitethernet0/1**、**gi 0/1**、**gi 0/1** のいずれかを指定できます。

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.10-20）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** {*port-range* | **macro** *macro_name*}	設定するインターフェイス範囲（VLAN または物理ポート）を指定し、インターフェイス コンフィギュレーション モードを開始します。 • **interface range** 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.10-8）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。

- *port-range* の有効なエントリは次のとおりです。
  - **vlan** *vlan-ID*、VLAN ID は 1 ～ 4094。

（注）　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* は 1 ～ 6。

（注）　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、コマンド **interface range gigabitethernet0/1 - 4** は有効な範囲ですが、コマンド **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 ～ 4 の速度を 100 Mb/s に設定します。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 4
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*	*macro_name* 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。

- *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 ～ 4094。

    （注）　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* は 1 ～ 6。

    （注）　ポート チャネルを指定してインターフェイス範囲を使用する場合は、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
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 *macro1* を作成する例を示します。

```
Switch# configure terminal
Switch(config)# define interface-range macro1 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.10-11）
- 「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.10-12）
- 「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.10-13）
- 「IEEE 802.3x フロー制御の設定」（P.10-16）
- 「インターフェイスでの Auto-MDIX の設定」（P.10-17）
- 「インターフェイスに関する記述の追加」（P.10-18）

イーサネット インターフェイスのデフォルト設定

表 10-1 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 12 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 21 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。

表 10-1　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
VLAN 許容範囲	VLAN 1 ～ 4094
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1
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 34 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。
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.21-7）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.21-3）を参照してください。
保護ポート	ディセーブル 「保護ポートの設定」（P.21-5）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.21-10）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.17-10）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。
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。

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 Catalyst 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。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.10-4）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。
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。このポートにケーブルを接続している場合、RJ-45 側がダウンの状態になっている、または接続されていない場合でも、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の状態になっている、または SFP モジュールが接続されていない場合でも、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.10-13）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** *interface-id* **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、**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。

インターフェイス タイプを変更すると、速度およびデュプレックス設定は削除されます。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。

Catalyst 2960 スイッチと 100BASE-*x*（*-x* は、-BX、-FX-FE、および-LX）SFP モジュールは、以下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

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 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、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.10-13）
- 「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.10-14）

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。

注意　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。

	コマンド	目的
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.10-13）を参照してください。
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.10-13）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 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
```

（注）　インターフェイス gi0/1 から gi0/16 の場合、サーバ方向の内部インターフェイスのみなので、サーバ速度とデュプレックス設定は適用されません。インターフェイス gi0/17 から gi0/20 の場合、SFP モジュール モードで動作しているときはサーバ速度とデュプレックス設定は適用されません。インター

フェイス gi0/23 から gi0/24 の場合、media-type internal に設定されているときは、サーバ速度とデュプレックス設定は適用されません。詳細については、「アクセス ポート」（P.10-2）を参照してください。

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一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズ フレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注）　Catalyst 2960 ポートは、ポーズ フレームを受信できますが、送信できません。

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	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**flowcontrol** {**receive**} {**on** | **off** | **desired**}	ポートのフロー制御モードを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id*	インターフェイス フロー制御の設定を確認します。
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。

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ちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、『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。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 10-2 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。

表 10-2　リンク状態と Auto-MDIX の設定

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

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed auto**	接続されたデバイスと速度の自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 4	**duplex auto**	接続されたデバイスとデュプレックス モードの自動ネゴシエーションを行うようにインターフェイスを設定します。
ステップ 5	**mdix auto**	インターフェイス上で Auto-MDIX をイネーブルにします。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show controllers ethernet-controller** *interface-id* **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。
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。

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
```

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** または **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。

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

スイッチ スタック上の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 jumbo mtu** 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。スイッチ スタック上のすべての 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。

（注） 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、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 10/100 インターフェイスで発信されるジャンボ フレームは廃棄されます。

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 jumbo mtu 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.10-20）
- 「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.10-21）
- 「インターフェイスのシャットダウンおよび再起動」（P.10-21）

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 10-3 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 10-3　インターフェイス用の show コマンド

コマンド	目的
show interfaces [*interface-id*]	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**]	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リストを表示します。
show interfaces [*interface-id*] **switchport**	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**	1 つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
show ip interface [*interface-id*]	IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [*interface-id*] **stats**	インターフェイスのパスごとに入出力パケットを表示します。
show interfaces transceiver properties	（任意）インターフェイスの速度およびデュプレックス設定を表示します。
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	SFP モジュールに関する物理および動作ステータスを表示します。

表 10-3　インターフェイス用の show コマンド （続き）

コマンド	目的
show running-config interface [*interface-id*]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア構成、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 *interface-id* **phy**	インターフェイスの Auto-MDIX 動作ステートを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 10-4 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 10-4　インターフェイス用の clear コマンド

コマンド	目的
clear counters [*interface-id*]	インターフェイス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。

（注）　**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** | **gigabitethernet**} *interface-id*} | {**port-channel** *port-channel-number*}	設定するインターフェイスを選択します。
ステップ 3	**shutdown**	インターフェイスをシャットダウンします。

	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。

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。



CHAPTER 11

SmartPort マクロの設定

この章では、Catalyst 2960 スイッチに Smartport マクロを設定し適用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。

- 「SmartPort マクロの概要」（P.11-1）
- 「SmartPort マクロの設定」（P.11-2）
- 「SmartPort マクロの表示」（P.11-8）

SmartPort マクロの概要

SmartPort マクロは、共通の設定を保存および共有するのに便利です。SmartPort マクロを使用すると、ネットワークでのスイッチの場所に基づいて機能および設定をイネーブルにしたり、ネットワークを通じて大規模な設定を配置したりできます。

各 SmartPort マクロは、定義した CLI（コマンドライン インターフェイス）コマンドの集まりです。SmartPort マクロは、既存の CLI コマンドの集まりであり、新しい CLI コマンドは含まれていません。

インターフェイスに SmartPort マクロを適用すると、マクロ内の CLI コマンドがインターフェイスに対して設定されます。インターフェイスに SmartPort マクロを適用しても、インターフェイスの既存の設定は失われません。新しいコマンドがインターフェイスに追加され、実行コンフィギュレーション ファイルに保存されます。

スイッチ ソフトウェアには、シスコの SmartPort のマクロがデフォルトで組み込まれています（表 11-1 を参照）。これらのマクロやコマンドは、**show parser macro** ユーザ EXEC コマンドを使用して表示できます。

表 11-1　シスコのデフォルト SmartPort マクロ

マクロ名[1]	説明
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。

表 11-1　シスコのデフォルト SmartPort マクロ （続き）

マクロ名[1]	説明
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	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	スイッチと WAN ルータを接続する場合、このインターフェイス コンフィギュレーション マクロを使用します。
cisco-wireless	スイッチとワイヤレス アクセス ポ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。

また、シスコが推奨するテスト済みのベースライン コンフィギュレーションのテンプレート集も提供されています。オンライン リファレンス ガイドのテンプレートには、利用するポートに応じた SmartPort マクロを作成できる CLI コマンドが含まれています。コンフィギュレーション テンプレートを使用して SmartPort マクロを作成し、シスコ推奨のネットワーク設計および設定を構築し、展開できます。シスコ推奨のコンフィギュレーション テンプレートの詳細については、Smartport の Web サイトを参照してください。

http://www.cisco.com/go/smartports

SmartPort マクロの設定

新しい SmartPort マクロを作成するか既存の SmartPort マクロをテンプレートにして、アプリケーション専用の新しい SmartPort マクロを作成できます。作成したマクロは、スイッチ、スイッチ インターフェイス、またはインターフェイス範囲にグローバルに適用できます。

ここでは、次の設定情報について説明します。

- 「SmartPort マクロのデフォルト設定」（P.11-2）
- 「SmartPort マクロ設定時の注意事項」（P.11-3）
- 「SmartPort マクロの作成」（P.11-4）
- 「SmartPort マクロの適用」（P.11-5）
- 「シスコのデフォルト SmartPort マクロの適用」（P.11-6）

SmartPort マクロのデフォルト設定

イネーブル設定の SmartPort マクロはありません。

SmartPort マクロ設定時の注意事項

スイッチでマクロを設定するときには、次の注意事項に従ってください。

- マクロを作成するときは、**exit** または **end** コマンドを使用しないでください。または **interface** *interface-id* を使用して、コマンド モードを変更しないでください。**exit** または **end**、または **interface** *interface-id* に続くコマンドが別のコマンド モードで実行されることがあるためです。
- マクロを作成するときは、すべての CLI コマンドを同じコンフィギュレーション モードにします。
- 一意の値を割り当てる必要のあるマクロを作成するときは、**parameter** *value* キーワードを使用して、インターフェイスに特定の値を指定します。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。キーワードの完全一致は、長いキーワード ストリングの一部に完全一致する部分がある場合でも、そのキーワードは一致したと見なされ、それに対応する値に置き換えられます。
- マクロ名は大文字と小文字が区別されます。たとえば、**macro name Sample-Macro** および **macro name sample-macro** は、別々の 2 つのマクロになります。
- 一部のマクロには、パラメータ値を必要とするキーワードを含んでいる場合があります。マクロで必要な値を表示するには、**macro global apply** *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 apply** *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。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。
- 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。
- コマンドを追加または削除してマクロ定義を変更する場合、元のマクロを適用したインターフェイスに変更は反映されません。新規または変更済みのコマンドを適用するには、インターフェイスに更新済みマクロを再適用する必要があります。
- 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。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。
- 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。

スイッチ ソフトウェアには、シスコの SmartPort のマクロがデフォルトで組み込まれています（表 11-1 を参照）。これらのマクロやコマンドは、**show parser macro** ユーザ EXEC コマンドを使用して表示できます。

シスコのデフォルト SmartPort マクロをインターフェイスに適用する場合、次の注意事項に従ってください。

- スイッチ上のマクロをすべて表示するには、**show parser macro** ユーザ EXEC コマンドを使用します。特定のマクロの内容を表示するには、**show parser macro** *macro-name* ユーザ EXEC コマンドを使用します。
- **$** で始まるキーワードは、一意のパラメータ値が必要であることを意味します。**parameter** *value* キーワードを使用して、シスコのデフォルト マクロに必要な値を加えます。

  シスコのデフォルト マクロでは、必要なキーワードを特定するのに **$** 文字を使用します。マクロを作成する場合、キーワードの定義に使用する **$** 文字に制限はありません。

SmartPort マクロの作成

Smartport マクロを作成するには、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	**macro name** *macro-name*	マクロ定義を作成し、マクロ名を入力します。マクロ定義には、最大 3000 文字を使用できます。 1 行ごとに 1 つのマクロ コマンドを指定します。マクロを終了するには、**@** 文字を使用します。マクロ内にコメント テキストを入力するには、行の最初に **#** 文字を使用します。 （任意）キーワードを指定するのにヘルプ ストリングを使用することで、マクロ内にキーワードを定義できます。マクロで使用するキーワードを定義するには、**# macro keywords** *word* を入力します。スペースで区切って、マクロにヘルプ ストリング キーワードを 3 つまで入力できます。 マクロ名は大文字と小文字が区別されます。たとえば、**macro name Sample-Macro** および **macro name sample-macro** は、別々の 2 つのマクロになります。 **exit** または **end** コマンドを使用しないこと、またはマクロで **interface** *interface-id* を使用して、コマンド モードを変更しないことを推奨します。**exit** または **end**、または **interface** *interface-id* に続くコマンドが別のコマンド モードで実行されることがあるからです。最良の結果を出すには、マクロ内のすべてのコマンドが同じコンフィギュレーション モードである必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show parser macro name** *macro-name*	マクロが作成されたことを確認します。

no 形式の **macro name** グローバル コンフィギュレーション コマンドでは、マクロ定義だけが削除されます。マクロがすでに適用されているインターフェイスの設定に影響はありません。

次に、スイッチポート アクセス VLAN およびセキュア MAC（メディア アクセス制御）アドレス数を定義し、また **# macro keywords** を使用してヘルプ ストリング キーワードを 2 つ含むマクロを作成する例を示します。

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
```

```
#macro keywords $VLANID $MAX
@
```

SmartPort マクロの適用

Smartport マクロを適用するには、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	**macro global** {**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スイッチに適用するには、**macro global apply** *macro-name* 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** *macro-name* を指定します。 （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。キーワードの値のペアは、最大 3 つまで入力できます。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。 一部のマクロには、パラメータ値を必要とするキーワードを含んでいる場合があります。**macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値の一覧が表示されます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。
ステップ 3	**macro global description** *text*	（任意）スイッチに適用するマクロの説明を入力します。
ステップ 4	**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 5	**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 6	**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インターフェイスに適用するには、**macro apply** *macro-name* 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 trace** *macro-name* を指定します。 （任意）インターフェイスに固有の一意のパラメータ値を指定します。キーワードの値のペアは、最大 3 つまで入力できます。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。 一部のマクロには、パラメータ値を必要とするキーワードを含んでいる場合があります。**macro apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値の一覧が表示されます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。
ステップ 7	**macro description** *text*	（任意）インターフェイスに適用するマクロの説明を入力します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show parser macro description** [**interface** *interface-id*]	マクロがインターフェイスに適用されたことを確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチ上のグローバル マクロ適用済みの設定を削除するには、マクロ内にある各コマンドの **no** バージョンのみを入力します。インターフェイス上のマクロ適用済みの設定を削除するには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを入力します。

次に、**snmp** という名前のユーザ作成マクロを適用し、ホスト名アドレスを **test-server** に設定し、IP precedence 値を **7** に設定する例を示します。

```
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

次に、**macro global trace** 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** という名前のユーザ作成マクロをデバッグし、スイッチに適用されたときのマクロ内の構文エラーまたは設定エラーを検出する例を示します。

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

次に、**desktop-config** という名前のユーザ作成マクロを適用し、設定を確認する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# macro apply desktop-config
Switch(config-if)# end
Switch# show parser macro description
Interface    Macro Description
---------------------------------------------------------------
Gi0/2      desktop-config
---------------------------------------------------------------
```

次に、**desktop-config** という名前のユーザ作成マクロを適用し、VLAN 1 での動作を VLAN 25 に置き換える例を示します。

```
Switch(config-if)# macro apply desktop-config vlan 25
```

シスコのデフォルト SmartPort マクロの適用

Smartport マクロを適用するには、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 SmartPort マクロを表示します。
ステップ 2	**show parser macro** *macro-name*	適用する特定のマクロを表示します。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	**parameter** *value* キーワードを使用して、シスコのデフォルト マクロに必要な値を加え、スイッチにマクロを適用します。**$** で始まるキーワードは、一意のパラメータ値が必要であることを意味します。 **macro global apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値の一覧が表示されます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。
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。

	コマンド	目的
ステップ 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	**parameter** *value* キーワードを使用して、シスコのデフォルト マクロに必要な値を加え、インターフェイスにマクロを適用します。**$** で始まるキーワードは、一意のパラメータ値が必要であることを意味します。 **macro apply** *macro-name* **?** コマンドを使用すると、マクロで必要な値の一覧が表示されます。キーワード値を入力しないでマクロを適用すると、コマンドは無効になり適用されません。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	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。

スイッチ上のグローバル マクロ適用済みの設定を削除するには、マクロ内にある各コマンドの **no** バージョンのみを入力します。インターフェイス上のマクロ適用済みの設定を削除するには、**default interface** *interface-id* インターフェイス コンフィギュレーション コマンドを入力します。

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

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
-------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# gigabitethernet0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

SmartPort マクロの表示

SmartPort マクロを表示するには、表 11-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 11-2　SmartPort マクロを表示するコマンド

コマンド	目的
show parser macro	設定されているすべてのマクロを表示します。
show parser macro name *macro-name*	特定のマクロを表示します。
show parser macro brief	設定されているマクロ名を表示します。
show parser macro description [**interface** *interface-id*]	すべてのインターフェイスまたは指定されたインターフェイスのマクロ説明を表示します。



CHAPTER 12

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。

（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。

- 「VLAN の概要」（P.12-1）
- 「標準範囲 VLAN の設定」（P.12-4）
- 「拡張範囲 VLAN の設定」（P.12-11）
- 「VLAN の表示」（P.12-14）
- 「VLAN トランクの設定」（P.12-14）
- 「VMPS の設定」（P.12-24）

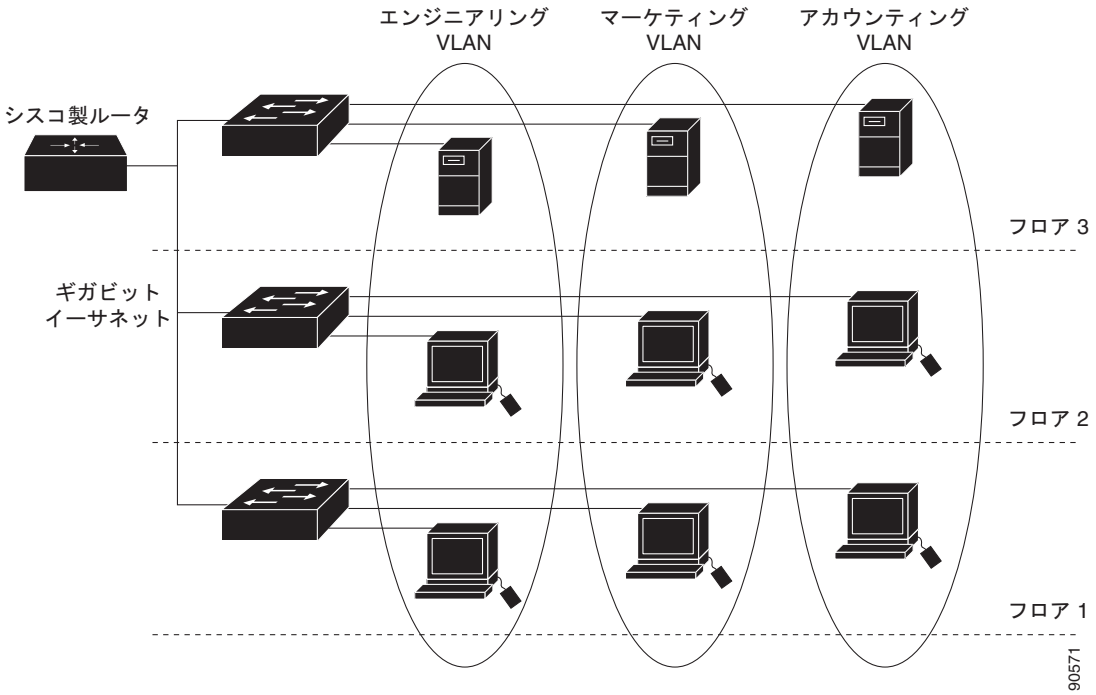
VLAN の概要

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 12-1 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 15 章「STP の設定」を参照してください。

（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 13 章「VTP の設定」を参照してください。

図 12-1 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 12-1　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 は、VLAN ID が 1 ～ 1005 の標準範囲 VLAN のみを学習します。1005 を超える VLAN ID は拡張範囲 VLAN と呼ばれ、VLAN データベースには格納されません。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。

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.12-5）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。

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 12-1 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 12-1　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.12-11）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.12-16）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、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.12-27）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 14 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 に作用しません。

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 12-4（P.12-15）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.6-20）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）。

（注） スイッチが VTP トランスペアレント モードの場合、拡張範囲 VLAN（ID が 1006 ～ 4094 の VLAN）も作成できます。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。「拡張範囲 VLAN の設定」（P.12-11）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。

注意 *vlan.dat* ファイルを手動で削除しようとすると、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応するコマンド リファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、第 13 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

（注）　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。

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.12-5）
- 「標準範囲 VLAN 設定時の注意事項」（P.12-5）
- 「VLAN コンフィギュレーション モードのオプション」（P.12-6）
- 「VLAN 設定の保存」（P.12-7）
- 「イーサネット VLAN のデフォルト設定」（P.12-7）
- 「イーサネット VLAN の作成または変更」（P.12-8）
- 「VLAN の削除」（P.12-10）
- 「VLAN へのスタティック アクセス ポートの割り当て」（P.12-11）

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。
- スイッチは VTP トランスペアレント モード（VTP はディセーブル）で、VLAN ID 1006 ～ 4094 もサポートします。これらは拡張範囲 VLAN であり、設定オプションには制限があります。拡張範囲 VLAN は VLAN データベースには格納されません。「拡張範囲 VLAN の設定」（P.12-11）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 16 章「MSTP の設定」を参照してください。

VLAN コンフィギュレーション モードのオプション

標準範囲 VLAN（VLAN ID が 1 ～ 1005）を設定するには、次に示す 2 つのコンフィギュレーション モードを使用します。

- 「config-vlan モードでの VLAN 設定」（P.12-6）

  config-vlan モードを開始するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力します。
- 「VLAN データベース コンフィギュレーション モードでの VLAN 設定」（P.12-6）

  VLAN データベース コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。

config-vlan モードでの VLAN 設定

config-vlan モードにアクセスするには、VLAN ID を指定して **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 12-2 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、config-vlan 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。

この config-vlan モードは、拡張範囲 VLAN（VLAN ID が 1005 より大きい）を作成するときに使用する必要があります。「拡張範囲 VLAN の設定」（P.12-11）を参照してください。

VLAN データベース コンフィギュレーション モードでの VLAN 設定

VLAN データベース コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。次に、新しい VLAN ID を指定して **vlan** コマンドを入力して VLAN を作成するか、既存の VLAN ID を入力して VLAN を変更します。デフォルトの VLAN 設定を使用するか

（表 12-2 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キーワー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** VLAN データベース コンフィギュレーション コマンドを参照してください。設定を終了したら、**apply** または **exit** を入力して、設定を有効にする必要があります。**exit** コマンドを入力すると、すべてのコマンドが適用されて、VLAN データベースが更新されます。VTP ドメイン内の他のスイッチに VTP メッセージが送信され、特権 EXEC モード プロンプトが表示されます。

VLAN 設定の保存

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 モードがサーバの場合、最初の 1005 の VLAN 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。

注意　起動時に VLAN データベース コンフィギュレーションが使用され、スタートアップ コンフィギュレーション ファイルに拡張範囲 VLAN 設定が含まれていた場合、システム起動時にこの情報は失われます。

イーサネット VLAN のデフォルト設定

表 12-2 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 12-2　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 ～ 4094 （注）　拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は VLAN データベースには保存されません。
VLAN 名	*VLANxxxx*。*xxxx* は VLAN ID 番号に等しい 4 桁の数字（先行ゼロを含む）です。	範囲なし
IEEE 802.10 SAID	100001（100000 と VLAN ID の和）	1 ～ 4294967294
MTU サイズ	1500	1500 ～ 18190
トランスレーショナル ブリッジ 1	0	0 ～ 1005
トランスレーショナル ブリッジ 2	0	0 ～ 1005
VLAN ステート	アクティブ	アクティブ、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）　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、それらを VLAN データベースに追加することはできません。「拡張範囲 VLAN の設定」（P.12-11）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.12-4）を参照してください。

config-vlan モードを使用してイーサネット 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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コ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、config-vlan 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.12-11）を参照してください。

	コマンド	目的
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 25 章「SPAN および RSPAN の設定」を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	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。

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** config-vlan コマンドを使用します。

次に、config-vlan モードを使用して、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 データベース コンフィギュレーション モードを使用することによって、イーサネット VLAN を作成または変更することもできます。

（注） VLAN データベース コンフィギュレーション モードは、RSPAN VLAN 設定または拡張範囲 VLAN をサポートしません。

VLAN データベース コンフィギュレーション モードを使用してイーサネット 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。

	コマンド	目的
ステップ 1	**vlan database**	VLAN データベース コンフィギュレーション モードを開始します。
ステップ 2	**vlan** *vlan-id* **name** *vlan-name*	番号を割り当てることによって、イーサネット VLAN を追加します。指定できる範囲は 1 ～ 1001 です。**vlan** *first-vlan-id* **end** *last-vlan-id* を入力すると、連続する VLAN の範囲を作成または変更できます。 **（注）** VLAN データベース コンフィギュレーション モードで VLAN ID を入力する場合、先行ゼロは入力しません。 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 3	**vlan** *vlan-id* **mtu** *mtu-size*	（任意）VLAN を変更するには、VLAN を指定し、MTU サイズなどの特性を変更します。

	コマンド	目的
ステップ 4	**exit**	VLAN データベースをアップデートし、アップデート情報を管理ドメイン全体に伝播して、特権 EXEC モードに戻ります。
ステップ 5	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	設定を確認します。
ステップ 6	**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 名をデフォルトの設定に戻すには、**no vlan** *vlan-id* **name** または **no vlan** *vlan-id* **mtu** VLAN データベース コンフィギュレーション コマンドを使用します。

次に、VLAN コンフィギュレーション モードを使用して、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# vlan database
Switch(vlan)# vlan 20 name test20
Switch(vlan)# exit
APPLY completed.
Exiting....
```

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no vlan** *vlan-id*	VLAN ID を入力して、VLAN を削除します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show vlan brief**	VLAN が削除されたことを確認します。
ステップ 5	**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 データベース コンフィギュレーション モードを使用して VLAN を削除するには、**vlan database** 特権 EXEC コマンド使用して、VLAN データベース コンフィギュレーション モードを開始してから、**no vlan** *vlan-id* VLAN データベース コンフィギュレーション コマンドを実行します。

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。

（注）　存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます （「イーサネット VLAN の作成または変更」（P.12-8）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。
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** *interface-id*	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

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。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。拡張範囲 VLAN を設定する場合は、必ず config-vlan モード（開始するには **vlan** *vlan-id* グローバル コンフィギュレーション コマンドを入力）を使用してください。拡張範囲は VLAN データベース コンフィギュレーション モード（開始するには **vlan database** 特権 EXEC コマンドを入力）ではサポートされません。

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。

（注）　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.12-2）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.12-12）
- 「拡張範囲 VLAN 設定時の注意事項」（P.12-12）
- 「拡張範囲 VLAN の作成」（P.12-13）

VLAN のデフォルト設定

表 12-2（P.12-8）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。

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 VLAN を追加するには、**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、config-vlan モードを開始する必要があります。VLAN データベース コンフィギュレーション モード（開始するには **vlan database** 特権 EXEC コマンドを入力）では、拡張範囲 VLAN を追加できません。
- 拡張範囲の VLAN ID 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。
- 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 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。
- グローバル コンフィギュレーション モードまたは VLAN データベース 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 のディセーブル化（VTP トランスペアレント モード）」（P.13-12）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。
- 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 16 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。このコマンドによって config-vlan モードが開始されます。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 12-2 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。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、config-vlan 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。

拡張範囲 VLAN は VLAN データベースに保存されずに、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。

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。
ステップ 3	**vlan** *vlan-id*	拡張範囲 VLAN ID を入力して、config-vlan 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）** config-vlan モードでは CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、**mtu** *mtu-size* コマンドおよび **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.25-17）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 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。

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.12-11）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、config-vlan 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。VLAN データベース内の標準範囲 VLAN（1 ～ 1005）を表示するには、**show** VLAN データベース コンフィギュレーション コマンド（開始するには **vlan database** 特権 EXEC コマンドを入力）を使用します。

表 12-3 に、VLAN をモニタするためのコマンドを示します。

表 12-3　VLAN モニタ コマンド

コマンド	コマンド モード	目的
show	VLAN データベース コンフィギュレーション	VLAN データベース内の VLAN のステータスを表示します。
show current [*vlan-id*]	VLAN データベース コンフィギュレーション	VLAN データベース内のすべての VLAN または特定の VLAN のステータスを表示します。
show interfaces [**vlan** *vlan-id*]	特権 EXEC	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*]	特権 EXEC	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.12-14）
- 「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.12-16）
- 「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.12-16）
- 「トランク ポートの負荷分散の設定」（P.12-21）

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。Catalyst 2960 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 34 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 12-4 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 12-4　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 *trunk* または *desirable* モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは **dynamic auto** です。
switchport mode dynamic desirable	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、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 12-5 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 12-5　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 ～ 4094
プルーニングに適格な VLAN 範囲	VLAN 2 ～ 1001
デフォルト VLAN（アクセス ポート用）	VLAN 1
ネイティブ VLAN（IEEE 802.1Q トランク用）	VLAN 1

トランク ポートとしてのイーサネット インターフェイスの設定

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.12-17）
- 「トランクでの許可 VLAN の定義」（P.12-18）
- 「プルーニング適格リストの変更」（P.12-20）
- 「タグなしトラフィック用ネイティブ VLAN の設定」（P.12-20）

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。

	コマンド	目的
ステップ 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	インターフェイスをレイヤ 2 トランクとして設定します（インターフェイスがレイヤ 2 アクセス ポートである場合、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エートします。
ステップ 4	**switchport access vlan** *vlan-id*	（任意）インターフェイスがトランキングを停止した場合に使用するデフォルト VLAN を指定します。
ステップ 5	**switchport trunk native vlan** *vlan-id*	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
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。

（注）　VLAN 1 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 VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザ トラフィック（スパニング ツリー アドバタイズなど）は VLAN 1 で送受信されなくなります。

スパニング ツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol（CDP）、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。

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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	（任意）トランク上で許可される VLAN のリストを設定します。 **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。 *vlan-list* 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 *Trunking VLANs Enabled* 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。

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.13-14）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。
ステップ 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	トランクからのプルーニングを許可する VLAN のリストを設定します（「VTP プルーニング」（P.13-4）を参照）。 **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。

（注）　ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定についての詳細は、「IEEE 802.1Q の設定に関する考慮事項」（P.12-16）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。 *vlan-id* 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。
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 15 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 12-2 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ～ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ～ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。

- VLAN 3 ～ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ～ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ～ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ～ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。

図 12-2　STP ポート プライオリティによる負荷分散

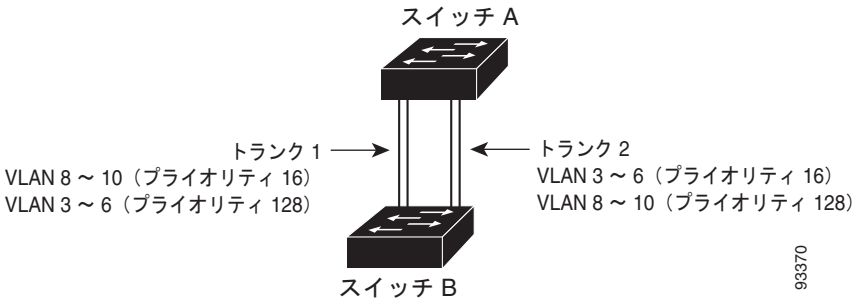


図 12-2 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	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 gigabitethernet 0/1**	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show interfaces gigabitethernet 0/1 switchport**	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。

	コマンド	目的
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 gigabitethernet 0/1**	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**spanning-tree vlan 8-10 port-priority 16**	VLAN 8 ～ 10 にポート プライオリティ 16 を割り当てます。
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 gigabitethernet0/2**	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 20	**spanning-tree vlan 3-6 port-priority 16**	VLAN 3 ～ 6 にポート プライオリティ 16 を割り当てます。
ステップ 21	**end**	特権 EXEC モードに戻ります。
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 12-3 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 12-3　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

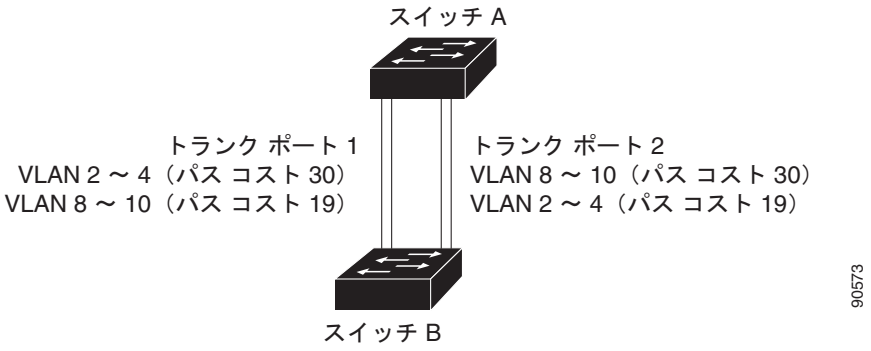


図 12-3 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	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 gigabitethernet0/1**	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5		スイッチ A 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 gigabitethernet0/1**	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 のスパニング ツリー パス コストを 30 に設定します。
ステップ 12	**end**	グローバル コンフィギュレーション モードに戻ります。
ステップ 13		スイッチ A に設定したもう一方のトランク インターフェイスで、ステップ 9 ～ 12 を繰り返し、VLAN 8、9、および 10 のスパニング ツリー パス コストを 30 に設定します。
ステップ 14	**exit**	特権 EXEC モードに戻ります。
ステップ 15	**show running-config**	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.12-25）
- 「VMPS クライアントのデフォルト設定」（P.12-26）
- 「VMPS 設定時の注意事項」（P.12-26）
- 「VMPS クライアントの設定」（P.12-27）

- 「VMPS のモニタ」（P.12-29）
- 「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.12-30）
- 「VMPS の設定例」（P.12-30）

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 12-6 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 12-6　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

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミックアクセス ポート VLAN メンバシップには、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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vmps server** *ipaddress* **primary**	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	**vmps server** *ipaddress*	（任意）セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vmps**	表示された *VMPS Domain Server* 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。

（注） 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。

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。

	コマンド	目的
ステップ 4	**show vmps**	表示された *Reconfirm Interval* 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。

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

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。

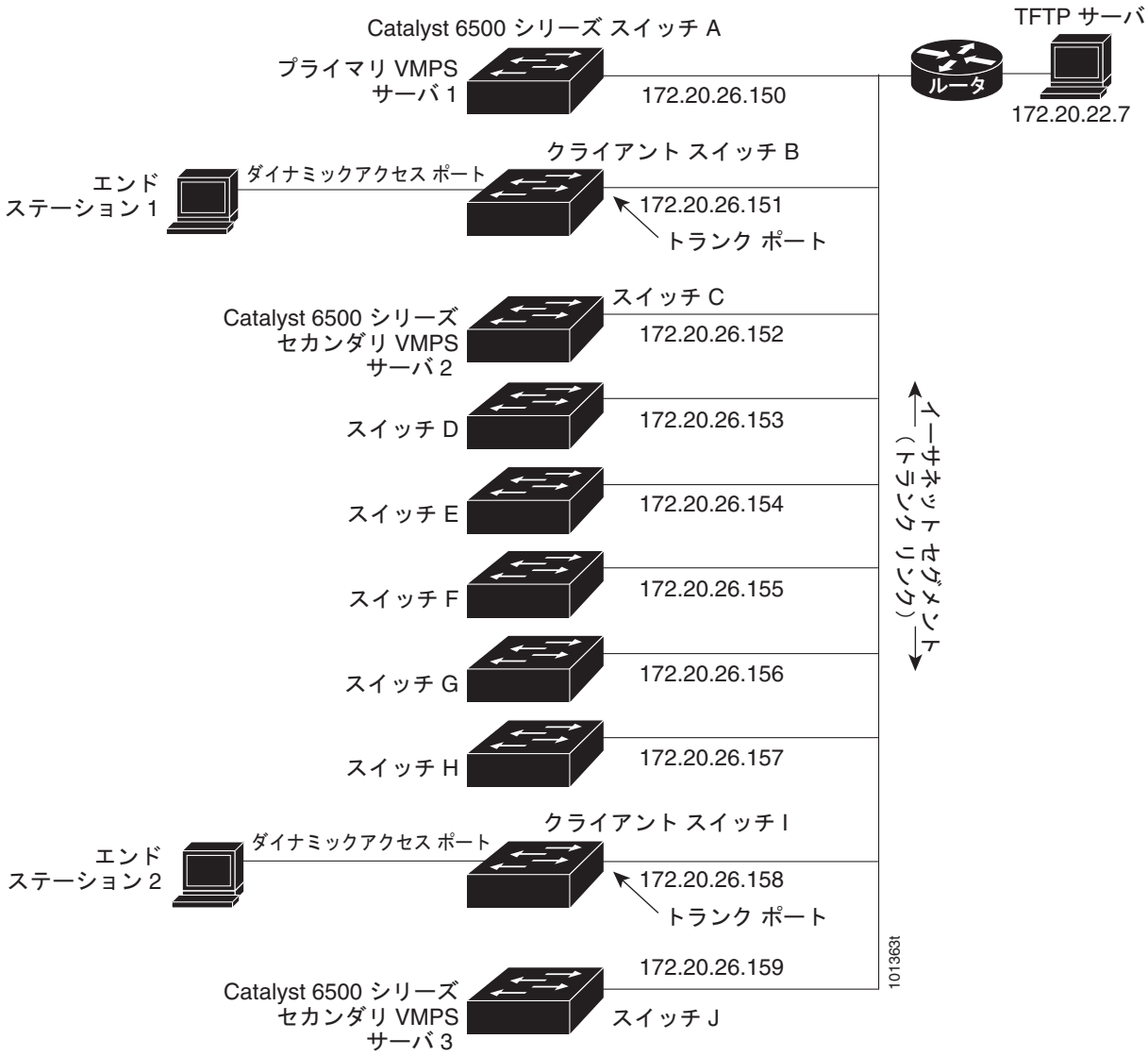
ディセーブルにされているダイナミックアクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の設定例

図 12-4 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 12-4　ダイナミック ポート VLAN メンバシップの構成例





CHAPTER 13

VTP の設定

この章では、Catalyst 2960 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。

（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。

- 「VTP の概要」（P.13-1）
- 「VTP の設定」（P.13-7）
- 「VTP のモニタ」（P.13-16）

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。

VTP は標準範囲 VLAN（VLAN ID 1 ～ 1005）だけを学習します。拡張範囲 VLAN（1005 を超える VLAN ID）は VTP ではサポートされず、VTP VLAN データベースにも格納されません。

ここでは、次の概要について説明します。

- 「VTP ドメイン」（P.13-2）
- 「VTP モード」（P.13-3）
- 「VTP アドバタイズ」（P.13-3）
- 「VTP バージョン 2」（P.13-4）
- 「VTP プルーニング」（P.13-4）

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。

注意　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.13-15）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.13-8）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 13-1 に示す VTP モードのいずれかに設定できます。

表 13-1　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 モードでは、VLAN 設定は NVRAM に保存されます。VTP サーバ モードがデフォルトの設定です。
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 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 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 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。 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。「拡張範囲 VLAN の設定」（P.12-11）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 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.12-14）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 2

ネットワークで VTP を使用する場合は、バージョン 1 または 2 のどちら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.12-4）を参照してください。
- 認識不能な Type-Length-Value（TLV）のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識されなかった TLV は、スイッチが VTP サーバ モードで動作している場合、NVRAM に保存されます。
- バージョン依存型トランスペアレント モード：VTP バージョン 1 の場合、VTP トランスペアレント スイッチが VTP メッセージ中のドメイン名およびバージョンを調べ、バージョンおよびドメイン名が一致する場合に限りメッセージを転送します。VTP バージョン 2 がサポートするドメインは 1 つだけなので、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。
- 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 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、VTP バージョン 1 およびバージョン 2 でサポートされています。

図 13-1 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 13-1　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

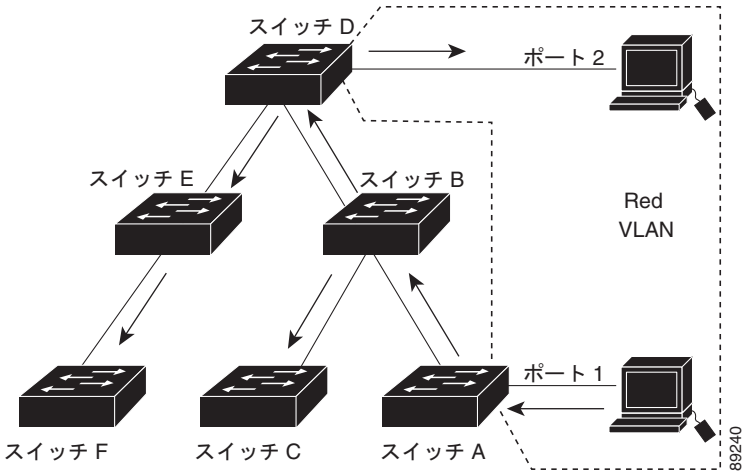
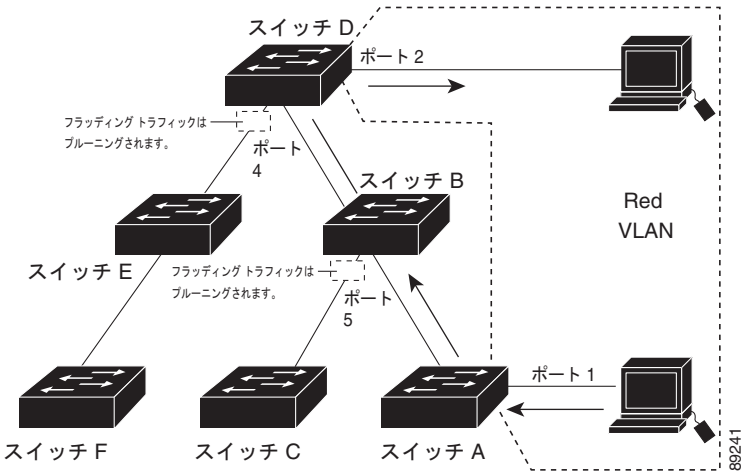


図 13-2 に、VTP プルーニングをイネーブルに設定したスイッチド ネットワークを示します。スイッチ A からのブロードキャスト トラフィックは、スイッチ C、E、F には転送されません。図に示されているリンク ポート（スイッチ B のポート 5、およびスイッチ D のポート 4）で、Red VLAN のトラフィックがプルーニングされるからです。

図 13-2　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.13-14）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.12-20）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.13-7）
- 「VTP 設定オプション」（P.13-7）
- 「VTP 設定時の注意事項」（P.13-8）
- 「VTP サーバの設定」（P.13-10）
- 「VTP クライアントの設定」（P.13-11）
- 「VTP のディセーブル化（VTP トランスペアレント モード）」（P.13-12）
- 「VTP バージョン 2 のイネーブル化」（P.13-13）
- 「VTP プルーニングのイネーブル化」（P.13-14）
- 「VTP ドメインへの VTP クライアント スイッチの追加」（P.13-15）

VTP のデフォルト設定

表 13-2 に、VTP のデフォルト設定を示します。

表 13-2　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	サーバ
VTP バージョン	バージョン 1（バージョン 2 はディセーブル）
VTP パスワード	なし
VTP プルーニング	ディセーブル

VTP 設定オプション

VTP を設定するには、次のコンフィギュレーション モードを使用します。

- 「グローバル コンフィギュレーション モードでの VTP 設定」（P.13-7）
- 「VLAN データベース コンフィギュレーション モードでの VTP 設定」（P.13-8）

VLAN データベース コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。

vtp 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。

グローバル コンフィギュレーション モードでの VTP 設定

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にも、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）、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 VTP 設定には VLAN データベース情報が使用されます。

VLAN データベース コンフィギュレーション モードでの VTP 設定

VLAN データベース コンフィギュレーション モード（開始するには **vlan database** 特権 EXEC コマンドを入力）で、すべての VTP パラメータを設定できます。使用できるキーワードの詳細については、このリリースのコマンド リファレンスに記載された **vtp** VLAN 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。VLAN データベース コンフィギュレーション モードで **exit** コマンドを入力すると、それまでに入力したすべてのコマンドに適用され、VLAN データベースが更新されます。VTP ドメイン内の他のスイッチに VTP メッセージが送信され、特権 EXEC モード プロンプトが表示されます。

VTP モードがトランスペアレントである場合、ドメイン名およびモード（トランスペアレント）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 コマンドを入力します。

VTP 設定時の注意事項

ここでは、ネットワークに VTP を実装するときに従う必要がある注意事項について説明します。

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で同じ VTP バージョンを実行する必要があります。
- VTP バージョン 2 対応のスイッチ上で VTP バージョン 2 をディセーブルに設定している場合、その VTP バージョン 2 対応スイッチは、同一 VTP ドメイン内で VTP バージョン 1 が稼動するスイッチとして動作できます（VTP バージョン 2 は、デフォルトでディセーブルに設定されています）。
- 同一 VTP ドメイン内のすべてのスイッチがバージョン 2 に対応する場合を除いて、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。
- 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 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。

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.12-14）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。

スイッチ上で拡張範囲 VLAN を設定している場合は、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 サーバの設定

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。

（注）　スイッチ上に拡張範囲 VLAN が設定されている場合は、VTP モードを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。

スイッチを VTP サーバ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	**vtp mode server**	スイッチを VTP サーバ モードに設定します（デフォルト）。
ステップ 3	**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。
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。
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。

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。

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、グローバル コンフィギュレーション モードを使用し、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 terminal
Switch(config)# vtp mode server
Switch(config)# vtp domain eng_group
Switch(config)# vtp password mypassword
Switch(config)# end
```

VLAN データベース コンフィギュレーション モードを使用して、VTP パラメータを設定することもできます。

VLAN データベース コンフィギュレーション モードを使用して、スイッチを VTP サーバに設定するには、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	**vlan database**	VLAN データベース コンフィギュレーション モードを開始します。
ステップ 2	**vtp server**	スイッチを VTP サーバ モードに設定します（デフォルト）。
ステップ 3	**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。
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。
ステップ 5	**exit**	VLAN データベースをアップデートし、アップデート情報を管理ドメイン全体に伝播して、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。

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。

スイッチをパスワードがない状態に戻すには、**no vtp password** VLAN データベース コンフィギュレーション コマンドを使用します。

次に、VLAN データベース コンフィギュレーション モードを使用し、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# vlan database
Switch(vlan)# vtp server
Switch(vlan)# vtp domain eng_group
Switch(vlan)# vtp password mypassword
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

VTP クライアントの設定

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。

次の注意事項に従ってください。

- スイッチ上に拡張範囲 VLAN が設定されている場合は、VTP モードをクライアント モードに変更できません。エラー メッセージが表示され、設定が許可されません。
- 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。

スイッチを VTP クライアン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	**vtp mode client**	スイッチを VTP クライアント モードに設定します。デフォルトの設定は VTP サーバ モードです。
ステップ 3	**vtp domain** *domain-name*	（任意）VTP 管理ドメイン名を入力します。1 ～ 32 文字の名前を使用できます。VTP サーバと同じドメイン名を指定する必要があります。 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。
ステップ 4	**vtp password** *password*	（任意）VTP ドメイン用のパスワードを入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show 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** 特権 EXEC コマンドを使用します。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。

（注）　**vlan database** 特権 EXEC コマンドを使用して VLAN データベース コンフィギュレーション モードを開始し、**vtp client** コマンドを入力して、VTP クライアントを設定することもできます。この手順は、「VTP サーバの設定」（P.13-10）の 2 番めの手順と同様です。**no vtp client** VLAN データベース コンフィギュレーション コマンドを使用して、スイッチを VTP サーバ モードに戻すか、または **no vtp password** VLAN データベース コンフィギュレーション コマンドを使用して、スイッチをパスワードがない状態に戻します。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。

VTP のディセーブル化（VTP トランスペアレント モード）

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。

（注）　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 トランスペアレント モードを設定して、VTP 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、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 モードに設定します（VTP 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 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 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。 **（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。

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。

（注） スイッチ上に拡張範囲 VLAN が設定されている場合は、VTP モードを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。

（注） **vlan database** 特権 EXEC コマンドを使用して VLAN データベース コンフィギュレーション モードを開始し、**vtp transparent** コマンドを入力して、VTP トランスペアレント モードを設定することもできます。この手順は、「VTP サーバの設定」（P.13-10）の 2 番めの手順と同様です。スイッチを VTP サーバ モードに戻すには、**no vtp transparent** VLAN データベース コンフィギュレーション コマンドを使用します。スイッチ上に拡張範囲 VLAN が設定されている場合は、VTP モードを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 2 のイネーブル化

VTP バージョン 2 対応スイッチでは、VTP バージョン 2 はディセーブルがデフォルトの設定です。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。スイッチにバージョンを設定できるのは、VTP サーバ モードまたはトランスペアレント モードの場合に限られます。

注意 同一 VTP ドメイン内のスイッチに関して、VTP バージョン 1 および VTP バージョン 2 間のインターオペラビリティはありません。VTP ドメイン内のすべてのスイッチで同じ VTP バージョンを使用する必要があります。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。

（注）　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 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 バージョンを設定する場合の注意事項については、「VTP バージョン」（P.13-9）を参照してください。

VTP バージョン 2 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 version 2**	スイッチ上で VTP バージョン 2 をイネーブルにします。 VTP バージョン 2 対応スイッチでは、VTP バージョン 2 はディセーブルがデフォルトの設定です。
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**	表示された *VTP V2 Mode* フィールドで、VTP バージョン 2 がイネーブルであることを確認します。

VTP バージョン 2 をディセーブルにするには、**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。

（注）　**vlan database** 特権 EXEC コマンドを使用して VLAN データベース コンフィギュレーション モードを開始し、**vtp v2-mode** VLAN データベース コンフィギュレーション コマンドを入力して、VTP バージョン 2 をイネーブルにすることもできます。VTP バージョン 2 をディセーブルにするには、**no vtp v2-mode** VLAN データベース コンフィギュレーション コマンドを使用します。

VTP プルーニングのイネーブル化

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。

（注）　**vlan database** 特権 EXEC コマンドを使用して VLAN データベース コンフィギュレーション モードを開始し、**vtp pruning** VLAN データベース コンフィギュレーション コマンドを入力して、VTP プルーニングをイネーブルにすることもできます。VTP プルーニングをディセーブルにするには、**no vtp pruning** VLAN データベース コンフィギュレーション コマンドを使用します。**vtp pruning** 特権 EXEC コマンドを使用して、VTP バージョン 2 をイネーブルにすることもできます。

プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。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。

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.12-20）を参照してください。

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 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 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。

	コマンド	目的
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。

vlan database 特権 EXEC コマンドを入力して VLAN データベース コンフィギュレーション モードを開始し、**vtp domain** *domain-name* コマンドを入力して、VTP ドメイン名を変更することもできます。このモードで VLAN 情報を更新し、特権 EXEC モードに戻るには、**exit** コマンドを入力する必要があります。

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。

（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 コマンドまたは **vtp transparent** VLAN データベース 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 13-3 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。

表 13-3　VTP モニタ コマンド

コマンド	目的
show vtp status	VTP スイッチの設定情報を表示します。
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。



CHAPTER 14

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.14-1）
- 「音声 VLAN の設定」（P.14-3）
- 「音声 VLAN の表示」（P.14-7）

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 31 章「QoS の設定」を参照してください。

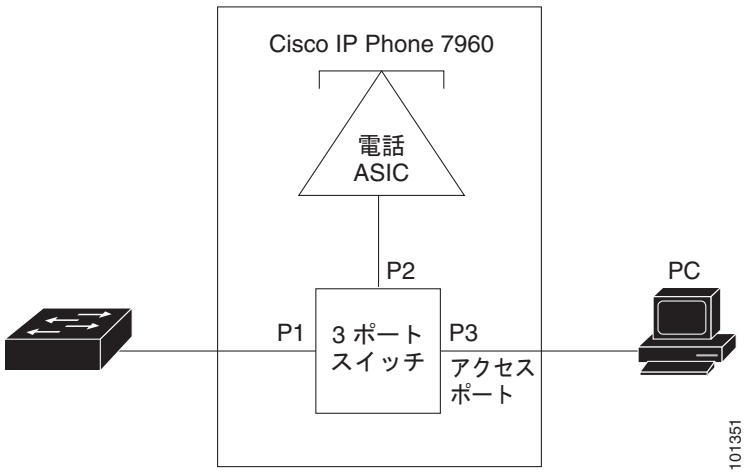
Cisco7960 IP Phone は設定可能なデバイスであり、IEEE 802.1p プライオリティに基づいてトラフィックを転送するように設定できます。Cisco IP Phone によって割り当てられたトラフィック プライオリティを信頼するように、または上書きするようにスイッチを設定できます。

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 14-1 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 14-1 に、Cisco7960 IP Phone の接続方法の例を示します。

図 14-1　スイッチに接続された Cisco7960 IP Phone



Cisco IP Phone の音声トラフィック

Cisco IP Phone と接続するアクセス ポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータ トラフィック用に使用するように設定できます。スイッチ上のアクセス ポートを設定して、Cisco Discovery Protocol（CDP）パケットを送信させることができます。CDP には、接続する IP Phone に対して、次のいずれかの方法でスイッチに音声トラフィックを送信するように指定します。

- レイヤ 2 CoS プライオリティ値のタグ付き音声 VLAN による送信
- レイヤ 2 CoS プライオリティ値のタグ付きアクセス VLAN による送信
- タグなし（レイヤ 2 CoS プライオリティ値なし）のアクセス VLAN による送信

（注） いずれの設定でも、音声トラフィックはレイヤ 3 IP precedence 値（音声トラフィックはデフォルトで 5、音声制御トラフィックは 3）を伝送します。

Cisco IP Phone 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 14-1 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.14-3）
- 「音声 VLAN 設定時の注意事項」（P.14-3）
- 「Cisco7960 IP Phone に接続するポートの設定」（P.14-4）

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 はスイッチのアクセス ポートに設定する必要があります。音声 VLAN はトランク ポートではサポートされません。

  （注）　音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 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 12 章「VLAN の設定」を参照してください。
- 音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチ上で QoS をイネーブルに設定し、さらに **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力してポートの信頼状態を trust に設定しておくことを推奨します。Auto-QoS 機能を使用すると、これらは自動的に設定されます。詳細は、第 31 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.12-27）を参照してください。
  - IEEE 802.1x 認証ポート。詳細については、「IEEE 802.1x 認証の設定」（P.9-22）を参照してください。

    （注）　音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにした場合、その IP Phone のスイッチへの接続が最大 30 秒間失われます。

  - 保護ポート。詳細については、「保護ポートの設定」（P.21-5）を参照してください。
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または Remote SPAN（RSPAN）セッションの送信元ポートまたは宛先ポート。
  - セキュア ポート。詳細については、「ポート セキュリティの設定」（P.21-8）を参照してください。

    （注）　音声 VLAN も設定しているインターフェイス上でポート セキュリティをイネーブルにする場合、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定しなければなりません。ポートを Cisco IP Phone に接続している場合、IP Phone に最大で 2 つの MAC アドレスが必要になります。IP Phone のアドレスは、音声 VLAN で学習され、アクセス VLAN でも学習される場合があります。PC を IP Phone に接続する場合、追加の MAC アドレスが必要になります。

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.14-5）
- 「着信データ フレームのプライオリティ設定」（P.14-6）

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* | **dot1p** | **none** | **untagged**}}	Cisco IP Phone による音声トラフィックの伝送方法を設定します。 • *vlan-id*：すべての音声トラフィックが特定の VLAN を経由して転送されるように IP Phone を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p 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 **show running-config interface** *interface-id*	音声 VLAN の設定を確認します。 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
```

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。

着信データ フレームのプライオリティ設定

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	**switchport priority extend** {**cos** *value* | **trust**}	Cisco IP Phone のアクセス ポートから受信したデータ トラフィックのプライオリティを設定します。 • **cos** *value*：PC または接続しているデバイスから受信したプライオリティを指定の CoS 値に変更するように、IP Phone を設定します。値は 0 ～ 7 です。7 が最高のプライオリティです。デフォルトのプライオリティは **cos** 0 です。 • **trust**：PC または接続しているデバイスから受信したプライオリティを信頼するように IP Phone のアクセス ポートを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
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。

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。



CHAPTER 15

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 16 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 17 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。

- 「スパニング ツリー機能の概要」（P.15-1）
- 「スパニング ツリー機能の設定」（P.15-11）
- 「スパニング ツリー ステータスの表示」（P.15-23）

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.15-2）
- 「スパニング ツリー トポロジと BPDU」（P.15-3）
- 「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.15-4）
- 「スパニング ツリー インターフェイス ステート」（P.15-4）
- 「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.15-7）
- 「スパニング ツリーおよび冗長接続」（P.15-8）
- 「スパニング ツリー アドレスの管理」（P.15-8）
- 「接続を維持するためのエージング タイムの短縮」（P.15-9）
- 「スパニング ツリー モードおよびプロトコル」（P.15-9）
- 「サポートされるスパニング ツリー インスタンス」（P.15-10）

- 「スパニング ツリーの相互運用性と下位互換性」（P.15-10）
- 「STP および IEEE 802.1Q トランク」（P.15-10）

設定情報については、「スパニング ツリー機能の設定」（P.15-11）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 17 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。

（注）　デフォルトでは、Small Form-Factor Pluggable（SFP）を搭載していないインターフェイスにのみ、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 15-1（P.15-4）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 15-1 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 15-1　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.15-15）、「セカンダリ ルート スイッチの設定」（P.15-16）、および「VLAN のスイッチ プライオリティの設定」（P.15-20）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。

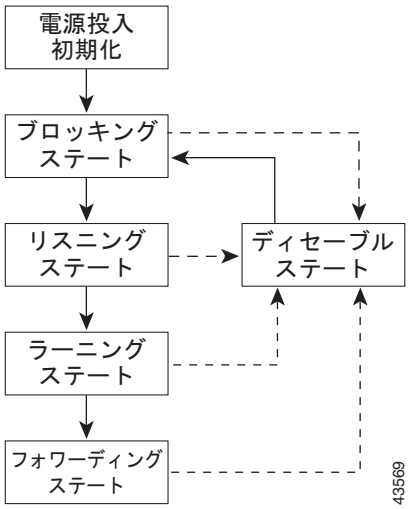
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：インターフェイスをフレーム転送に関与させることをスパニング ツリーが決定した場合、ブロッキング ステートから最初に移行するステートです。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニング ツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニング ツリー インスタンスが稼動していないためです。

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 15-1 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 15-1　スパニング ツリー インターフェイス ステート



デフォルト設定では、スイッチを起動するとスパニング ツリーがイネーブルになります。その後、スイッチの各インターフェイス、VLAN、ネットワークがブロッキング ステートからリスニングおよびラーニングという移行ステートを通過します。スパニング ツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニング ツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. スパニング ツリーがインターフェイスをブロッキング ステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニング ステートになります。

2. スパニング ツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートで、スイッチがデータベース転送のためにエンド ステーションの位置情報を学習している間、インターフェイスはフレーム転送を引き続きブロックします。
4. 転送遅延タイマーが満了すると、スパニング ツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスはフレームの転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは最初、他のスイッチと BPDU を交換するまで、ルートとして動作します。この BPDU 交換によって、ネットワーク上のどのスイッチがルート、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、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。

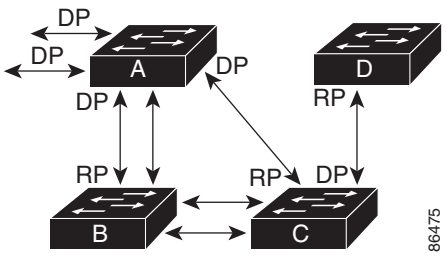
ディセーブル インターフェイスは、次の機能を実行します。

- 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 15-2 では、スイッチ A がルート スイッチとして選定されます（すべてのスイッチのスイッチ プライオリティがデフォルト（32768）に設定されており、スイッチ A の MAC アドレスが最小であるため）。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチとは限りません。ルート スイッチになるように、最適なスイッチのプライオリティを引き上げる（数値を引き下げる）と、スパニング ツリーの再計算が強制的に行われ、最適なスイッチをルートとした新しいトポロジが形成されます。

図 15-2　スパニング ツリー トポロジ



RP = ルート ポート
DP = 指定ポート

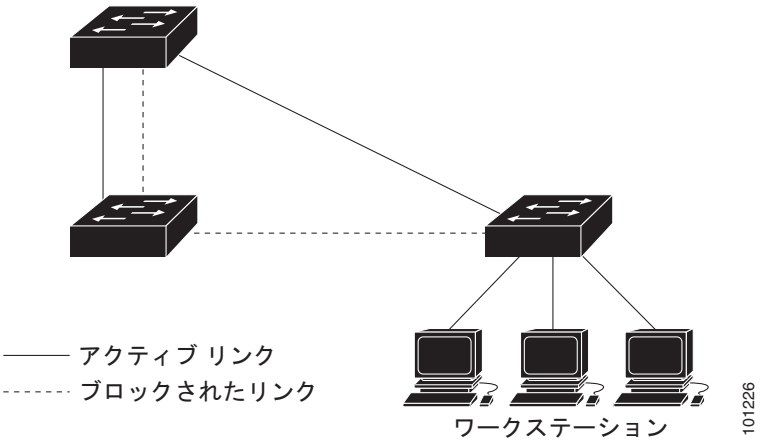
スパニング ツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない場合があります。たとえば、ルート ポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルート ポートが変更される可能性があります。最高速のリンクをルート ポートにすることが理想です。

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 15-3 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 15-3　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 34 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 を同一のスパニング ツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要となるスパニング ツリー インスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree

Protocol（RSTP）（IEEE 802.1w 準拠）上で実行され、転送遅延を解消し、ルート ポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパニング ツリーの高速コンバージェンスを可能にします。RSTP を使用せずに 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 16 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.15-12）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 15-2 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 15-2　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 12 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.15-11）
- 「スパニング ツリー設定時の注意事項」（P.15-12）
- 「スパニング ツリー モードの変更」（P.15-13）（必須）
- 「スパニング ツリーのディセーブル化」（P.15-14）（任意）
- 「ルート スイッチの設定」（P.15-15）（任意）
- 「セカンダリ ルート スイッチの設定」（P.15-16）（任意）
- 「ポート プライオリティの設定」（P.15-17）（任意）
- 「パス コストの設定」（P.15-18）（任意）
- 「VLAN のスイッチ プライオリティの設定」（P.15-20）（任意）
- 「スパニング ツリー タイマーの設定」（P.15-20）（任意）

スパニング ツリー機能のデフォルト設定

表 15-3 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 15-3　スパニング ツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル 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.15-10）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

表 15-3　スパニング ツリー機能のデフォルト設定 （続き）

機能	デフォルト設定
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 16 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。

注意　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。

（注）　スイッチ上の使用可能なスパニング ツリー インスタンスをすべて使い切ってしまったあとに、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.15-10）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.17-10）を参照してください。

注意　ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

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	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	スパニング ツリー モードを設定します。 • **pvst** 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 16 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。

	コマンド	目的
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** および **show spanning-tree interface** *interface-id*	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.15-10）のスパニング ツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニング ツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。

注意　スパニング ツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

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*	*vlan-id* 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 15-1（P.15-4）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）。

（注）　ルート スイッチとして設定する必要のある値が 1 未満の場合、**spanning-tree vlan** *vlan-id* **root** グローバル コンフィギュレーション コマンドは失敗します。

（注）　ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼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	**spanning-tree vlan** *vlan-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	指定された VLAN のルートになるように、スイッチを設定します。 • *vlan-id* 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。 • *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。 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.15-15）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** *port-channel-number*）です。

	コマンド	目的
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。 *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 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* または **show spanning-tree vlan** *vlan-id*	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。

（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、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.12-21）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** *port-channel-number*）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。 *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 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。
ステップ 6	**show spanning-tree interface** *interface-id* または **show spanning-tree vlan** *vlan-id*	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。

（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.12-21）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。
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 15-4 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 15-4　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。

表 15-4　スパニング ツリー タイマー （続き）

変数	説明
最大エージング タイマー	インターフェイスが受信したプロトコル情報をスイッチに保存させておく時間を制御します。
転送保留カウント	1 秒間停止する前に送信できる BPDU 数を制御します。

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。
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。 • *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 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 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* **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
ステップ 1	**configure terminal**	グローバル コ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 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。 *value* に指定できる範囲は 1 ～ 20 です。デフォルト値は 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 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 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 15-5 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 15-5　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。



CHAPTER 16

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） Cisco IOS Release 12.2(25)SED への Multiple Spanning Tree（MST）の実装は、IEEE 802.1s 標準に準拠しています。それ以前の Cisco IOS リリースに関しては、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 15 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 17 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.16-2）
- 「RSTP の概要」（P.16-9）
- 「MSTP 機能の設定」（P.16-15）
- 「MST コンフィギュレーションおよびステータスの表示」（P.16-27）

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.16-2）
- 「IST、CIST、および CST」（P.16-3）
- 「ホップ カウント」（P.16-6）
- 「境界ポート」（P.16-6）
- 「IEEE 802.1s の実装」（P.16-7）
- 「IEEE 802.1D STP との相互運用性」（P.16-9）

設定情報については、「MSTP 機能の設定」（P.16-15）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 16-1（P.16-5）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.16-3）および「MST リージョン間の動作」（P.16-4）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 15-1（P.15-4）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 16-1（P.16-5）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。

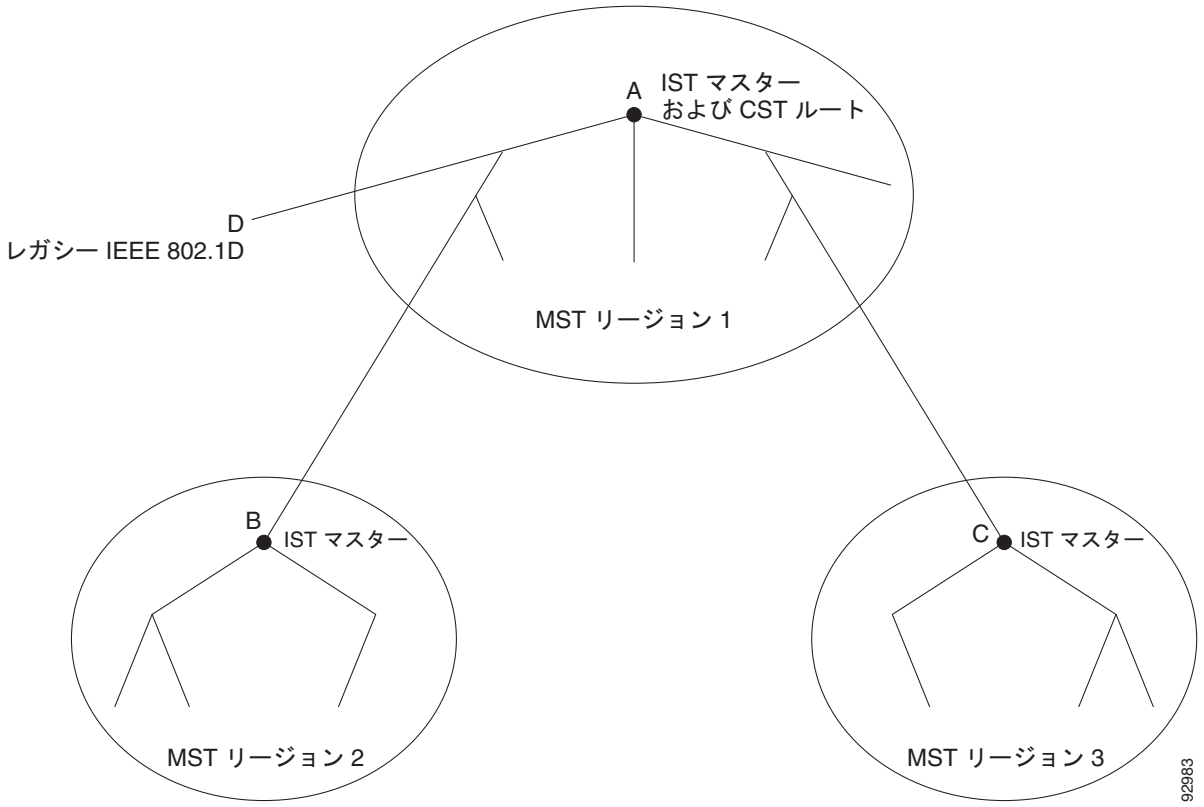
MST リージョン間の動作

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 16-1 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。

図 16-1　MST リージョン、CIST マスター、および CST ルート



BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニング ツリー情報を BPDU に追加して、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 インスタンスでのみ設定されますが、その影響はすべての MST インスタンスに及びます。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 16-1（P.16-6）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 16-1　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、常にコスト値が 0、ホップ カウント値が最大値に設定された BPDU（つまり 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（同一リージョンからの）および外部の 2 種類のメッセージを識別します。メッセージが外部のものであれば、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。

（注）　レガシー STP スイッチがセグメントに存在する場合、メッセージは常に外部と見なされます。

先行標準の実装から他に変更された点は、送信スイッチ ID を持つ RSTP またはレガシー IEEE 802.1Q スイッチの部分に、CIST リージョナル ルート スイッチ ID フィールドが加えられたことです。一貫した送信スイッチ ID を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。

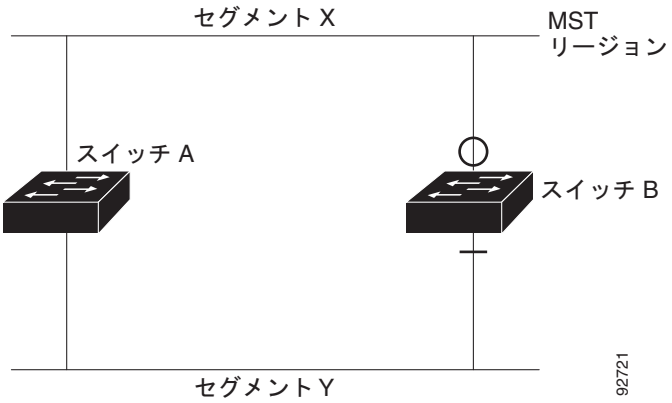
- 境界ポートが CIST リージョナル ルートのルート ポートである場合 : CIST インスタンス ポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わったあとであれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディング ステートに移行できます。現在 MSTI ポートは、マスターという特別な役割を担っています。
- 境界ポートが CIST リージョナル ルートのルート ポートでない場合 : MSTI ポートは、CIST ポートのステートと役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU（M レコード）を受信しない場合、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 16-2 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 16-2　　標準スイッチおよび先行標準のスイッチでの相互運用



（注）　標準と先行標準の MST 実装の間での干渉を少なくすることを推奨します。

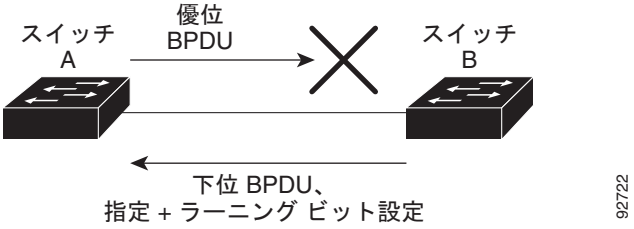
単一方向リンクの失敗の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアを使用することで、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 16-3 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。

図 16-3　　単一方向リンクの失敗の検出



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.16-9）
- 「高速コンバージェンス」（P.16-10）
- 「ポートの役割の同期化」（P.16-12）
- 「BPDU のフォーマットおよびプロセス」（P.16-13）

設定については、「MSTP 機能の設定」（P.16-15）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.15-3）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 16-2 に、IEEE 802.1D と RSTP のポート ステートの比較を示します。

表 16-2　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 16-4 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。

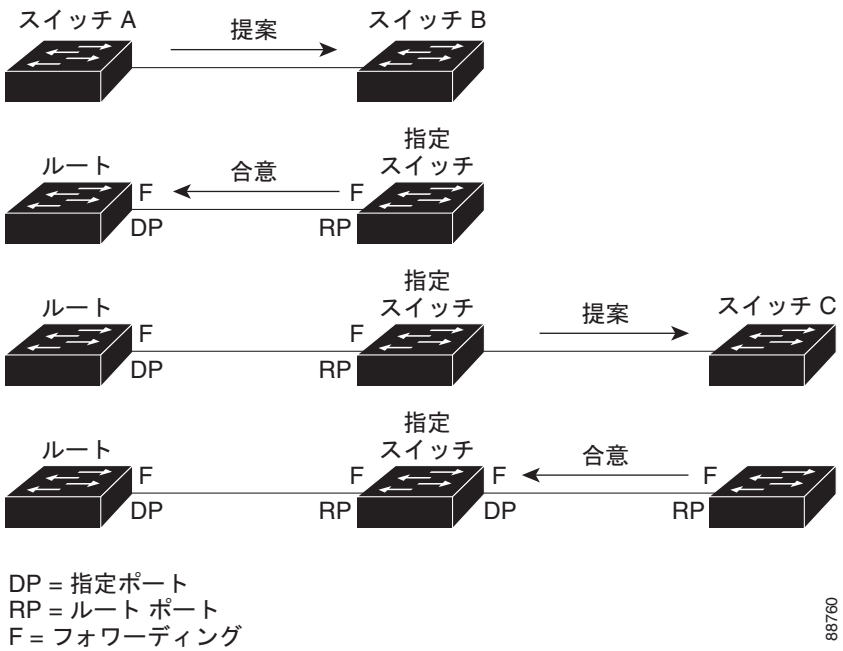
  スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルート ポートとして選択し、すべての非エッジ ポートをブロッキング ステートにします。さらに、新しいルート ポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

  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 16-4　高速コンバージェンスの提案/合意ハンドシェイク



DP = 指定ポート
RP = ルート ポート
F = フォワーディング

ポートの役割の同期化

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。

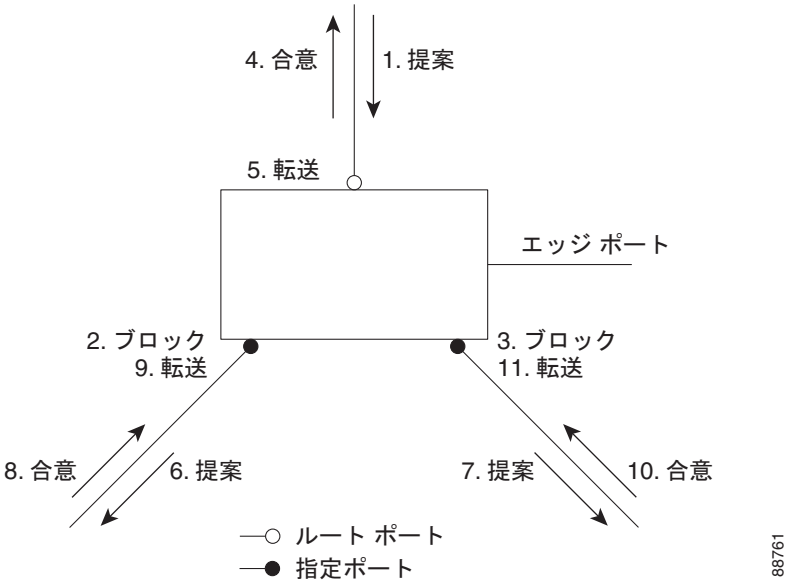
他のすべてのポートが同期化されると、スイッチはルート ポートで受信した優位のルート情報に同期化されます。スイッチ上の個々のポートは次の場合に同期化された状態となります。

- 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 16-5 は、この一連のイベントを示します。

図 16-5　高速コンバ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 16-3 に、RSTP のフラグ フィールドを示します。

表 16-3　RSTP BPDU フラグ

ビット	機能
0	トポロジの変更（TC）
1	提案
2 ～ 3：	ポートの役割：
00	不明
01	代替ポート
10	ルート ポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	トポロジの変更の確認（TCA）

送信スイッチは、自身を LAN 上の指定スイッチにするために、RSTP BPDU に提案フラグを設定します。提案メッセージでは、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.16-15）
- 「MSTP 設定時の注意事項」（P.16-16）
- 「MST リージョンの設定および MSTP のイネーブル化」（P.16-16）（必須）
- 「ルート スイッチの設定」（P.16-18）（任意）
- 「セカンダリ ルート スイッチの設定」（P.16-19）（任意）
- 「ポート プライオリティの設定」（P.16-20）（任意）
- 「パス コストの設定」（P.16-21）（任意）
- 「スイッチ プライオリティの設定」（P.16-22）（任意）
- 「Hello タイムの設定」（P.16-23）（任意）
- 「転送遅延時間の設定」（P.16-24）（任意）
- 「最大エージング タイムの設定」（P.16-24）（任意）
- 「最大ホップ カウントの設定」（P.16-25）（任意）
- 「リンク タイプの指定による高速移行の保証」（P.16-25）（任意）
- 「ネイバ タイプの指定」（P.16-26）（任意）
- 「プロトコル移行プロセスの再起動」（P.16-26）（任意）

MSTP のデフォルト設定

表 16-4 に、MSTP のデフォルト設定を示します。

表 16-4　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.15-10）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.15-10）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.12-17）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.17-10）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。 MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 9	**end**	特権 EXEC モードに戻ります。
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、PVST+ をイネーブルに戻すには、**no spanning-tree mode** または **spanning-tree mode pvst** グローバル 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
1         10-20
-------------------------------

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 15-1（P.15-4）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** *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	スイッチをルート スイッチに設定します。 • *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。 • （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。
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。 • *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。 • （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.16-18）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。

	コマンド	目的
ステップ 3	**spanning-tree mst** *instance-id* **port-priority** *priority*	ポート プライオリティを設定します。 • *instance-id* 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* または **show spanning-tree mst** *instance-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。

（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。

	コマンド	目的
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 ～ 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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show spanning-tree mst interface** *interface-id* または **show spanning-tree mst** *instance-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。

（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。 *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 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。 *hop-count* 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**	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-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.16-10）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
ステップ 1	**configure terminal**	グローバル コ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、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 ～ 4094 です。ポートチャネルの範囲は 1 ～ 6 です。
ステップ 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。
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 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 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　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。



CHAPTER 17

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 15 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 16 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.17-1）
- 「オプションのスパニング ツリー機能の設定」（P.17-9）
- 「スパニング ツリー ステータスの表示」（P.17-17）

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.17-2）
- 「BPDU ガードの概要」（P.17-2）
- 「BPDU フィルタリングの概要」（P.17-3）
- 「UplinkFast の概要」（P.17-3）
- 「BackboneFast の概要」（P.17-5）
- 「EtherChannel ガードの概要」（P.17-7）
- 「ルート ガードの概要」（P.17-8）
- 「ループ ガードの概要」（P.17-9）

PortFast の概要

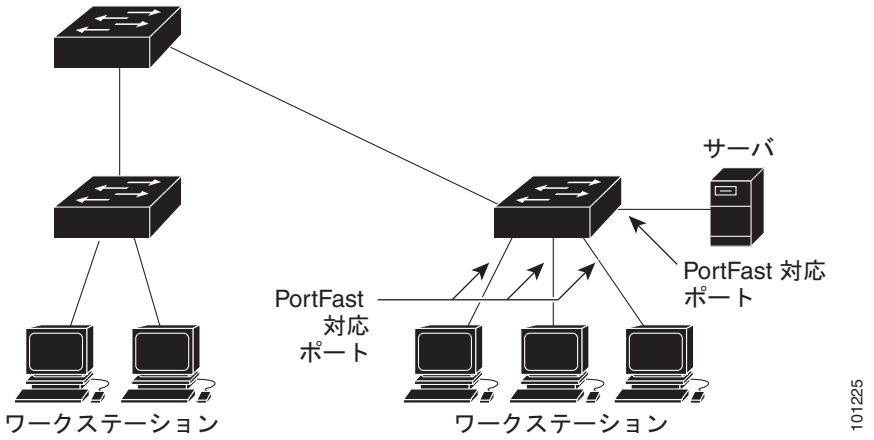
PortFast 機能を使用すると、アクセス ポートまたはトランク ポートとして設定されているインターフェイスが、リスニング ステートおよびラーニング ステートを経由せずに、ブロッキング ステートから直接フォワーディング ステートに移行します。単一のワークステーションまたはサーバに接続されたインターフェイス上で PortFast を使用すると、スパニング ツリーが収束するのを待たずにデバイスをただちにネットワークに接続できます（図 17-1 を参照）。

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。

（注）　PortFast の目的は、インターフェイスがスパニング ツリーのコンバージェンスを待機する時間を最小限に抑えることです。したがって、PortFast はエンド ステーションに接続されたインターフェイス上で使用する場合にのみ有効になります。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 17-1　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。

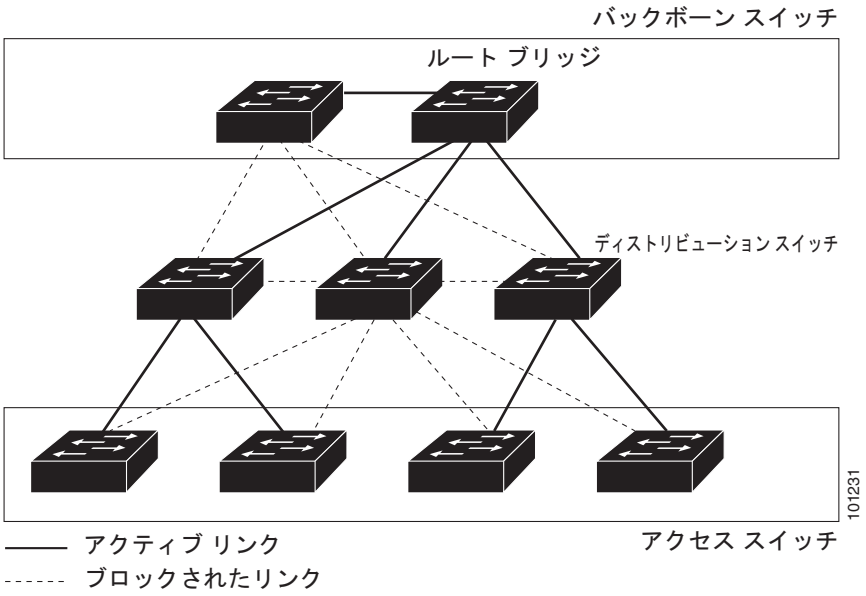
注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニング ツリーをディセーブルにすることと同じであり、スパニング ツリー ループが発生することがあります。

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 17-2 に、ディストリビューション スイッチおよびアクセス スイッチに少なくとも 1 つの冗長リンクが確保されている複雑なネットワークの例を示します。冗長リンクは、ループを防止するために、スパニング ツリーによってブロックされています。

図 17-2　階層型ネットワークのスイッチ



スイッチの接続が切断されると、スイッチはスパニング ツリーが新しいルート ポートを選択すると同時に代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニング ツリーが再設定された場合は、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用して UplinkFast をイネーブルにすることにより、新しいルート ポートを短時間で選択できます。ルート ポートは、通常のスパニング ツリー手順とは異なり、リスニング ステートおよびラーニング ステートを経由せず、ただちにフォワーディング ステートに移行します。

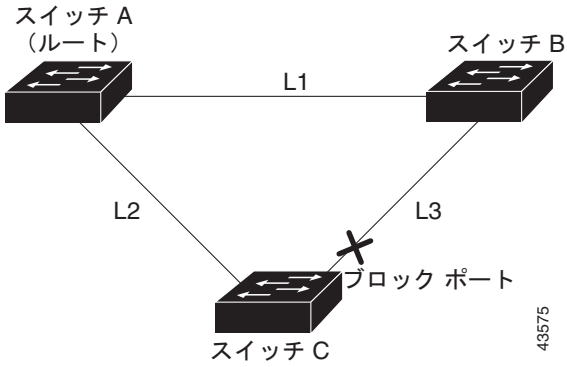
スパニング ツリーが新規ルート ポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト パケットをフラッディングし、インターフェイス上で学習した各アドレスにパケットを送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャスト トラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒 150 パケットです）。ただし、0 を入力すると、ステーション学習フレームが生成されないので、接続切断後スパニング ツリー トポロジがコンバージェンスする速度が遅くなります。

（注）　UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリング クローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ 2 リンク間でロードバランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ 2 インターフェイスの集合であり、いかなるときも、その中の 1 つのインターフェイスだけが転送を行います。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。

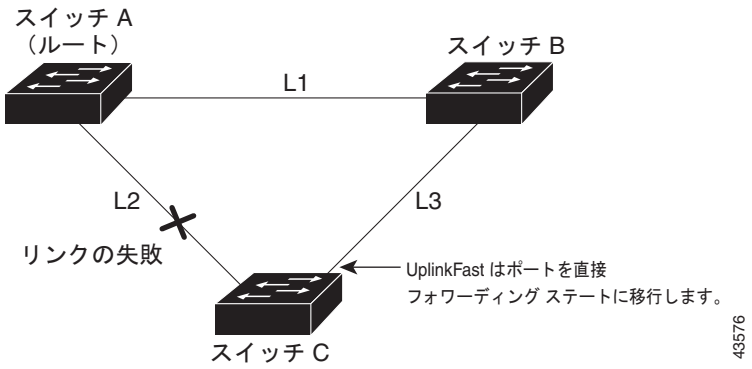
図 17-3 に、リンク障害が発生していないトポロジの例を示します。ルート スイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキング ステートです。

図 17-3　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 17-4 を参照）。この切り替えに必要な時間は、約 1 ～ 5 秒です。

図 17-4　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 17-5 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 17-5　　間接リンク障害発生前の BackboneFast の例

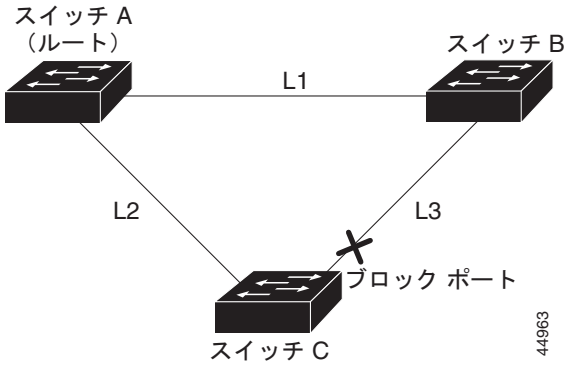


図 17-6 のリンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、その障害を検出できません。一方スイッチ B は、L1 によってルート スイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、BackboneFast は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング 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 17-6 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 17-6　間接リンク障害発生後の BackboneFast の例

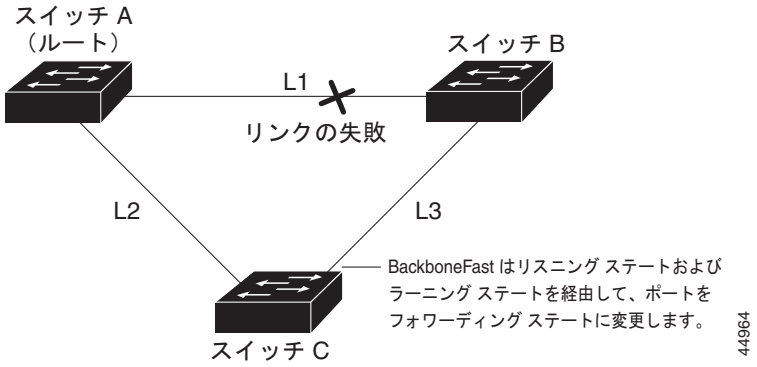
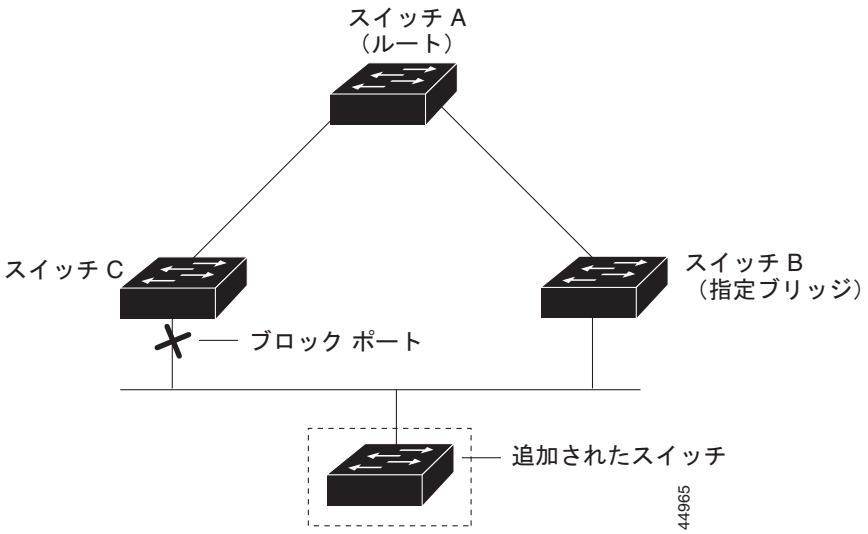


図 17-7 のように、新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルート スイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルート スイッチであるスイッチ A への指定スイッチであることを学習します。

図 17-7　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.34-9）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 17-8 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。

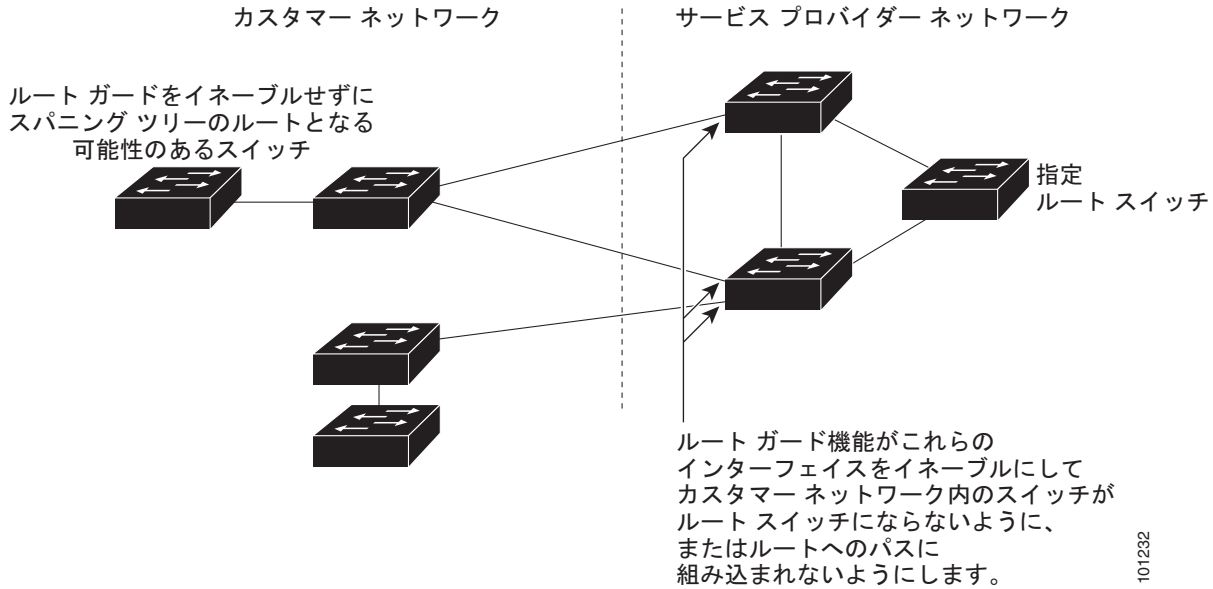
スイッチが MST モードで動作している場合、ルート ガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがルート ガードによって Internal Spanning-Tree（IST）インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

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。

注意　ルート ガード機能は使い方を誤ると、接続が切断されることがあります。

図 17-8　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 ネットワーク全体に設定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.17-10）
- 「オプションのスパニング ツリー設定時の注意事項」（P.17-10）
- 「PortFast のイネーブル化」（P.17-10）（任意）
- 「BPDU ガードのイネーブル化」（P.17-11）（任意）
- 「BPDU フィルタリングのイネーブル化」（P.17-12）（任意）
- 「冗長リンク用 UplinkFast のイネーブル化」（P.17-14）（任意）

- 「BackboneFast のイネーブル化」（P.17-14）（任意）
- 「EtherChannel ガードのイネーブル化」（P.17-15）（任意）
- 「ルート ガードのイネーブル化」（P.17-16）（任意）
- 「ループ ガードのイネーブル化」（P.17-16）（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 17-1 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 17-1　オプションのスパニング ツリー機能のデフォルト設定

機能	デフォルト設定
PortFast、BPDU フィルタリング、BPDU ガード	グローバルにディセーブル（インターフェイス単位で個別に設定する場合を除く）
UplinkFast	グローバルにディセーブル
BackboneFast	グローバルにディセーブル
EtherChannel ガード	グローバルにイネーブル
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 14 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
ステップ 1	**configure terminal**	グローバル コ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 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 BPDU を受信する PortFast 対応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。

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。

注意　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。

注意　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。

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** *pkts-per-second*]	UplinkFast をイネーブルにします。 （任意）*pkts-per-second* 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 misconfig**	EtherChannel ガード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。

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。

（注） 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** または **show spanning-tree mst**	どのインターフェイスが代替ポートまたはルート ポートであるかを確認します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spanning-tree loopguard default**	ループ ガードをイネーブルにします。 ループ ガードは、デフォルトではディセーブルに設定されています。
ステップ 4	**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 17-2 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 17-2　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。



CHAPTER 18

Flex Link および MAC アドレス テーブル移動更新機能の設定

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.18-1）
- 「Flex Link および MAC アドレス テーブル移動更新機能の設定」（P.18-4）
- 「Flex Link および MAC アドレス テーブル移動更新のモニタ」（P.18-11）

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.18-1）
- 「VLAN Flex Link ロード バランシングおよびサポート」（P.18-2）
- 「MAC アドレス テーブル移動更新」（P.18-3）

Flex Link

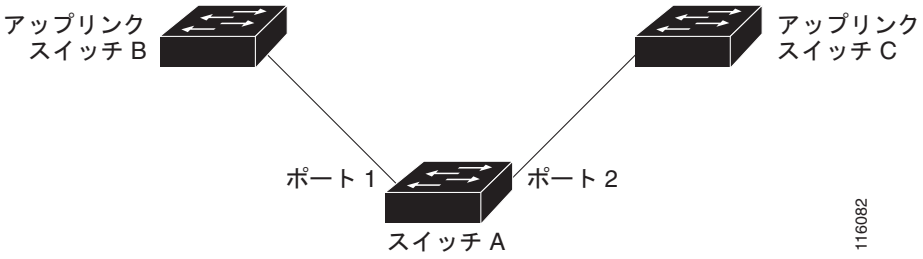
Flex Link は、レイヤ 2 インターフェイス（スイッチ ポートまたはポート チャネル）のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、Spanning Tree Protocol（STP; スパニングツリー プロトコル）の代替ソリューションを提供します。ユーザは、STP をディセーブルにしても、基本的リンク冗長性を保つことができます。Flex Link は、通常、お客様がスイッチで STP を実行しない場合のサービス プロバイダーまたは企業ネットワークに設定されます。スイッチが STP を実行中の場合は、STP がすでにリンク 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 18-1 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、トラフィックは転送されません。ポート 1 がダウンした場合はポート 2 がアップし、トラフィックをスイッチ C に転送し始めます。ポート 1 は、再び動作を開始するとスタンバイ モードになり、トラフィックを転送しません。ポート 2 がトラフィック転送を続けます。

また、優先してトラフィックの転送に使用するポートを指定して、プリエンプト メカニズムを設定することもできます。たとえば、図 18-1 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。

図 18-1　　Flex Link の設定例



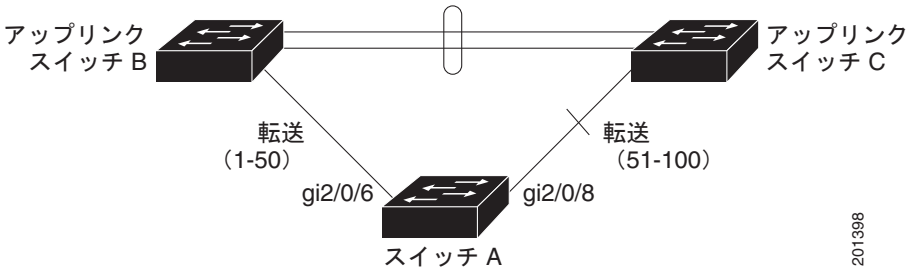
プライマリ（転送）リンクがダウンした場合、トラップがネットワーク管理ステーションに通知します。スタンバイ リンクがダウンした場合、トラップがユーザに通知します。

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。

図 18-2　VLAN Flex Link ロード バランシングの設定例



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 18-3 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。

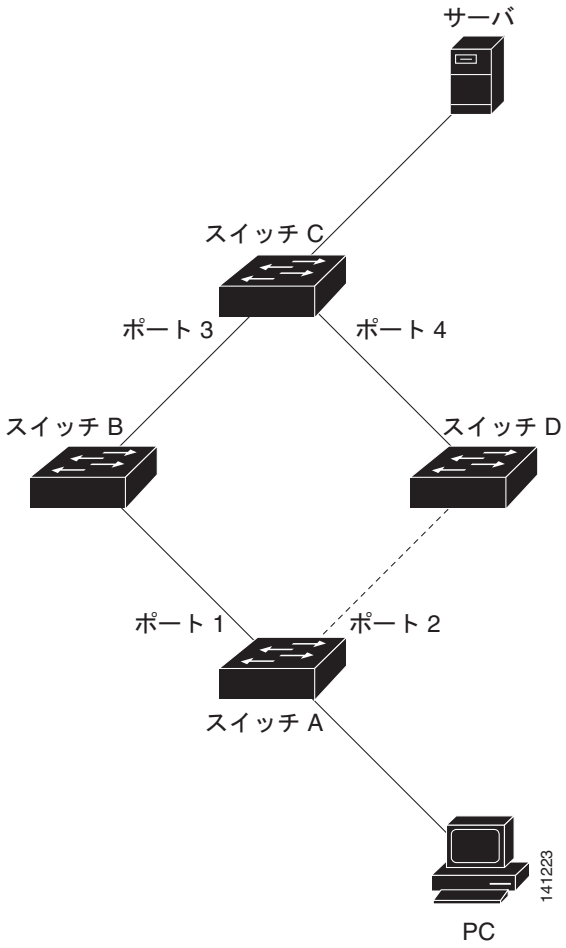
MAC アドレス テーブル移動更新機能が設定されておらず、ポート 1 がダウンした場合は、ポート 2 がトラフィックの転送を開始します。しかし、少しの間、スイッチ C がポート 3 経由でサーバから PC にトラフィックを転送し続けるため、ポート 1 がダウンしていることにより、PC へのトラフィックが途切れます。スイッチ C がポート 3 で PC の MAC アドレスを削除し、ポート 4 で再度学習した場合は、トラフィックはポート 2 経由でサーバから PC へ転送される可能性があります。

図 18-3 で MAC アドレス テーブル移動更新機能が設定され、各スイッチでイネーブルになっていて、ポート 1 がダウンした場合は、ポート 2 が PC からサーバへのトラフィックの転送を開始します。スイッチは、ポート 2 から MAC アドレス テーブル移動更新パケットを送出します。スイッチ C はこのパケットをポート 4 で受信し、ただちに PC の MAC アドレスをポート 4 で学習します。これにより、再収束時間が短縮されます。

アクセススイッチであるスイッチ A を設定し、MAC アドレス テーブル移動更新メッセージを送信（*send*）することができます。また、アップリンク スイッチ B、C、および D を設定して、MAC アドレス テーブル移動更新メッセージの取得（*get*）および処理を行うこともできます。スイッチ C がスイッチ A から MAC アドレス テーブル移動更新メッセージを受信すると、スイッチ C はポート 4 で PC の MAC アドレスを学習します。スイッチ C は、PC の転送テーブル エントリを含め、MAC アドレス テーブルをアップデートします。

スイッチ A が、MAC アドレス テーブル移動更新を待機する必要はありません。スイッチはポート 1 上の障害を検出すると、ただちに、新しい転送ポートであるポート 2 からのサーバ トラフィックの転送を開始します。この変更は、100 ミリ秒（ms）以内に行われます。PC はスイッチ A に直接接続され、その接続状態に変更はありません。スイッチ A による、MAC アドレス テーブルでの PC エントリの更新は必要ありません。

図 18-3　MAC アドレス テーブル移動更新の例



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.18-4）
- 「設定時の注意事項」（P.18-5）
- 「Flex Link の設定」（P.18-6）
- 「Flex Link の VLAN ロード バランシングの設定」（P.18-8）
- 「MAC アドレス テーブル移動更新機能の設定」（P.18-9）

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。

- 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 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。

	コマンド	目的
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** *interface-id* **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	**switchport backup interface** *interface-id* **preemption delay** *delay-time*	ポートが他のポートより先に使用されるまでの遅延時間を設定します。 （注）　遅延時間の設定は、forced モードおよび bandwidth モードでのみ有効です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
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
ステップ 1	**configure terminal**	グローバル コ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* **prefer vlan** *vlan-range*	物理レイヤ 2 インターフェイス（またはポート チャネル）をインターフェイスがある 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。
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。

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すると、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 を保持します。

```
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 Gi0/8 ではブロックされ、Gi0/6 でフォワーディングされます。

```
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。

	コマンド	目的
ステップ 3	**switchport backup interface** *interface-id* または **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*	物理レイヤ 2 インターフェイス（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。 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 : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
```

```
Xmt last interface : None
```

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 ・ s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 18-1 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 18-1　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 backup**	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。



CHAPTER 19

DHCP 機能の設定

この章では、Catalyst 2960 スイッチで DHCP スヌーピングと Option 82 データ挿入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 機能の概要」（P.19-1）
- 「DHCP 機能の設定」（P.19-7）
- 「DHCP スヌーピング情報の表示」（P.19-12）

DHCP 機能の概要

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.19-2）
- 「DHCP リレー エージェント」（P.19-2）
- 「DHCP スヌーピング」（P.19-2）
- 「Option 82 データ挿入」（P.19-3）
- 「DHCP スヌーピング バインディング データベース」（P.19-5）

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。このデータベースの詳細については、「DHCP スヌーピング情報の表示」（P.19-12）を参照してください。

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 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。

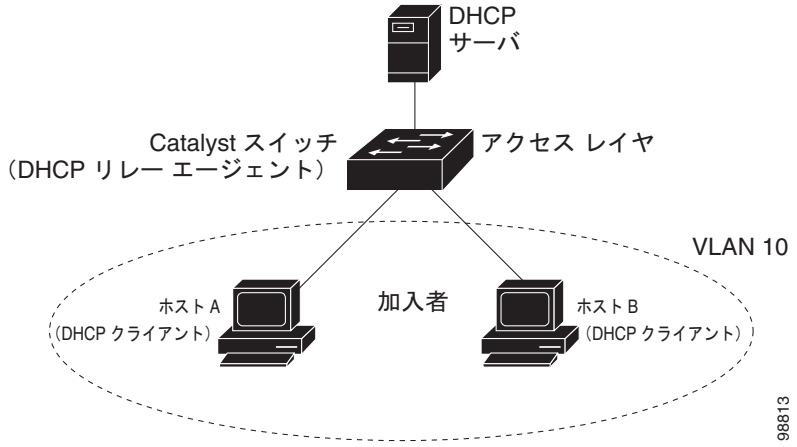
Option 82 データ挿入

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 19-1 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 19-1　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 19-2 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

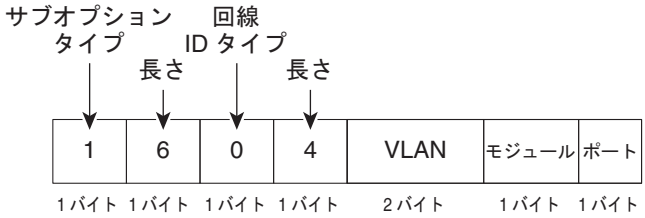
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

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。

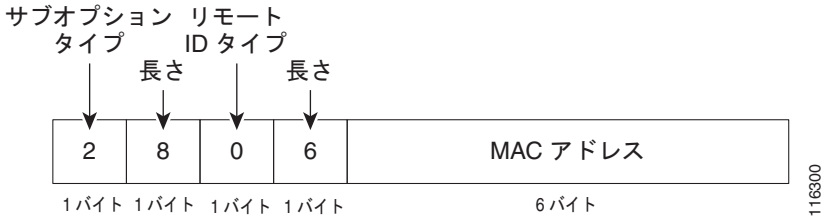
図 19-2 は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合です。

図 19-2　サブオプションのパケット形式

回線 ID サブオプション フレーム フォーマット



リモート ID サブオプション フレーム フォーマット



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。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
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の *initial-checksum* エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa0/4 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 機能の設定

ここでは、次の設定情報について説明します。

- 「DHCP のデフォルト設定」（P.19-7）
- 「DHCP スヌーピング設定時の注意事項」（P.19-7）
- 「DHCP リレー エージェントの設定」（P.19-9）
- 「DHCP スヌーピングおよび Option 82 のイネーブル化」（P.19-9）
- 「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.19-11）

DHCP のデフォルト設定

表 19-1 に、DHCP のデフォルト設定を示します。

表 19-1　DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要。[1]
DHCP リレー エージェント	イネーブル。[2]
DHCP パケット転送アドレス	未設定。
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）。[2]
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。[2]
DHCP スヌーピングをグローバルにイネーブル	ディセーブル。
DHCP スヌーピング情報オプション	イネーブル。
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[3]	ディセーブル。
DHCP スヌーピング レート制限	未設定。
DHCP スヌーピング信頼状態	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。
- 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.6-3）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。
- Cisco IOS Release 12.2(37)SE から、**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。

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一連の 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 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。 **（注）** このコマンドは、信頼できるデバイスに接続された集約スイッチだけで入力してください。
ステップ 6	**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 7	**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。**no** キーワードを使用すると、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できます。デフォルト設定は untrusted です。
ステップ 8	**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 スヌーピングがイネーブルである複数の 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 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	**ip dhcp snooping verify mac-address**	（任意）信頼できないポートに着信した DHCP パケットの送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認するようにスイッチを設定します。デフォルトでは、送信元 MAC アドレスがパケットのクライアント ハードウェア アドレスと一致することを確認します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show running-config**	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。

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 2	**ip dhcp snooping database** {**flash:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 • **flash:**/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*
ステップ 3	**ip dhcp snooping database timeout** *seconds*	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルト値は 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** *seconds*	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルト値は 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 19-2 に示す特権 EXEC コマンドを使用します。

表 19-2　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。



CHAPTER 20

IGMP スヌーピングおよび MVR の設定

この章では、Internet Group Management Protocol（IGMP）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。

（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 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.20-1）
- 「IGMP スヌーピングの設定」（P.20-7）
- 「IGMP スヌーピング情報の表示」（P.20-16）
- 「MVR の概要」（P.20-18）
- 「MVR の設定」（P.20-20）
- 「MVR 情報の表示」（P.20-24）
- 「IGMP フィルタリングおよびスロットリングの設定」（P.20-24）
- 「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.20-29）

（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、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。

（注）　IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャスト ルータは、すべての VLAN に一般クエリーを定期的に送信します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

スイッチは、MAC（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.20-14）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.20-3）
- 「マルチキャスト グループへの加入」（P.20-3）
- 「マルチキャスト グループからの脱退」（P.20-5）
- 「即時脱退」（P.20-6）
- 「IGMP 脱退タイマーの設定」（P.20-6）
- 「IGMP レポート抑制」（P.20-6）

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。

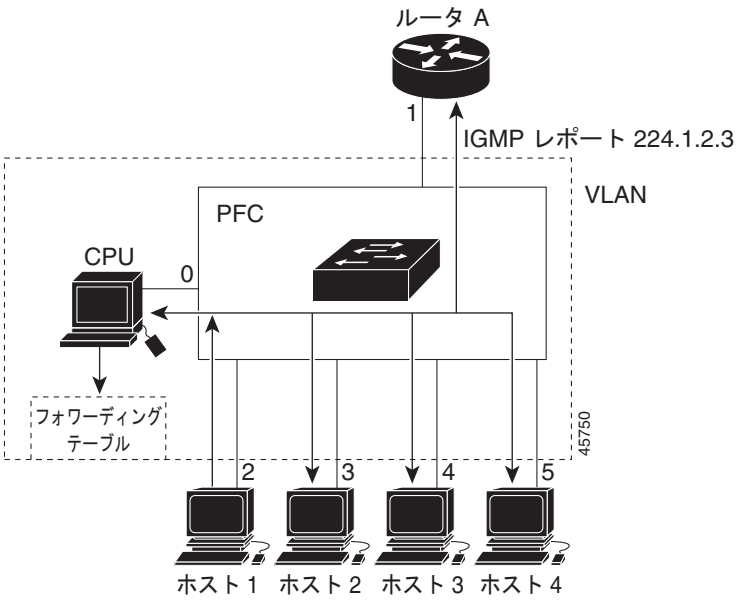
IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細については、次の URL を参照してください。

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 20-1 を参照してください。

図 20-1　IGMP Join の初期メッセージ



ルータ A がスイッチに一般クエリーを送り、スイッチはそのクエリーをポート 2 ～ 5、つまり同一 VLAN のすべてのメンバーに転送します。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 20-1 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 20-1　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 20-2 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 20-2 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 20-2　2 番めのホストのマルチキャスト グループへの加入

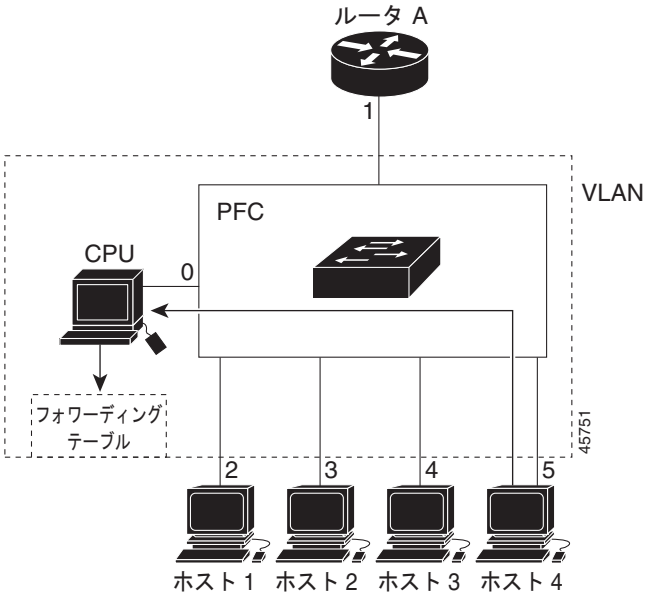


表 20-2　更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリーを定期的に送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャスト トラフィックを受信しなければならない場合、ルータは VLAN に引き続き、マルチキャスト トラフィックを転送します。スイッチは、その IGMP スヌーピングによって維持された IP マルチキャスト グループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したスイッチは、グループ固有のクエリーを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャスト グループのトラフィックに関与しているかどうかを学習します。スイッチはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼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.20-11）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あと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.20-11）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.20-16）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.20-7）
- 「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.20-7）
- 「スヌーピング方法の設定」（P.20-8）
- 「マルチキャスト ルータ ポートの設定」（P.20-9）
- 「グループに加入するホストの静的な設定」（P.20-10）
- 「IGMP 即時脱退のイネーブル化」（P.20-11）
- 「IGMP 脱退タイマーの設定」（P.20-11）
- 「TCN 関連のコマンドの設定」（P.20-12）
- 「IGMP スヌーピング クエリアの設定」（P.20-14）
- 「IGMP レポート抑制のディセーブル化」（P.20-16）

IGMP スヌーピングのデフォルト設定

表 20-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 20-3　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
ステップ 1	**configure terminal**	グローバル コ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 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 スヌーピングをグローバルにイネーブルに設定しておく必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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。

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** *vlan-id* **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** *vlan-id* **mrouter interface** *interface-id*	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。VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ip-address* 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* **immediate-leave**	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。
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 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** *time*	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 ～ 5000 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 ～ 5000 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.20-12）
- 「フラッディング モードからの回復」（P.20-13）
- 「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.20-13）

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

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、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 tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニング ツリーのルートであるかどうかに関わらず、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
ステップ 1	**configure terminal**	グローバル コ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	**no ip igmp snooping tcn flood**	スパニング ツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
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** *ip_address*	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用しようとします。 **（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** *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 5	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]	（任意）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 ～ 10 です。指定できる interval の範囲は 1 ～ 255 秒です。
ステップ 6	**ip igmp snooping querier timer expiry** *timeout*	（任意）IGMP クエリアが期限切れになる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 20-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 20-4　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
show ip igmp snooping [**vlan** *vlan-id*]	スイッチ上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。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**] | **user**[**count**]]	マルチキャスト VLAN またはその VLAN の特定のパラメータについて、マルチキャスト テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 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。 • *ip_address*：指定のグループ IP アドレスのマルチキャスト グループについて、特性を表示します。 • **user**：ユーザによって設定されたマルチキャスト エントリだけを表示します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	動的に学習された、あるいは手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 **（注）** IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**vlan** *vlan-id*]	IP アドレス、および VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	IP アドレスおよび VLAN で受信した最新の IGMP クエリー メッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。

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 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。

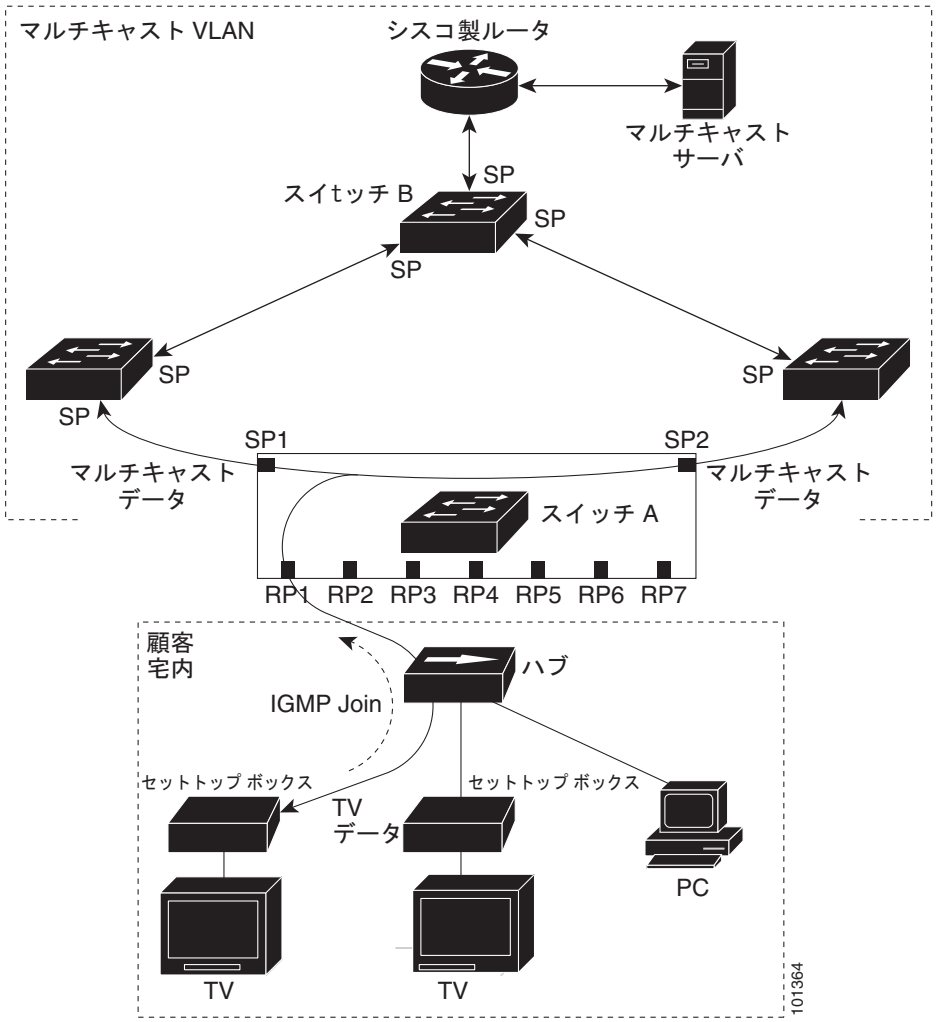
- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホスト メンバシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバー ポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 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 20-3 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 20-3　　MVR の例



RP = レシーバー ポート
SP = 送信元ポート

注：　すべての送信元ポートは
マルチキャスト VLAN に所属します。

加入者がチャネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップ ボックスからマルチキャスト ストリームに対する IGMP Leave メッセージが送信されます。スイッチの CPU は、レシーバー 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.20-20）
- 「MVR 設定時の注意事項および制限事項」（P.20-21）
- 「MVR グローバル パラメータの設定」（P.20-21）
- 「MVR インターフェイスの設定」（P.20-23）

MVR のデフォルト設定

表 20-5 に、MVR のデフォルト設定を示します。

表 20-5　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

表 20-5　MVR のデフォルト設定 （続き）

機能	デフォルト設定
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（ポート単位）	レシーバー ポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

MVR 設定時の注意事項および制限事項

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。

	コマンド	目的
ステップ 3	**mvr group** *ip-address* [*count*]	スイッチ上で IP マルチキャスト アドレスを設定するか、または *count* パラメータを使用して、連続する MVR グループ アドレスを設定します（*count* の範囲は 1 ～ 256、デフォルトは 1）。このアドレスに送信されたマルチキャスト データは、スイッチ上のすべての送信元ポートおよびそのマルチキャスト アドレスのデータを受信するために選ばれたすべてのレシーバー 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。
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** | **compatible**}	（任意）MVR の動作モードを指定します。 • **dynamic**：送信元ポートでダイナミック MVR メンバ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 2 MVR 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** **show mvr interface** 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。

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 gigabitethernet0/2
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 20-6 のコマンドを使用します。

表 20-6　MVR 情報を表示するためのコマンド

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。
show mvr interface [*interface-id*] [**members** [**vlan** *vlan*-**id**]]	すべての MVR インターフェイスおよびそれぞれの 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。 • Type：RECEIVER（レシーバー）または SOURCE（送信元） • 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、ポートが転送中または転送中ではないことを示します。 – INACTIVE は、ポートが VLAN に含まれていないことを意味します。 • Immediate Leave（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 [*ip-address*]	すべての IP マルチキャスト グループまたは指定した IP マルチキャスト グループ IP アドレスに含まれているレシーバー ポートおよび送信元ポートがすべて表示されます。

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.20-25）
- 「IGMP プロファイルの設定」（P.20-26）（任意）
- 「IGMP プロファイルの適用」（P.20-27）（任意）
- 「IGMP グループの最大数の設定」（P.20-27）（任意）
- 「IGMP スロットリング アクションの設定」（P.20-28）（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 20-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 20-7　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.20-28）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。
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。
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。

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（制限なし）に戻すには、このコマンドの **no** 形式を使用します。

このコマンドは、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** *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。

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 20-8 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 20-8　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ド

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	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上のすべてのインターフェイスの設定を表示します。



CHAPTER 21

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.21-1）
- 「保護ポートの設定」（P.21-5）
- 「ポート ブロッキングの設定」（P.21-7）
- 「ポート セキュリティの設定」（P.21-8）
- 「ポート単位のトラフィック制御設定の表示」（P.21-18）

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.21-1）
- 「ストーム制御のデフォルト設定」（P.21-3）
- 「ストーム制御およびしきい値レベルの設定」（P.21-3）

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。

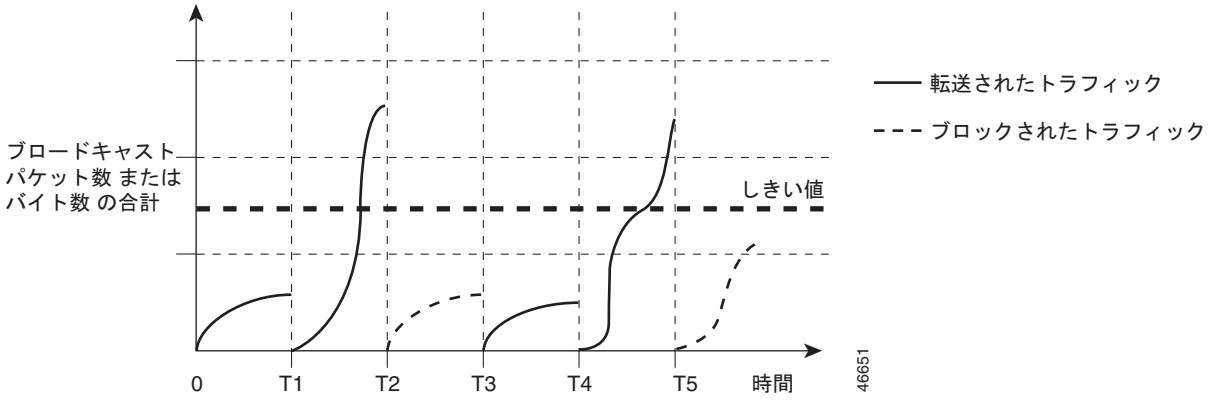
- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のパケット数
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レートの秒単位のビット数

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。

（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 21-1 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。

図 21-1　ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過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** *pps* [*pps-low*]}	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 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 ～ 10000000000.0 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 ～ 10000000000.0 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 ～ 10000000000.0 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** ～ 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、g など）を使用できます。

	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 error-disable 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
```

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.21-6）
- 「保護ポート設定時の注意事項」（P.21-6）
- 「保護ポートの設定」（P.21-6）

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。

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.21-7）
- 「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.21-7）

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。

マルチキャストおよびユニキャスト パケットのフラッディングをインターフェイスで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。
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。
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.21-8）
- 「ポート セキュリティのデフォルト設定」（P.21-10）
- 「ポート セキュリティの設定時の注意事項」（P.21-11）
- 「ポート セキュリティのイネーブル化および設定」（P.21-12）
- 「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.21-16）

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.21-8）
- 「セキュリティ違反」（P.21-9）

セキュア MAC アドレス

ポートで許可されるセキュア アドレスの最大数を設定するには、**switchport port-security maximum** *value* インターフェイス コンフィギュレーション コマンドを使用します。

（注）　最大値をインターフェイス上ですでに設定されているセキュア アドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- スタティック セキュア MAC アドレス：**switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- ダイナミック セキュア MAC アドレス：動的に設定されてアドレス テーブルにのみ保存され、スイッチの再起動時に削除されます。
- *スティッキー* セキュア MAC アドレス：動的に学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

*スティッキー ラーニング*をイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。スティッキー ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはスティッキー ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキー 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対処に基づいて、次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。

（注） トランク ポートに protect 違反モードを設定することは推奨しません。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 21-1 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。

表 21-1　セキュリティ違反モードの処置

違反モード	トラフィックの転送[1]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示[2]	違反カウンタの増加	ポートのシャットダウン
protect	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]

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 21-2 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 21-2　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。

（注）　音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN 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 には最大で 2 つの MAC アドレスが必要になります。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。
- 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 21-3 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 21-3　　他のスイッチ機能とポート セキュリティとの互換性

ポート タイプまたはポートの機能	ポート セキュリティとの互換性
DTP [1] ポート[2]	なし
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 アナライザ）送信元ポート	あり
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	**switchport mode** {**access** | **trunk**}	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。 *vlan-id* : 音声トラフィックに使用する VLAN を指定します。
ステップ 5	**switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。
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 [violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]	（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。 **（注）** トランク ポートに protect モードを設定することは推奨しません。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	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 **（注）** このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。 • *vlan-id*：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 1 つを入力してください。 • *vlan-id*：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。
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 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 FastEthernet0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングの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 port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。 **（注）** スイッチは、スティッキー セキュア アドレスのポート セキュリティ エージングをサポートしていません。 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。 *time* 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 ～ 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	**show port-security** [**interface** *interface-id*] [**address**]	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 コマンドを使用します。

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 21-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 21-4　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** *interface-id*]	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を、各インターフェイスで許容されるセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [**interface** *interface-id*] **address**	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface *interface-id* **vlan**	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。



CHAPTER 22

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.22-1）
- 「CDP の設定」（P.22-2）
- 「CDP のモニタおよびメンテナンス」（P.22-4）

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.22-2）
- 「CDP の特性の設定」（P.22-2）
- 「CDP のディセーブル化およびイネーブル化」（P.22-3）
- 「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.22-4）

CDP のデフォルト設定

表 22-1 に、CDP のデフォルト設定を示します。

表 22-1　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。

（注）　ステップ 2 ～ 4 はすべて任意であり、どの順番で実行してもかまいません。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp timer** *seconds*	（任意）CDP 更新の送信頻度（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。

	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.22-4）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。

（注）　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
```

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。

コマンド	説明
show cdp entry *entry-name* [**protocol** | **version**]	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。
show cdp interface [*interface-id*]	CDP がイネーブルに設定されているインターフェイス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。
show cdp neighbors [*interface-id*] [**detail**]	デバイス　タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、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。



CHAPTER 23

LLDP および LLDP-MED の設定

この章では、Catalyst 2960 スイッチで Link Layer Discovery Protocol（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）を設定する方法について説明します。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（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。

- 「LLDP および LLDP-MED の概要」（P.23-1）
- 「LLDP および LLDP-MED の設定」（P.23-3）
- 「LLDP および LLDP-MED のモニタリングおよびメンテナンス」（P.23-7）

LLDP および LLDP-MED の概要

ここでは、次の概要について説明します。

- 「LLDP の概要」（P.23-1）
- 「LLDP-MED の概要」（P.23-2）

LLDP の概要

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探索プロトコルです。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。設定の情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV（IEEE 802.1 に固有の TLV）
- MAC/PHY コンフィギュレーション / ステータス TLV（IEEE 802.3 に固有の TLV）

（注）　スイッチ スタックは、ネットワーク内で 1 つのスイッチと見なされます。したがって、LLDP は個々のスタック メンバーではなく、スイッチ スタックを検出します。

LLDP-MED の概要

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。

- 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。

- 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。

- 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）へ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。

（注）　LLDP と LLDP-MED は、ネットワーク内で同時に動作できません。デフォルトでは、ネットワーク デバイスは、エンドポイント デバイスから LLDP-MED パケットを受信するまで、LLDP パケットのみを送信します。その後ネットワーク デバイスは、LLDP パケットのみを受信するまで、LLDP-MED パケットを送信します。

LLDP および LLDP-MED 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 LLDP 設定」（P.23-3）
- 「LLDP 特性の設定」（P.23-4）
- 「LLDP のグローバルなディセーブル化およびイネーブル化」（P.23-4）
- 「インターフェイス上での LLDP のディセーブル化およびイネーブル化」（P.23-5）
- 「LLDP-MED TLV の設定」（P.23-6）

デフォルト LLDP 設定

表 23-1 に、LLDP のデフォルト設定を示します。デフォルト設定を変更するには、LLDP グローバル コンフィギュレーション コマンドおよび LLDP インターフェイス コンフィギュレーション コマンドを使用します。

表 23-1　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	イネーブル
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	イネーブル（すべての TLV を送受信可）
LLDP インターフェイス ステート	イネーブル
LLDP 受信	イネーブル

表 23-1　デフォルト LLDP 設定 （続き）

機能	デフォルト設定
LLDP 送信	イネーブル
LLDP med-tlv-select	イネーブル（すべての LLDP-MED TLV を送信可）

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。

これら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。

（注）　ステップ 2 ～ 5 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	**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**	（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** *seconds*	（任意）LLDP 更新の送信頻度（秒）を設定します。 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	**copy running-config startup-config**	（任意）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
```

その他の LLDP **show** コマンドについては、「LLDP および LLDP-MED のモニタリングおよびメンテナンス」（P.23-7）を参照してください。

LLDP のグローバルなディセーブル化およびイネーブル化

LLDP はデフォルトでイネーブルです。

LLDP をグローバルに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 lldp run**	LLDP 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 LLDP-MED 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**	LLDP 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、LLDP をグローバルにディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# no lldp run
Switch(config)# end
```

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
```

インターフェイス上での LLDP のディセーブル化およびイネーブル化

LLDP 情報を送受信するために、サポートされるすべてのインターフェイスで LLDP はデフォルトでイネーブルになっています。

（注）　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。

インターフェイス上で LLDP 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*	LLDP 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 lldp transmit**	インターフェイス上で LLDP パケットは送信されません。
ステップ 4	**no lldp receive**	インターフェイス上で LLDP パケットは受信されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ディセーブル化されている LLDP をインターフェイス上で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 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	**lldp transmit**	インターフェイス上で LLDP パケットは送信されます。
ステップ 4	**lldp receive**	インターフェイス上で LLDP パケットは受信されます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）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 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-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 パケットのみを送信します。デバイスは LLDP パケットのみを受信するまで、LLDP-MED パケットの送信を続けます。

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 23-2 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 23-2　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*	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	**no lldp med-tlv-select** *tlv*	ディセーブルにする 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。

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** *tlv*	イネーブルにする TLV を指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
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、ディセーブル化されている 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
```

LLDP および LLDP-MED のモニタリングおよびメンテナンス

デバイス上の LLDP および LLDP-MED をモニタリングおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

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	ネイバに関する情報を格納する LLDP テーブルを削除します。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間など、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（*）を入力してすべての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。
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。 必要なインターフェイスの情報だけを表示できます。

コマンド	説明
show lldp neighbors [*interface-id*] [**detail**]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバ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。



CHAPTER 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）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。アグレシッブ モードの UDLD は、光ファイバ リンクおよびツイストペア リンク上の片方向トラフィックと、光ファイバ リンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ 1 のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバ 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 メカニズムはリンクの物理的な問題を検出しないため、リンクは稼動状態でなくなります。この場合、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。

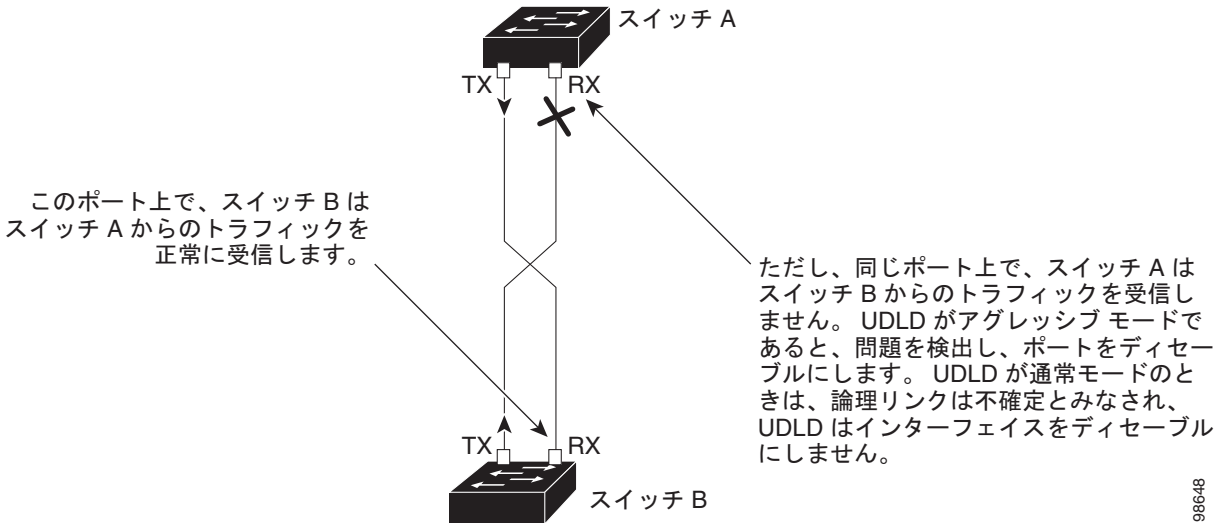
  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

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。

図 24-1　UDLD による単一方向リンクの検出



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.24-4）
- 「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.24-5）
- 「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.24-6）

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。

注意　ループ ガードは、ポイントツーポイント リンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

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 time** *message-timer-interval*}	UDLD の動作モードを指定します。 • **aggressive**：すべての光ファイバ ポート上で、UDLD をアグレッシブ モードでイネーブルにします。 • **enable**：スイッチ上のすべての光ファイバ ポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、**udld enable** グローバル コンフィギュレーション コマンドの設定を上書きします。 アグレッシブおよび通常モードの詳細については、「動作モード」（P.24-1）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.24-5）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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。

	コマンド	目的
ステップ 3	**udld port** [**aggressive**]	UDLD はデフォルトでディセーブルです。 • **udld port**：指定されたポート上で、UDLD を通常モードでイネーブルにします。 • **udld port aggressive**：指定されたポート上で、UDLD をアグレッシブ モードでイネーブルにします。 （注）　特定の光ファイバ ポート上で UDLD をディセーブルにする場合は、**no udld port** インターフェイス コンフィギュレーション コマンドを使用します。 アグレッシブおよび通常モードの詳細については、「動作モード」（P.24-1）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 コマンドのあとに **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。



CHAPTER 25

SPAN および RSPAN の設定

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。

（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。

- 「SPAN および RSPAN の概要」（P.25-1）
- 「SPAN および RSPAN の設定」（P.25-9）
- 「SPAN および RSPAN のステータス表示」（P.25-24）

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。

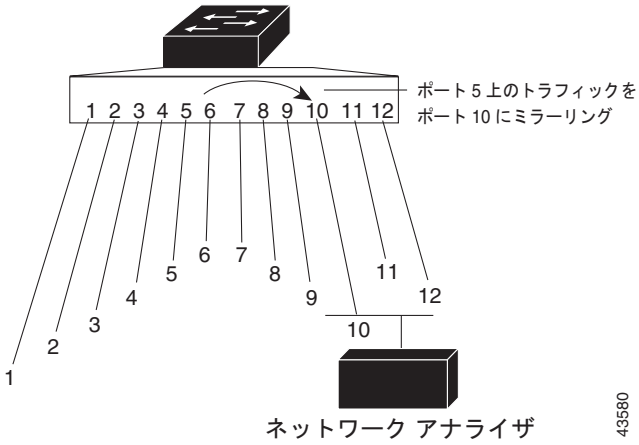
ここでは、次の概要について説明します。

- 「ローカル SPAN」（P.25-2）
- 「リモート SPAN」（P.25-2）
- 「SPAN と RSPAN の概念および用語」（P.25-3）
- 「SPAN および RSPAN と他の機能の相互作用」（P.25-8）

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。たとえば、図 25-1 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。

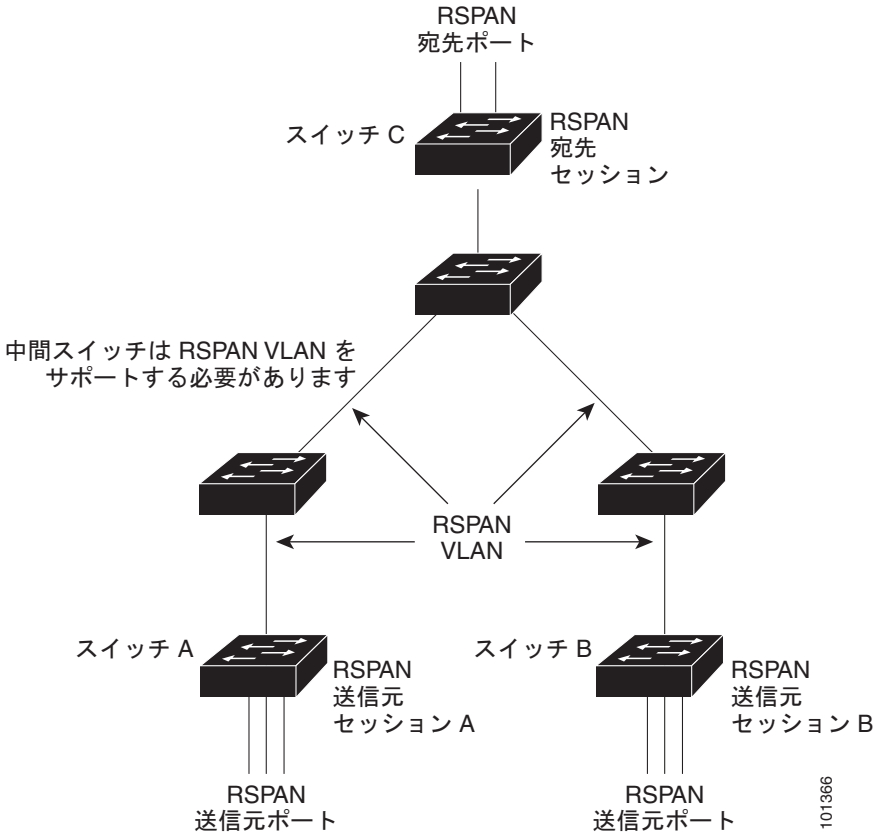
図 25-1　　単一スイッチでのローカル SPAN の設定例



リモート SPAN

RSPAN は異なるスイッチ（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 25-2 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 25-2　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.25-7）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.25-9）
- 「ローカル SPAN の設定」（P.25-9）
- 「RSPAN の設定」（P.25-16）

SPAN および RSPAN のデフォルト設定

表 25-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 25-1　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.25-10）
- 「ローカル SPAN セッションの作成」（P.25-10）
- 「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.25-13）
- 「フィルタリングする VLAN の指定」（P.25-15）

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** | **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 ～ 66 です。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* 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 *interface-id* 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。 • *vlan-id* 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。 *interface-id* 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	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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 へ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.25-10）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	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation {dot1q | replicate}**] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 *session_number* 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。 *interface-id* 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	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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** | **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 ～ 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 ～ 66 です。 *interface-id* 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。 *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。 *vlan-id* 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。

	コマンド	目的
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。 *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。 *interface-id* 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。
ステップ 7	**show monitor** [**session** *session_number*] **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。

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.25-17）
- 「RSPAN VLAN としての VLAN の設定」（P.25-17）
- 「RSPAN 送信元セッションの作成」（P.25-18）
- 「RSPAN 宛先セッションの作成」（P.25-20）
- 「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.25-21）
- 「フィルタリングする VLAN の指定」（P.25-23）

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.25-10）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 以下）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 ～ 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 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 *session_number* の範囲は、1 ～ 66 です。 RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 • *interface-id* 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。 • *vlan-id* 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* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 *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。
ステップ 6	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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** *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 ～ 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 6	**monitor session** *session_number* **source remote vlan** *vlan-id*	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 ～ 66 です。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 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。 *interface-id* 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。

	コマンド	目的
ステップ 9	**show monitor** [**session** *session_number*] **show running-config**	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。

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.25-20）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。
ステップ 3	**monitor session** *session_number* **source remote vlan** *vlan-id*	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 ～ 66 です。 *vlan-id* には、モニタする送信元 RSPAN VLAN 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* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。 *session_number* には、ステップ 4 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。 *interface-id* 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*] **show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RSPAN 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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションに対する既存の SPAN 設定を削除します。 *session_number* の範囲は、1 ～ 66 です。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
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 ～ 66 です。 *interface-id* 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。 *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。 *vlan-id* 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** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number* 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。 *vlan-id* 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	**show monitor** [**session** *session_number*] **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。

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 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 26

RMON の設定

この章では、Catalyst 2960 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。

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。

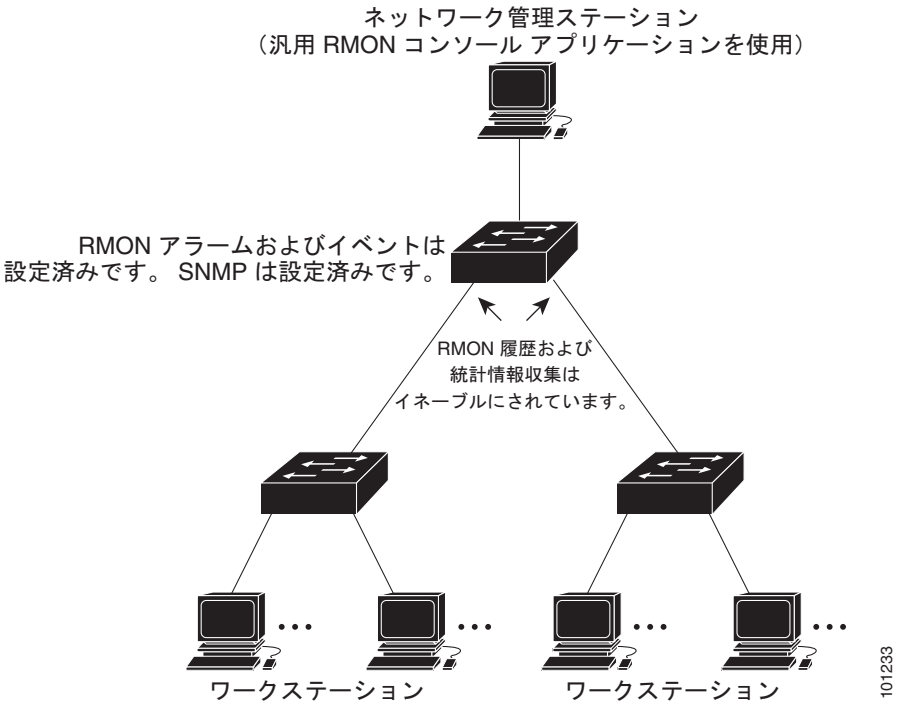
この章で説明する内容は、次のとおりです。

- 「RMON の概要」（P.26-1）
- 「RMON の設定」（P.26-2）
- 「RMON ステータスの表示」（P.26-6）

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 26-1 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。

図 26-1　リモート モニタリングの例



スイッチは次の RMON グループ（RFC 1757 で定義）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。

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.26-3）
- 「RMON アラームおよびイベントの設定」（P.26-3）（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.26-5）（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.26-5）（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 28 章「SNMP の設定」を参照してください。

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。

	コマンド	目的
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** *string* 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**	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、**no rmon 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、**no rmon 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** *index* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]	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。 • *index* 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。
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。

	コマンド	目的
ステップ 3	**rmon collection stats** *index* [**owner** *ownername*]	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。 • *index* 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 26-1 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 26-1　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。



CHAPTER 27

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.27-1）
- 「システム メッセージ ロギングの設定」（P.27-2）
- 「ロギング設定の表示」（P.27-14）

注意 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。

（注） Syslog フォーマットは 4.3 Berkeley Standard Distribution（BSD）UNIX と互換性があります。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログ メッセージにタイム スタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステム メッセージ ガイドを参照してください。

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.27-2）
- 「システム メッセージ ロギングのデフォルト設定」（P.27-3）
- 「メッセージ ロギングのディセーブル化」（P.27-4）（任意）
- 「メッセージ表示宛先デバイスの設定」（P.27-5）（任意）
- 「ログ メッセージの同期化」（P.27-6）（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.27-7）（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.27-8）（任意）
- 「メッセージ重大度の定義」（P.27-8）（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.27-10）（任意）
- 「設定変更ロガーのイネーブル化」（P.27-11）（任意）
- 「UNIX Syslog サーバの設定」（P.27-12）（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 27-1 に、Syslog メッセージの要素を示します。

表 27-1　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.27-8）を参照してください。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。**service timestamps log [datetime | log]** グローバル コンフィギュレーション コマンドが設定されている場合だけ、この情報が表示されます。 詳細については、「ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化」（P.27-7）を参照してください。
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 27-4（P.27-13）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 27-3（P.27-9）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 27-2 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 27-2　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 27-3（P.27-9）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

表 27-2　システム メッセージ ロギングのデフォルト設定 （続き）

機能	デフォルト設定
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 27-4（P.27-13）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 27-3（P.27-9）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** または **show logging**	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.27-6）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。 **（注）** バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサ メモリを表示するには、**show memory** 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定*しない*でください。
ステップ 3	**logging** *host*	UNIX Syslog サーバ ホストにメッセージを記録します。 *host* 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.27-12）を参照してください。
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 27-3（P.27-9）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。

	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。

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。

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*]	メッセージの同期ロギングを行うように、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** *line-number* コマンドを使用します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ～ 15 です。 16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。 **line vty 0 15** また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。 **line vty 2** このコマンドを入力すると、ライン コンフィギュレーション モードになります。

	コマンド	目的
ステップ 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]	メッセージの同期ロギングをイネーブルにします。 • （任意）**level** *severity-level* 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。
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。

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service timestamps log uptime** または **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	ログのタイム スタンプをイネーブルにします。 最初のコマンドを実行するとログ メッセージのタイム スタンプがイネーブルになり、システムを再起動した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 スタンプがイネーブルになります。選択したオプションに応じて、ローカル タイム ゾーンを基準とした日付、時間（ミリ秒）、タイム ゾーン名をタイム スタンプとして表示できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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。

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-channel1, 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。
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 27-3 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 27-3（P.27-9）を参照）。

	コマンド	目的
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 27-3（P.27-9）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 27-3（P.27-9）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.27-12）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** または **show logging**	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。

（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 27-3 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 27-3　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 27-3（P.27-9）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。 *level* キーワードのリストについては、表 27-3（P.27-9）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 27-3 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_chapter09186a00801a8086.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もっとも古いログ 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。

```
Switch# show archive log config all
 idx   sess           user@line      Logged command
   38     11   unknown user@vty3     |no aaa authorization config-commands
   39     12   unknown user@vty3     |no aaa authorization network default group radius
   40     12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41     13   unknown user@vty3     |no aaa accounting system default
   42     14           temi@vty4     |interface GigabitEthernet4/0/1
   43     14           temi@vty4     | switchport mode trunk
   44     14           temi@vty4     | exit
   45     16           temi@vty5     |interface FastEthernet5/0/1
```

```
46    16           temi@vty5     | switchport mode trunk
47    16           temi@vty5     | exit
```

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 27-4（P.27-13）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 27-3（P.27-9）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。*level* キーワードについては、表 27-3（P.27-9）を参照してください。
ステップ 4	**logging facility** *facility-type*	Syslog ファシリティを設定します。*facility-type* キーワードについては、表 27-4（P.27-13）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 27-4 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 27-4　ロギング facility-type キーワード

facility-type キーワード	説明
auth	許可システム
cron	cron ファシリティ
daemon	システム デーモン
kern	カーネル
local0 ～ local7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9 ～ sys14	システムで使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX から UNIX へのコピー システム

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。



CHAPTER 28

SNMP の設定

この章では、Catalyst 2960 スイッチに 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 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。

- 「SNMP の概要」（P.28-1）
- 「SNMP の設定」（P.28-6）
- 「SNMP ステータスの表示」（P.28-18）

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.28-2）
- 「SNMP マネージャ機能」（P.28-3）
- 「SNMP エージェント機能」（P.28-4）
- 「SNMP コミュニティ ストリング」（P.28-4）

- 「SNMP を使用して MIB 変数にアクセスする方法」（P.28-4）
- 「SNMP 通知」（P.28-5）
- 「SNMP ifIndex MIB オブジェクト値」（P.28-6）

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 28-1 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 28-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ ストリング	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。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	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。
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	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv （暗号化ソフトウェア イメージが必要）	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。 標準の CBC-DES（DES-56）に基づいた認証に加え、Data Encryption Standard（DES）56 ビット暗号化も可能です。

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 28-2 に示す動作を実行します。

表 28-2　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。

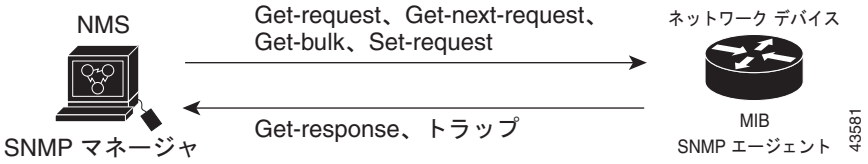
SNMP を使用して MIB 変数にアクセスする方法

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 28-1 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。

図 28-1　SNMP ネットワーク



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。

（注）　SNMPv1 は informs をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかが送信側にわからないからです。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 28-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 28-3　ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI[1]	1 ～ 4999
EtherChannel	5000 ～ 5012
ループバック	5013 ～ 5077
トンネル	5078 ～ 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 ～ 14500
ヌル	14501

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

ここでは、次の設定情報について説明します。

- 「SNMP のデフォルト設定」（P.28-7）
- 「SNMP 設定時の注意事項」（P.28-7）
- 「SNMP エージェントのディセーブル化」（P.28-8）
- 「コミュニティ ストリングの設定」（P.28-8）
- 「SNMP グループおよびユーザの設定」（P.28-10）
- 「SNMP 通知の設定」（P.28-12）
- 「エージェント コンタクトおよびロケーションの設定」（P.28-16）
- 「SNMP を通して使用する TFTP サーバの制限」（P.28-16）
- 「SNMP の例」（P.28-17）

SNMP のデフォルト設定

表 28-4 に、SNMP のデフォルト設定を示します。

表 28-4　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 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで **noauth**（noAuthNoPriv）になります。
SNMP 通知タイプ	タイプ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 Configuration Fundamentals Command Reference, Release 12.2*』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** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	コミュニティ ストリングを設定します。 • *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。
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	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	SNMP のローカル コピーまたはリモート コピー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、123400000000000000000000 というエンジン ID を設定する場合、**snmp-server engineID local 1234** のように入力できます。 • **remote** を指定した場合、SNMP のリモート コピーが置かれているデバイスの *ip-address* を指定し、任意でリモート デバイスの UDP ポートを指定します。デフォルト値は 162 です。

	コマンド	目的
ステップ 3	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート デバイスに新規 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（*privacy* とも呼ばれます）。 （注）　**priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。 • （任意）**read** *readview* 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	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	SNMP 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（64 文字以下）が必要です。 • （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。
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、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 28-5 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。

表 28-5　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。

表 28-5　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
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。
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。
hsrp	Hot Standby Router Protocol（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバ変更、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。
port-security	SNMP ポート セキュリティ トラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate *rate***
rtr	SNMP Response Time Reporter（RTR）のトラップを生成します。
snmp	認証、コールド スタート、ウォーム スタート、リンク アップ、またはリンク ダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 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 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。この機能は、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN 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）　**cpu** [**threshold**]、**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。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 28-5 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** *ip-address engineid-string*	リモート ホスト用のエンジン ID を指定します。
ステップ 3	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	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**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	SNMP グループを設定します。
ステップ 5	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]	SNMP トラップ動作の受信側を指定します。 • *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。 • *community-string* 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。 • （任意）*notification-type* には、表 28-5（P.28-12）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** *notification-types*	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 28-5（P.28-12）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。
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。

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server tftp-server-list** *access-list-number*	SNMP を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。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、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。
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 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 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP 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 28-6 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, Release 12.2*』を参照してください。

表 28-6　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。



CHAPTER 29

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、アクセス制御リスト（ACL）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、コマンドやテーブルではアクセス リストとも呼ばれます。

（注） この章の IP ACL に関する情報は、IP Version 4（IPv4）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.29-1）
- 「IPv4 ACL の設定」（P.29-4）
- 「名前付き MAC 拡張 ACL の作成」（P.29-20）
- 「IPv4 ACL の設定の表示」（P.29-22）

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。

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.31-7）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.29-2）
- 「フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理」（P.29-3）

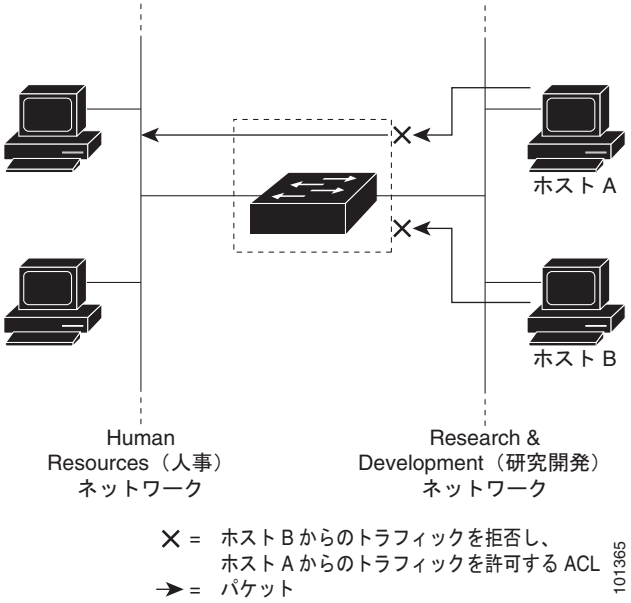
ポート ACL

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

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 29-1 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 29-1　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

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 29-1（P.29-6）を参照）またはブリッジ グループ ACL
- IP アカウンティング
- 着信および発信レート制限（QoS ACL によるレート制限を除く）
- リフレクシブ ACL またはダイナミック ACL（スイッチ クラスタリング機能で使用される専用のダイナミック ACL を除く）
- 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。

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.29-5）
- 「端末回線への IPv4 ACL の適用」（P.29-16）
- 「インターフェイスへの IPv4 ACL の適用」（P.29-17）
- 「ハードウェアおよびソフトウェアによる IP ACL の処理」（P.29-17）
- 「IPv4 ACL の設定例」（P.29-18）

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.29-6）
- 「番号付き標準 ACL の作成」（P.29-7）
- 「番号付き拡張 ACL の作成」（P.29-8）
- 「ACL 内の ACE の並べ替え」（P.29-12）
- 「名前付き標準 ACL および名前付き拡張 ACL の作成」（P.29-12）
- 「ACL での時間範囲の使用」（P.29-14）
- 「ACL へのコメントの挿入」（P.29-15）

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 29-1 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 29-1　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 ～ 99	IP 標準アクセス リスト	あり
100 ～ 199	IP 拡張アクセス リスト	あり
200 ～ 299	プロトコル タイプコード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 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 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200 ～ 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 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	あり

（注） 番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

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。 *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。 *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* 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。
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.29-16）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.29-17）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と宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

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。

（注） このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、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	**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*] （注）　**dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* 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。 （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。 *source* 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。 *destination* 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。 *destination-wildcard* 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。 • 0.0.0.0 255.255.255.255（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.29-14）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 0.0.0.0 255.255.255.255 の省略形と destination および destination wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよびワイルドカードの代わりに **any** キーワードを使用できます。
または	**access-list** *access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	source および source wildcard の値 *source* 0.0.0.0 の省略形と destination および destination wildcard の値 *destination* 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のワイルドカードまたはマスクの代わりに **host** キーワードを使用できます。
ステップ 2b	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*]	（任意）拡張 TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は **tcp** を入力します。 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）。 *port* 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、『*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。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。 • *flag*：指定された TCP ヘッダー ビットを基準にして照合します。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。
ステップ 2c	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 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。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[*operator* [*port*]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag** および **established** パラメータは無効です。

	コマンド	目的
ステップ 2d	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 ICMP アクセス リストおよびアクセス条件を定義します。 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。 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。 • *icmp-type*：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。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリング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、『*Cisco IOS IP Configuration Guide, Release 12.2*』の「Configuring IP Services」を参照してください。
ステップ 2e	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 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。 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。 *igmp-type*：IGMP メッセージ タイプと照合するには、0 ～ 15 の番号またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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。

（注）　ACL を作成するときには、アクセス リストの末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号付き拡張 ACL を端末回線（「端末回線への IPv4 ACL の適用」（P.29-16）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.29-17）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、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_guide09186a0080134a60.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.29-5）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
ステップ 3	**deny** {*source* [*source-wildcard*] | **host** *source* | **any**} または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**}	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。 • **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
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 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** *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**time-range** *time-range-name*]	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。 プロトコルおよび他のキーワードの定義については、「番号付き拡張 ACL の作成」（P.29-8）を参照してください。 • **host** *source*：source および source wildcard の値 *source* 0.0.0.0 • ***host destination***：destination および destination wildcard の値 *destination* 0.0.0.0 • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。
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.29-17）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.29-5）および「名前付き標準 ACL および名前付き拡張 ACL の作成」（P.29-12）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。

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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**time-range** *time-range-name*	作成する時間範囲には意味のある名前（*workhours* など）を割り当て、時間範囲コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 3	**absolute** [**start** *time date*] [**end** *time date*] または **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* または **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	適用対象の機能がいつ動作可能になるかを指定します。 • 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 • 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	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。

設定した時間範囲の制限を削除するには、**no time-range** *time-range-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、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
   10 deny tcp any any time-range new_year_day_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入

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.29-17）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。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ～ 16 です。
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	（デバイスへの）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
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 インターフェイスだけに適用してください。
- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。

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。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in**}	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。
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**} 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
```

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。

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。

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 gigabitethernet0/1
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。

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。
ステップ 3	{**deny** | **permit**} {**any** | **host** *source MAC address* | *source MAC address mask*} {**any** | **host** *destination MAC address* | *destination MAC address mask*} [*type mask* | **lsap** *lsap mask* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp** | *0-65535*] [**cos** *cos*]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての（**any**）送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト（**host**）送信元 MAC アドレス、およびすべての（**any**）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。 （任意）以下のオプションを入力することもできます。 • *type mask*：Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる *don't care* ビットのマスクが EtherType に適用されます。 • **lsap** *lsap mask*：IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で *don't care* ビットのマスクを指定できます。 • **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**—A non-IP protocol. • **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	**show mac access-group** [**interface** *interface-i*d]	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
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 *mac1* をポートに適用してポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface 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 29-2 に記載された特権 EXEC コマンドを使用します。

表 29-2　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。
show running-config [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface** ***interface-i***d]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。



CHAPTER 30

Cisco IOS IP SLA 動作の設定

この章では、Catalyst 2960 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。Catalyst 2960 スイッチは、IP SLA responder の機能だけをサポートしているので、IP SLA 機能をすべてサポートしているデバイスにのみ設定できます。

IP LSA の詳細については、次の URL の『*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
コマンド構文については、次の URL 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/ps6441/products_command_reference_book09186a008049739b.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.30-1）
- 「IP SLA 動作の設定」（P.30-5）
- 「IP SLA 動作のモニタリング」（P.30-7）

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 サーバなどのリモート 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、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）、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。

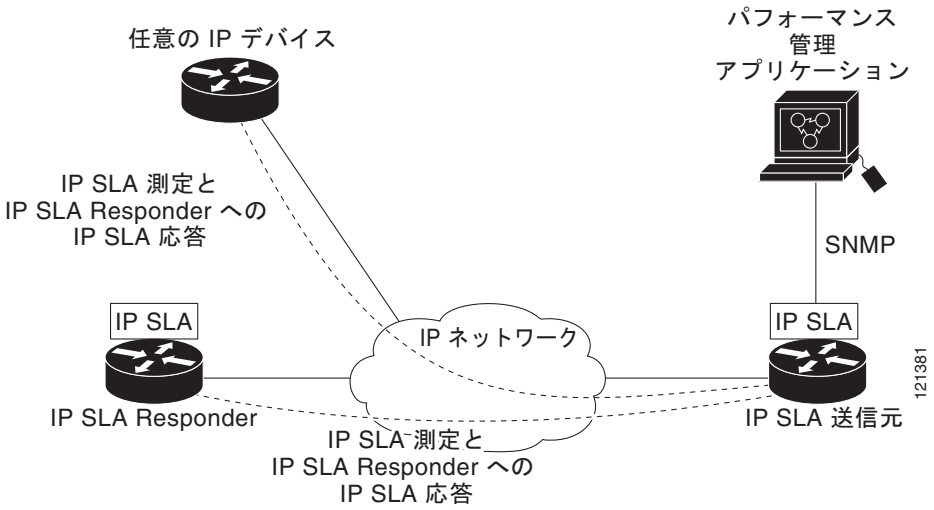
- 「Cisco IOS IP SLA によるネットワーク パフォーマンスの測定」（P.30-2）
- 「IP SLA Responder と IP SLA コントロール プロトコル」（P.30-3）
- 「IP SLA の応答時間の計算」（P.30-4）

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 30-1 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 30-1　　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

（注） スイッチでは、DLSw+ 動作を使用した VoIP サービス レベル分析または IP サービス レベル分析はサポートしません。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 responder には Cisco IOS Layer 2 responder 設定可能スイッチが使用できます。たとえば、Catalys 2960 や Cisco ME 2400 スイッチなどです。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 30-1 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。

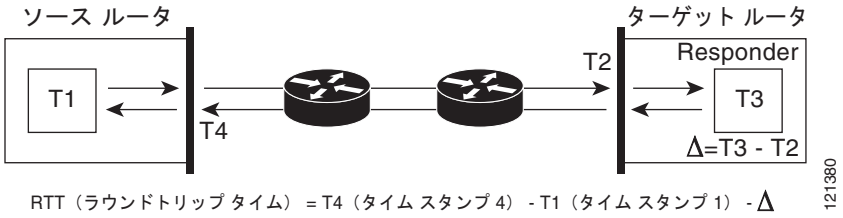
IP SLA の応答時間の計算

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 30-2 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。

図 30-2　　Cisco IOS IP SLA responder タイム スタンプ



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッタ、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。この内容に含まれるのは responder の設定手順および responder のサポートのみ含む Catalyst 2960 スイッチです。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.30-5）
- 「設定時の注意事項」（P.30-5）
- 「IP SLA Responder の設定」（P.30-6）

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 ULR の『*Cisco IOS IP SLAs Command Reference, 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

詳しい説明と設定手順については、次の URL の『*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 responder は、Catalyst 2960 や Cisco ME 2400 スイッチなど、レイヤ 2 スイッチを含む Cisco IOS ソフトウェアベース デバイスでのみ利用可能です。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** *ip-address* **port** *port-number*	スイッチを IP SlA 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** *ip-address* : 宛先 IP アドレスを入力します。 • **port** *port-number* : 宛先ポート番号を入力します。 （注）　IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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 または Catalyst 3560 のような 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 30-1 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 30-1　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。



CHAPTER 31

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のみです。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 policy map 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.31-1）
- 「自動 QoS の設定」（P.31-19）
- 「自動 QoS 情報の表示」（P.31-29）
- 「標準 QoS の設定」（P.31-29）
- 「標準 QoS 情報の表示」（P.31-70）

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 31-1 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 2 ISL 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 2 CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

- レイヤ 3 パケットのプライオリティ ビット

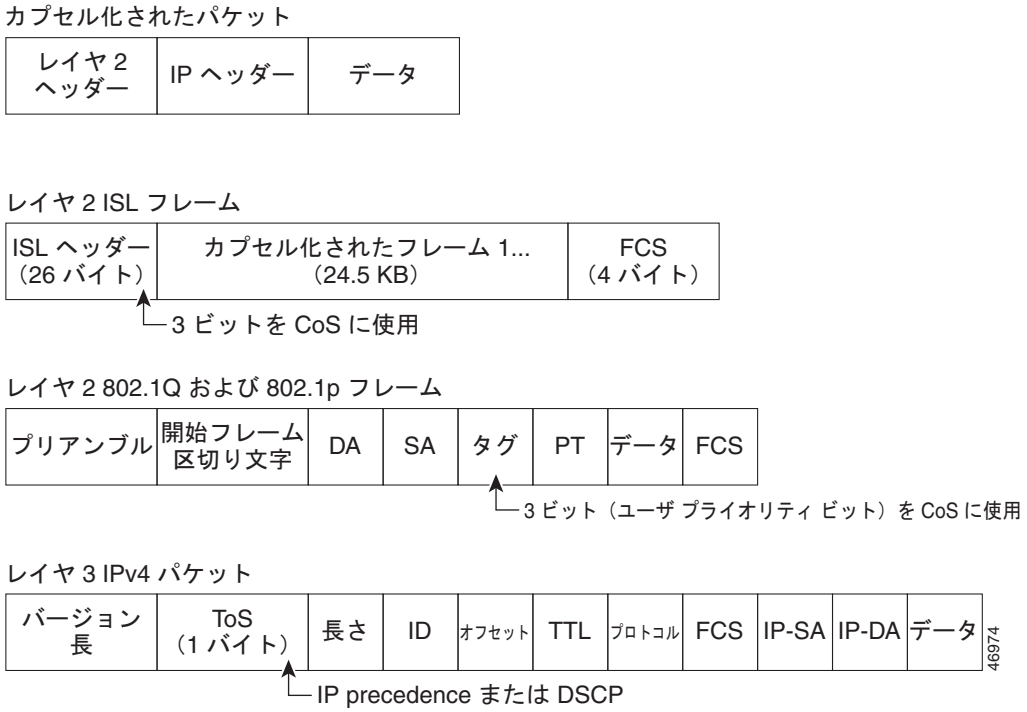
  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP）値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

  IP precedence 値の範囲は 0 ～ 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 31-1　　フレームおよびパケットにおける QoS 分類レイヤ



インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの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）。

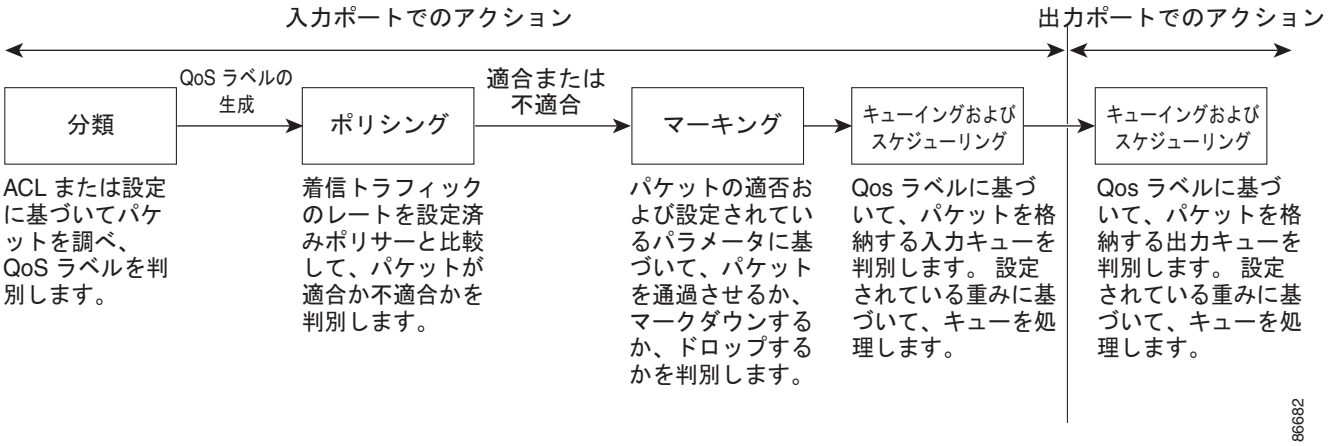
図 31-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- 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.31-5）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.31-8）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.31-8）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.31-11）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.31-12）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.31-11）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 31-2　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 31-3（P.31-7）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 31-3 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 MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

IP トラフィックには、次の分類オプションを使用できます（図 31-3 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。

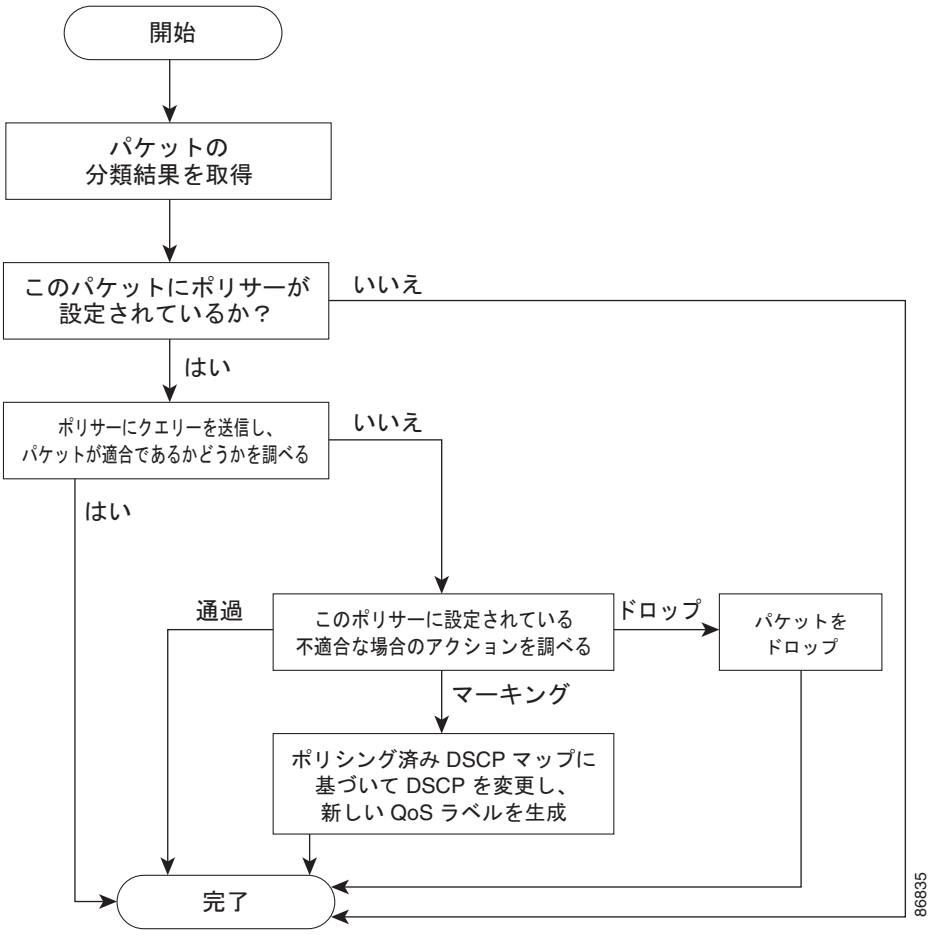
- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。

- 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.31-10）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.31-34）を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 31-3　分類フローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。QoS のコンテキストでは、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。

（注）　アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義したあとで、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.31-40）を参照してください。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。パケットをクラス マップ条件と照合したあとで、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.31-8）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.31-40）を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てたあとで、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 31-4 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.31-10）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。

QoS は物理ポートのみに設定できます。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.31-9）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.31-46）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.31-50）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。

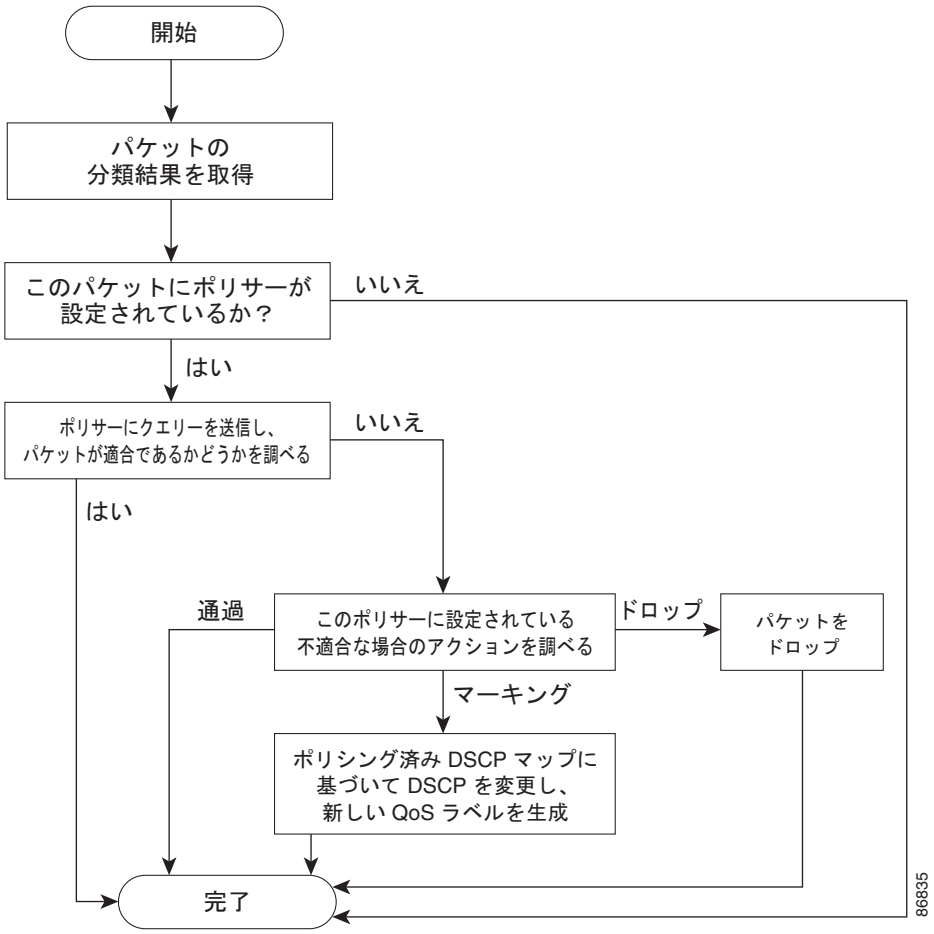
バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

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 31-4 に、ポリシングおよびマーキングのプロセスを示します。

図 31-4　物理ポートのポリシングおよびマーキング フローチャート



マッピング テーブル

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

  DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。このマップを設定するには、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用します。

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといいます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用してキューを選択します。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。

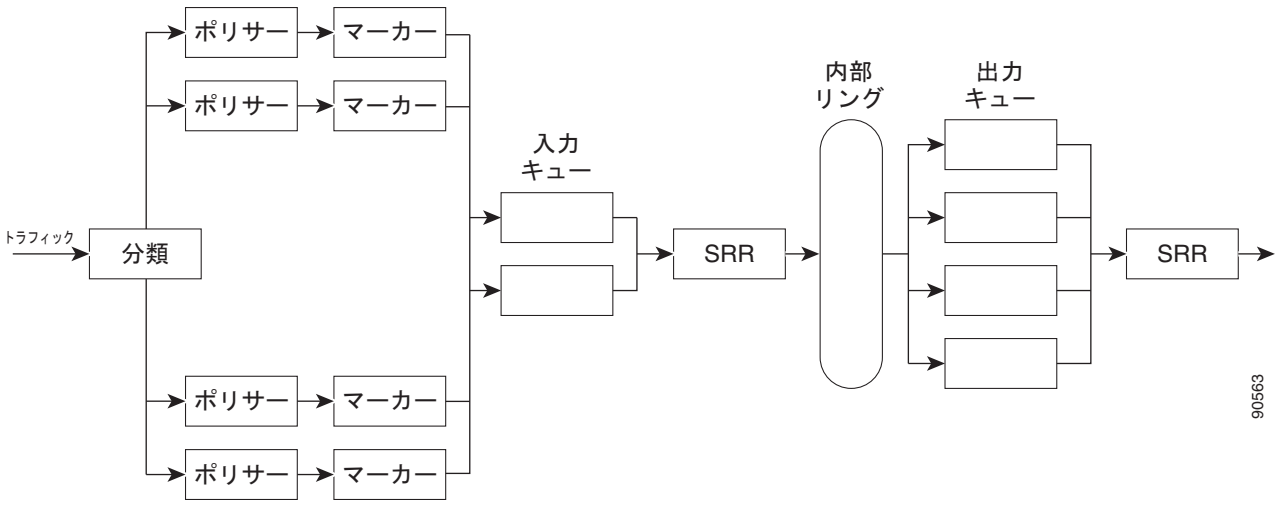
設定情報については、「DSCP マップの設定」（P.31-53）を参照してください。

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.31-13）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.31-16）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 31-5 を参照）。

図 31-5　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

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。

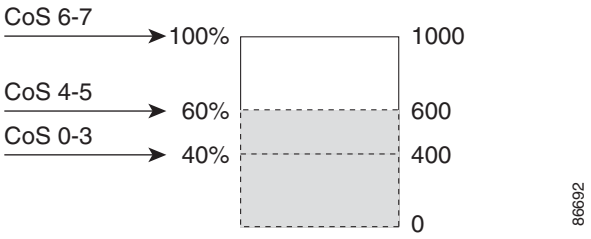
フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームは廃棄されます。

図 31-6 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。

図 31-6　WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」（P.31-59）、「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.31-63）、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.31-65）を参照してください。

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットが 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。

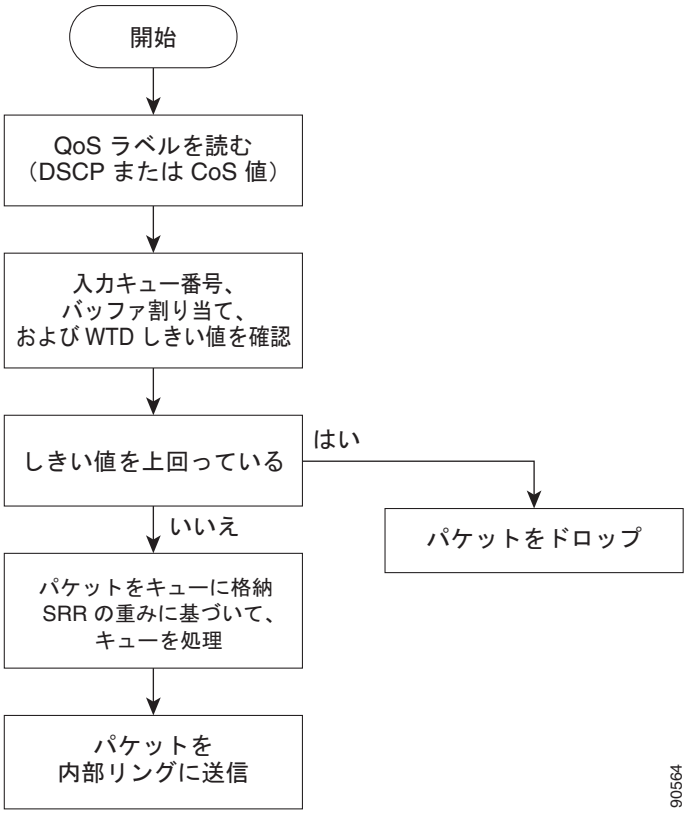
共有モードでは、各キューは設定された重みに従って帯域幅を共有します。帯域幅に対してはこのレベルが保証されますが、このレベルに限定されるわけではありません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。

詳細については、「入力キュー間の帯域幅の割り当て」（P.31-61）、「出力キューでの SRR シェーピング重みの設定」（P.31-66）、および「出力キューでの SRR 共有重みの設定」（P.31-67）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 31-7 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 31-7　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 31-1 にこれらのキューの説明を示します。

表 31-1　入力キューのタイプ

キュー タイプ [1]	機能
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 qos srr-queue input threshold**、**mls qos srr-queue input dscp-map**、および **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用できます。
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.31-12）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。

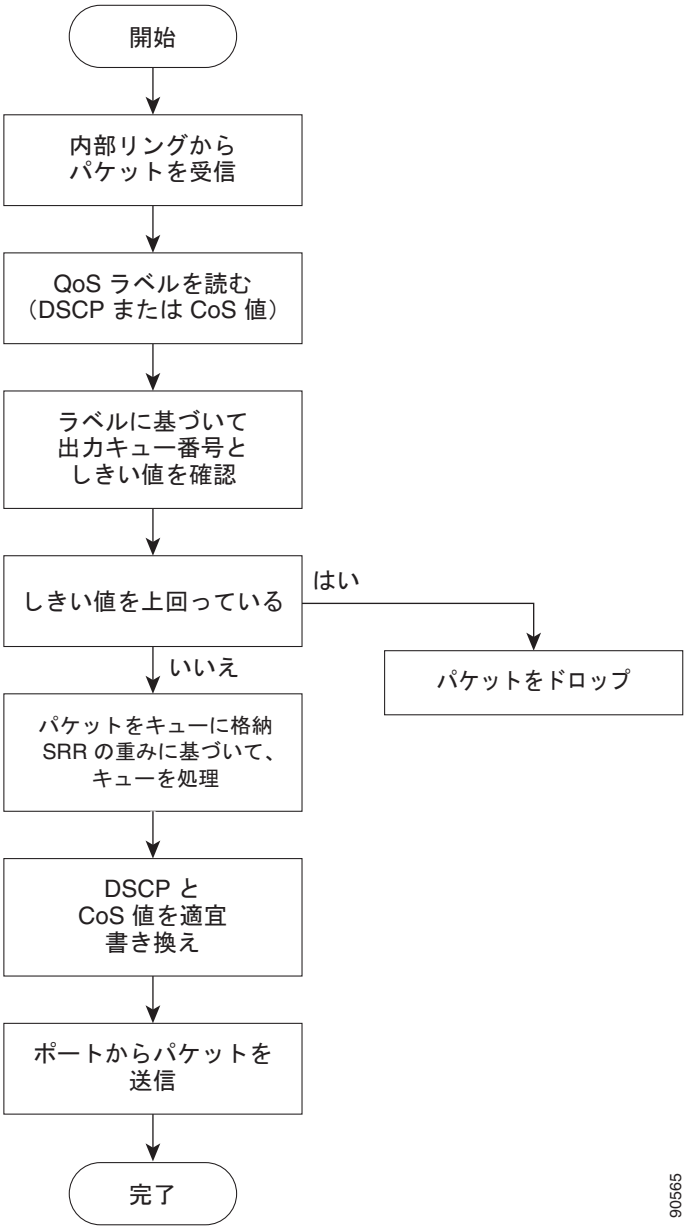
ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットが廃棄されるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定情報については、「入力キューの特性の設定」（P.31-58）を参照してください。

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 31-8 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。

（注）　緊急キューがイネーブルの場合、SRR によって空になるまで処理されてから、他の 3 つのキューが処理されます。

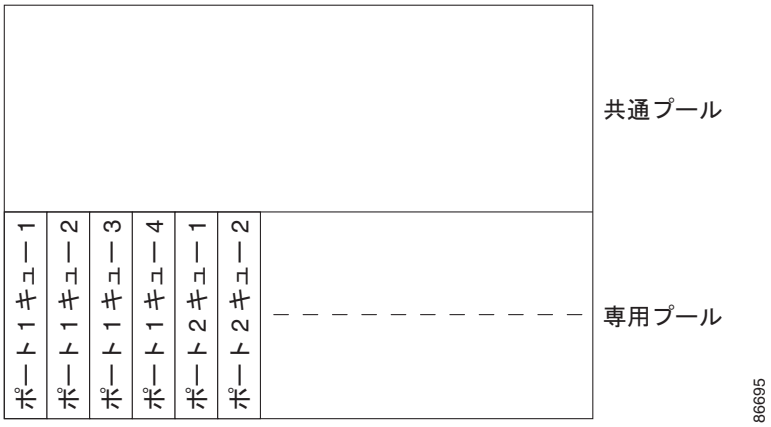
図 31-8　出力ポートのキューイングおよびスケジューリング フローチャート



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に割り当てられます。スイッチに存在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 31-9 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 31-9　　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 ステートに設定されていて、変更できません。WTD の仕組みの詳細については、「WTD」（P.31-12）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。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。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.31-12）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.31-62）を参照してください。

（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。

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

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.31-20）
- 「コンフィギュレーションにおける自動 QoS の影響」（P.31-24）
- 「自動 QoS 設定時の注意事項」（P.31-24）
- 「VoIP 用自動 QoS のイネーブル化」（P.31-25）
- 「自動 QoS 設定例」（P.31-27）

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 31-2 を参照）。

表 31-2　トラフィック タイプ、パケット ラベル、キュー

	VoIP[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（キュー 2）					0、1（キュー 1）	
CoS/出力キュー マップ	5（キュー 1）	3、6、7（キュー 2）			4（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. VoIP = Voice over IP

表 31-3 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 31-3　入力キューの自動 QoS 設定

入力キュー	キュー番号	CoS/キュー マップ	キュー重み（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0, 1	81%	67%
プライオリティ	2	2, 3, 4, 5, 6, 7	19%	33%

表 31-4 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 31-4　出力キューの自動 QoS 設定

出力キュー	キュー番号	CoS/キュー マップ	キュー重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ	1	5	最大 100%	16%	10%
SRR 共有	2	3, 6, 7	10%	6%	10%
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 31-3 および表 31-4 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 31-3 および表 31-4 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 31-3 および表 31-4 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.31-36）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 31-5 にリストされているコマンドをポートに適用します。

表 31-5　生成される自動 QoS 設定

説明	自動的に生成されるコマンド
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を設定します。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**

表 31-5　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 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 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
スイッチが自動的に入力キューを設定します。キュー 2 がプライオリティ キューでキュー 1 が共有モードです。また、スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**

表 31-5　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**
auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。	Switch(config)# **mls qos map policed-dscp 24 26 46 to 0** Switch(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** Switch(config-cmap)# **match ip dscp ef** Switch(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** Switch(config-cmap)# **match ip dscp cs3 af31** Switch(config)# **policy-map AutoQoS-Police-SoftPhone** Switch(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** Switch(config-pmap-c)# **set dscp ef** Switch(config-pmap-c)# **police 320000 8000 exceed-action policed-dscp-transmit** Switch(config-pmap)# **class AutoQoS-VoIP-Control-Trust** Switch(config-pmap-c)# **set dscp cs3** Switch(config-pmap-c)# **police 32000 8000 exceed-action policed-dscp-transmit**
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。	Switch(config-if)# **service-policy input AutoQoS-Police-SoftPhone**

表 31-5　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-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。	witch(config)# **mls qos map policed-dscp 24 26 46 to 0** Switch(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** Switch(config-cmap)# **match ip dscp ef** Switch(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** Switch(config-cmap)# **match ip dscp cs3 af31** Switch(config)# **policy-map AutoQoS-Police-CiscoPhone** Switch(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** Switch(config-pmap-c)# **set dscp ef** Switch(config-pmap-c)# **police 320000 8000 exceed-action policed-dscp-transmit** Switch(config-pmap)# **class AutoQoS-VoIP-Control-Trust** Switch(config-pmap-c)# **set dscp cs3** Switch(config-pmap-c)# **police 32000 8000 exceed-action policed-dscp-transmit**
クラス マップとポリシー マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-CiscoPhone*）を、Cisco 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。

（注）　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 **auto qos 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ていた場合（Cisco IOS Release 12.2(37)SE 以前）、Cisco IOS Release 12.2(40)SE で新規導入された自動 QoS 生成コマンドはポートに適用されません。このコマンドを自動的に適用するには、ポートの設定を一度削除してから再びポートに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.31-24）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。

	コマンド	目的
ステップ 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**}	自動 QoS をイネーブルにします。 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 31-10 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 31-10　ネットワークでの自動 QoS の設定例

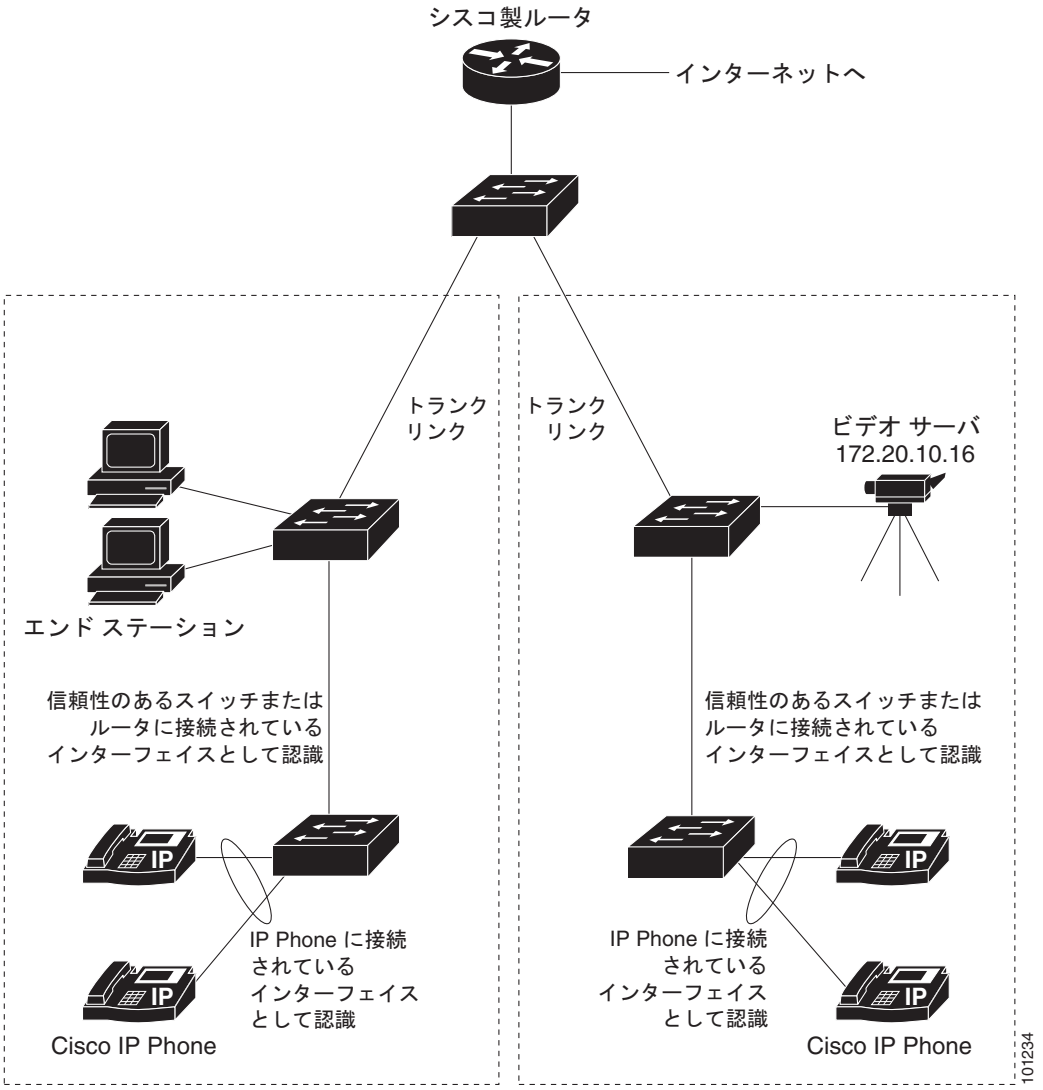


図 31-10 に、VoIP トラフィックを他のすべてのトラフィックに優先するネットワークを示します。QoS ドメインの端にあるワイヤリング クローゼットのスイッチで、自動 QoS がイネーブルとなっています。

（注）　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 31-10 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.31-29）
- 「標準 QoS 設定時の注意事項」（P.31-32）
- 「QoS のグローバルなイネーブル化」（P.31-33）（必須）
- 「ポートの信頼状態による分類の設定」（P.31-34）（必須）
- 「QoS ポリシーの設定」（P.31-40）（必須）
- 「DSCP マップの設定」（P.31-53）（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.31-58）（任意）
- 「出力キューの特性の設定」（P.31-62）（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.31-30）および「出力キューのデフォルト設定」（P.31-31）を参照してください。

入力キューのデフォルト設定

表 31-6 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 31-6　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 [1]	4	4
プライオリティ キューの帯域幅 [2]	0	10
WTD ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみパケットを送信します。
2. キュー 2 はプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 31-7 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 31-7　デフォルトの CoS 入力キューしきい値マップ

CoS 値	キュー ID- しきい値 ID
0–4	1–1
5	2–1
6, 7	1–1

表 31-8 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 31-8　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 31-9 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 31-9　出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
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 31-10 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 31-10　デフォルトの CoS 出力キューしきい値マップ

CoS 値	キュー ID- しきい値 ID
0, 1	2–1
2, 3	3–1
4	4–1
5	1–1
6, 7	4–1

表 31-11 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 31-11　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 31-12（P.31-53）のとおりです。

デフォルトの IP precedence/DSCP マップは、表 31-13（P.31-54）のとおりです。

デフォルトの DSCP/CoS マップは、表 31-14（P.31-56）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.31-32）
- 「ポリシングの注意事項」（P.31-32）
- 「一般的な QoS の注意事項」（P.31-33）

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。入力サービス ポリシー マップに ACL の信頼ステートメントが含まれている場合、利用可能な QoS TCAM に収めるにはアクセスリストが大きすぎる可能性があり、ポリシー マップをポートに適用する際にエラーが発生する場合もあります。可能な限り、QoS ACL の行数を最小限に抑えてください。

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のみです。VLAN と Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）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.31-29）、「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.31-13）、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.31-16）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 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

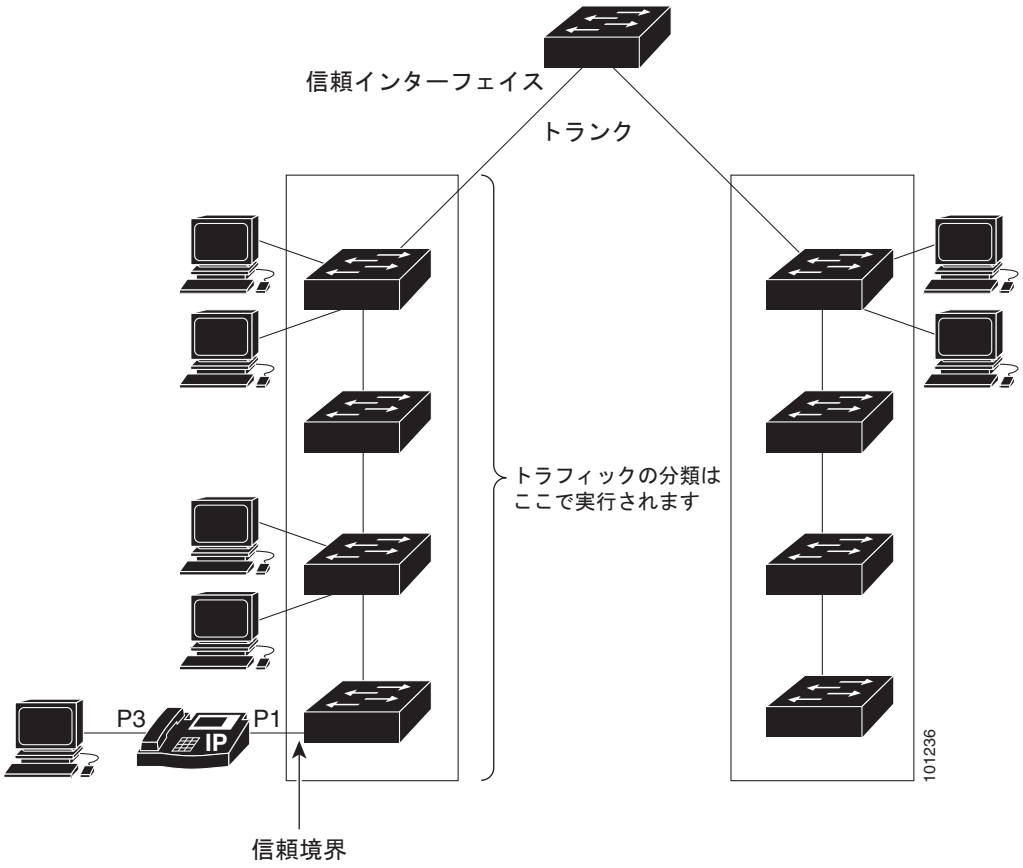
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「QoS ポリシーの設定」（P.31-40）に記載されている作業を 1 つまたは複数実行する必要があります。

- 「QoS ドメイン内のポートの信頼状態の設定」（P.31-34）
- 「インターフェイスの CoS 値の設定」（P.31-36）
- 「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.31-36）
- 「DSCP 透過モードのイネーブル化」（P.31-38）
- 「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.31-38）

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 31-11 に、ネットワーク トポロジの例を示します。

図 31-11　QoS ドメイン内のポートの信頼状態



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。
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.31-36）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.31-53）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** {*default-cos* | **override**}	デフォルトのポート CoS 値を設定します。 • *default-cos* 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

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して（図 31-11（P.31-34）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。

信頼境界機能をポート上で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**	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** または **mls qos trust dscp**	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	**mls qos trust device cisco-phone**	Cisco IP Phone が信頼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。

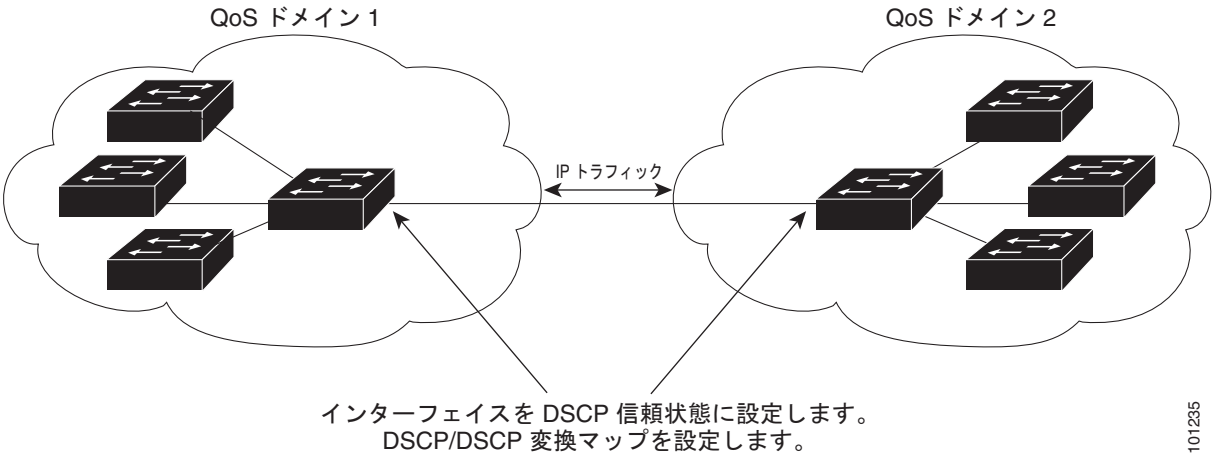
no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

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 31-12 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 31-12　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** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングする空のマップです。 • *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。 • *in-dscp* 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。 • *out-dscp* 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。
ステップ 4	**mls qos trust dscp**	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* 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.31-5）および「ポリシングおよびマーキング」（P.31-8）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.31-32）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.31-41）
- 「クラス マップによるトラフィックの分類」（P.31-44）
- 「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.31-46）
- 「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.31-50）

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 0.0.0.255
! (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.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。 • *dst-MAC-addr* 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）*type mask* 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。*type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致をテストする前に Ethertype に適用される *無視（don't care）* ビットを入力します。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
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.31-46）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 **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] または **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「ACL によるトラフィックの分類」（P.31-41）を参照してください。 **（注）** アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

	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。 • *class-map-name* 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	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name* 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** *ip-precedence-list* 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 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。
- Cisco IOS Release 12.2(25)SED 以降では、**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 コマンドを使用してパケット 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。
- Cisco IOS Release 12.2(40)SE 以降は、ポリシー マップとポート信頼状態の両方を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。

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 1	**configure terminal**	グローバル コ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。 • *class-map-name* 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。

	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.31-53）を参照してください。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* 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	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.31-32）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.31-55）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	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	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)# 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
```

- Cisco IOS Release 12.2(40)SE 以降は、ポリシー マップとポート信頼状態の両方を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。

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* **exceed-action** {**drop** | **policed-dscp-transmit**}	同じポリシー マップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」（P.31-32）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.31-55）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.31-44）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.31-46）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.31-46）を参照してください。
ステップ 6	**police aggregate** *aggregate-policer-name*	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 *aggregate-policer-name* 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。

	コマンド	目的
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。ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface 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.31-53）（任意）
- 「IP precedence/DSCP マップの設定」（P.31-54）（任意）
- 「ポリシング済み DSCP マップの設定」（P.31-55）（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.31-56）（任意）
- 「DSCP/DSCP 変換マップの設定」（P.31-57）（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 31-12 に、デフォルトの CoS/DSCP マップを示します。

表 31-12　デフォルトの CoS/DSCP マップ

CoS 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-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 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

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

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 31-13 に、デフォルトの IP precedence/DSCP マップを示します。

表 31-13　デフォルトの IP precedence/DSCP マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

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** *dscp1...dscp8*	IP precedence/DSCP マップを変更します。 *dscp1...dscp8* 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

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

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** *mark-down-dscp*	ポリシング済み DSCP マップを変更します。 • *dscp-list* 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。 • *mark-down-dscp* 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 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注）　このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

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 31-14 に、デフォルトの DSCP/CoS マップを示します。

表 31-14　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40–47	5
48–55	6
56–63	7

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。 • *dscp-list* 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 ～ 63、CoS の範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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# show mls qos maps dscp-cos
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    00 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

（注）　上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

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-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。 • *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。 • *in-dscp* 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。 • *out-dscp* 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** *dscp-mutation-name*	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* 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 qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface 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 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    00 00 00 00 00 00 00 00 10 10
      1 :    10 10 10 10 14 15 16 17 18 19
      2 :    20 20 20 23 24 25 26 27 28 29
      3 :    30 30 30 30 30 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

（注） 上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

入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。

- 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.31-59）（任意）
- 「入力キュー間のバッファ スペースの割り当て」（P.31-60）（任意）
- 「入力キュー間の帯域幅の割り当て」（P.31-61）（任意）

- 「入力プライオリティ キューの設定」（P.31-61）（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 dscp1...dscp8* または **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を入力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ～ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 • *queue-id* 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。 • *dscp1...dscp8* 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。 • *cos1...cos8* 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	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*	入力キューに 2 つの WTD しきい値の割合（しきい値 1 および 2 用）を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。 • *queue-id* 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 ～ 6 を、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 ～ 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 ～ 6）に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値（20 ～ 26）よりも先に廃棄されます。

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** *percentage1 percentage2*	入力キュー間にバッファを割り当てます。 デフォルトでは、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 *percentage1 percentage2* 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** または **show mls qos input-queue**	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）。 *weight1* および *weight2* 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.31-61）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** または **show mls qos input-queue**	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** または **show mls qos input-queue**	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 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.31-63）
- 「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.31-63）（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.31-65）（任意）
- 「出力キューでの SRR シェーピング重みの設定」（P.31-66）（任意）
- 「出力キューでの SRR 共有重みの設定」（P.31-67）（任意）
- 「出力緊急キューの設定」（P.31-68）（任意）
- 「出力インターフェイスの帯域幅の制限」（P.31-69）（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。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** *qset-id* **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。 • *qset-id* 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。
ステップ 3	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*	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。 • *qset-id* 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。 • *drop-threshold1 drop-threshold2* 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。 *qset-id* 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。

	コマンド	目的
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
Switch(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 dscp1...dscp8* または **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ～ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ～ 39 および 48 ～ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ～ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 • *queue-id* に指定できる範囲は、1 ～ 4 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。 • *dscp1...dscp8* 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。 • *cos1...cos8* 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。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 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.31-12）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.31-67）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 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 *weight1 weight2 weight3 weight4* 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 ～ 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 weight2 weight3 weight4*	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 *weight1 weight2 weight3 weight4* 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 ～ 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

Cisco IOS Release 12.1(19)EA1 から、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パケットより高くできます。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。

	コマンド	目的
ステップ 3	**interface** *interface-id*	出力ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**priority-queue out**	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、*srr-queue bandwidth shape* または **srr-queue bandwidth share** コマンドの **weight1** が無視されます（比率計算に使用されません）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
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。

	コマンド	目的
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 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 31-15 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 31-15　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 [*interface-id*] [**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。
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 **（注）** 着信トラフィックの分類情報を表示する場合は、**show policy-map interface** 特権 EXEC コマンドを使用しないでください。**control-plane** および **interface** キーワードはサポートされていません。表示される統計情報は無視してください。
show running-config | include rewrite	透過的な DSCP 設定を表示します。



CHAPTER 32

IPv6 ホスト機能の設定

Internet Protocol（IP; インターネット プロトコル）バージョン 6（IPv6）は、TCP/IP プロトコル スイートで IP バージョン 4（IPv4）の代わりに使用されるネットワークレイヤ IP です。この章では、Catalyst 2960 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 33 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 および 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）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。「SDM テンプレート」（P.32-6）を参照してください。

（注） 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.32-1）
- 「IPv6 の設定」（P.32-8）
- 「IPv6 の表示」（P.32-11）

IPv6 の概要

IPv6 を使用する主な目的は、ユーザ数および一意なグローバル IP アドレスを必要とするアプリケーションの急激な増加に対応できるように、インターネット グローバル アドレス スペースを拡張することです。IPv4 は 32 ビット アドレスを使用して、約 40 億の使用可能アドレスを提供します。これらのアドレスの大部分は政府機関や大規模な組織に割り当てられていて、使用可能な IP アドレス数が急速に減少しています。IPv6 は 128 ビットの送信元および宛先アドレスを使用しているため、グローバルに一意な IP アドレスを IPv4 よりもはるかに多く提供できます。

IPv6 のアーキテクチャを使用すると、既存の IPv4 ユーザは IPv6 に簡単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、QoS（Quality Of Service）、グローバルに一意なアドレスなどのサービスを利用できます。IPv6 アドレス スペースは柔軟であるため、プライベート アドレスの必要性が減少し、ネットワーク エッジ上の境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を使用する必要がなくなります。IPv6 では、より新しいユニキャスト方式が採用されています。IP アドレスに 16 進値が導入され、デリミタとしてピリオド（.）でなくコロン（:）が使用されます。

IPv6 には、IPv4 と比べて次の利点もあります。

- アドレスの管理および委任が容易
- *ステートレス自動設定*（Dynamic Host Configuration Protocol [DHCP] と似ているが、指定された DHCP アプリケーションまたはサーバが不要）によるアドレス自動設定が容易
- IPSec（暗号化セキュリティ）内蔵
- モバイル デバイス向けに最適化されたルーティング
- Duplicate Address Detection（DAD）機能

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//warp/public/732/Tech/ipv6/

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.32-2）
- 「サポート対象の IPv6 ユニキャスト ルーティング機能」（P.32-3）
- 「SDM テンプレート」（P.32-6）

IPv6 アドレス

IPv6 はユニキャスト（1 対 1）、マルチキャスト（1 対多）、およびエニキャスト（1 対最近接）の 3 つのアドレス タイプをサポートします。マルチキャスト アドレスは、ブロードキャスト アドレスの代わりに使用されます。スイッチがサポートするのは、IPv6 ユニキャスト アドレスのみです。このリリースでは、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（x:x:x:x:x:x:x:x 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、次の URL にある『Cisco IOS IPv6 Configuration Library』の「Implementing Addressing and Basic Connectivity」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00807fcf4b.html

「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 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル（RFC 2460）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.32-3）
- 「ICMPv6」（P.32-4）
- 「近接ディスカバリ」（P.32-4）
- 「IPv6 のステートレス自動設定および重複アドレス検出」（P.32-5）
- 「IPv6 アプリケーション」（P.32-5）
- 「デュアル IPv4/IPv6 プロトコル スタック」（P.32-6）

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャスト アドレスをサポートします（RFC 2373）。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 Universal 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（1111 1110 10）およびインターフェイス ID を使用します。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。

次の URL にある『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章の、「IPv6 Unicast Addresses」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00807fcf4b.html

各 IPv6 ホスト インターフェイスは、ハードウェア内で最大 3 つのアドレスをサポートできます（集約可能なグローバル ユニキャスト アドレスを 1 つ、リンクに対してローカルなユニキャスト アドレスを 1 つ、およびプライバシ アドレスをゼロ個以上）。

IPv6 用 DNS

IPv6 には、Domain Name System（DNS; ドメイン ネーム システム）の名前/アドレスおよびアドレス/名前の検索プロセスをサポートする新しい DNS レコード タイプが導入されています。新しい 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）（RFC 2463）機能は、IPv4 と同じです。ICMP は ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。IPv6 では、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。基本的な IPv6 パケット ヘッダーの Next Header フィールド値が 58 の場合は、IPv6 ICMP パケットであることを意味します。

近接ディスカバリ

スイッチは、IPv6 対応の Neighbor Discovery Protocol（NDP）（RFC 2461、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 Static Neighbor Discovery もサポートします。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。

ICMP パケット ヘッダーの Type フィールド値が 135 の場合は、ネイバ送信請求メッセージであることを意味します。ノードが同じローカル リンク上の別のノードのリンクレイヤ アドレスを判別する必要がある場合は、ローカル リンク上でこれらのメッセージが送信されます。ネイバ送信請求メッセージを受信した宛先ノードは、ICMP パケット ヘッダーの Type フィールド値が 136 のネイバ アドバタイズメント メッセージを送信して、応答します。

ICMP パケット ヘッダーの Type フィールド値が 137 の場合は、IPv6 ネイバ リダイレクト メッセージであることを意味します。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（RFC 2463）をサポートしています。マスク長が 64 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。宛先へのパス上にさらに適した先頭ホップ ノードが存在することをホストに通知する場合、ルータはネイバ リダイレクト メッセージを送信します。ルータがネイバ リダイレクト メッセージを受信しても、ルーティング テーブルは更新されず、ホストはネイバ リダイレクト メッセージを送信しません。

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 CPU によってアクティブに解決されている同じネイバである場合、そのようなパケットが追加されると、スイッチはハードウェアで廃棄を実行します。この廃棄を実行することで、CPU に余分な負荷がかからないようになり、IPv6 ルーテッド環境においてスイッチ CPU を効率よく利用できるようになります。

IPv6 のステートレス自動設定および重複アドレス検出

IPv6 は 2 つのタイプの自動設定をサポートします。

- ステートレス自動設定（RFC 2462）：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。
- ステートフル自動設定：DHCP バージョン 6 を使用します。

スイッチではステートレス自動設定がサポートされているため、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ことができます。

IPv6 ノードのすべてのインターフェイスには、インターフェイス ID（ルータの MAC アドレス）およびリンクに対してローカルなプレフィクス FE80::/10 に基づいて自動設定された、リンクに対してローカルなアドレスが必要です。リンクに対してローカルなアドレスを使用すると、ノードとリンク上のその他のノードとの通信が可能になり、ノードをさらに設定することができます。手動設定を行ったり、DHCP サーバなどのサーバを利用したりしなくても、ノードをネットワークに接続して、グローバルな IPv6 アドレスを自動的に生成することができます。IPv6 の場合、リンク上のルータはルータ アドバタイズメント メッセージを使用して、グローバル プレフィクス、およびリンクのデフォルト ルータとして動作するための機能をアドバタイズします。リンク上のノードがグローバル IPv6 アドレスの自動設定できるようにするには、ルータ アドバタイズメント メッセージ内のプレフィクス（64 ビット）にインターフェイス ID（64 ビット）を付加します。

ノードによって設定された 128 ビット IPv6 アドレスには、リンク上で一意であることを確認するための重複アドレス検出（RFC 2462）が実行されます。アドバタイズされたプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスはグローバルに一意であることが保証されます。システムが起動すると、ホストから、ICMP パケット ヘッダーの Type フィールド値が 133 であるルータ送信請求メッセージが送信されます。これにより、スケジューリングされた次のルータ アドバタイズメント メッセージを待機しなくても、ホストを即座に自動設定することができます。IPv6 重複アドレス検出は、ユニキャスト アドレスがインターフェイスに割り当てられる前に実行されます。自動生成された、サイトに対してローカルな IPv6 アドレスは、スイッチではサポートされません。

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

Cisco IOS を使用したこれらのアプリケーションの管理の詳細については、次の URL にある『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00807fcf4b.html

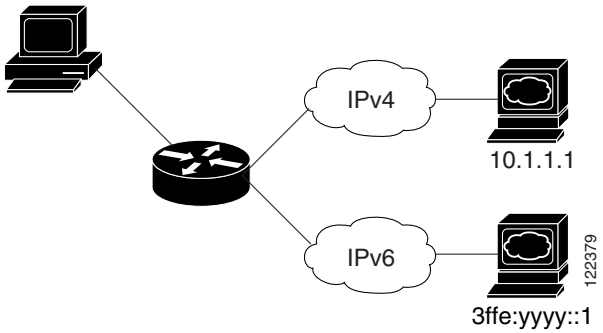
デュアル IPv4/IPv6 プロトコル スタック

IPv6 に移行する方法の 1 つは、デュアル IPv4/IPv6 プロトコル スタックを使用することです。デュアル スタックを使用すると、ノードで稼動中のアプリケーションに緩やかな段階的アップグレードを行うことができます。IPv6 にアップグレードされたアプリケーションは、IPv6 プロトコル スタックを使用します。アップグレードされていない、IPv4 のみをサポートするアプリケーションと、アップグレード済みアプリケーションを、同じノード上で共存させることができます。新規のアップグレード済みアプリケーションは、IPv4 と IPv6 の両方のプロトコル スタックを使用できます。

Cisco IOS ソフトウェアは、デュアル IPv4/IPv6 プロトコル スタック方式をサポートしています。IPv4 および IPv6 ルーティングがイネーブル化されていて、インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、インターフェイスは IPv4 と IPv6 の両方のトラフィックを転送します。

図 32-1 に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 32-1　インターフェイス上での IPv4/IPv6 のデュアル サポート



スイッチは Ternary CAM（TCAM）を使用して、ユニキャスト ルート、MAC（メディア アクセス制御）アドレス、Access Control List（ACL; アクセス コントロール リスト）、およびその他の機能を格納します。また、スイッチの使用方法に応じてメモリ リソースを割り当てるための Switching Database Manager（SDM; スイッチング データベース マネージャ）テンプレートを備えています。IPv4 および IPv6 プロトコルの両方で 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。「SDM テンプレート」（P.32-6）を参照してください。

SDM テンプレート

ほとんどの Catalyst 2960 スイッチには、ユニキャスト ルート、MAC アドレス、ACL、および他の機能を格納するための TCAM が 1 つあります。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。スイッチ環境に最適なテンプレートを選択するには、**sdm prefer** 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。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。

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。

（注） 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、警告メッセージが生成されます。

- 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 および 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。

（注）　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。

デュアル IPv4/IPv6 SDM テンプレート

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

（注）　このリリースでは、IPv6 のマルチキャスト ルーティングまたは QoS はサポートされていません。このリリースは、IPv6 Multicast Listener Discovery（MLD）スヌーピングをサポートしています。

- デュアル IPv4 および IPv6 デフォルト SDM テンプレート：スイッチのレイヤ 2、QoS と IPv4 の ACL、および レイヤ 2 と IPv6 の ACL をサポート。

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

表 32-1 では、各新規テンプレートによって割り当てられた機能リソースの概数を示します。

表 32-1　各テンプレートが許容する機能リソースの概数

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 + マルチキャスト ルート	.25 K	.25 K	.25 K
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	.25 K
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	.25 K
IPv4 MAC セキュリティ ACE	384	128	.25 K
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

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.32-8）
- 「IPv6 ICMP レート制限の設定」（P.32-8）
- 「IPv6 のスタティック ルートの設定」（P.32-9）

IPv6 のデフォルト設定

表 32-2 に IPv6 のデフォルト設定を示します。

表 32-2　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 ICMP レート制限の設定

IPv6 ICMP レート制限ではトークン バケット アルゴリズムを使用して、IPv6 ICMP エラー メッセージをネットワークに送信する場合のレートを制限します。エラー メッセージの間隔は、タイム インターバルおよびバケット サイズで指定します。traceroute など一部のアプリケーションでは、一連の要求に対する応答を迅速かつ連続的に送信しなければならない場合があるため、エラー メッセージ間隔のみを指定した場合は、アプリケーションに障害が発生することがあります。トークン バケットを使用すると、エラー メッセージの送信能力をそれぞれ表す複数のトークンを仮想バケットに格納できます。メッセージを送信するたびに、バケットからトークンが 1 つ削除されます。一連のエラー メッセージが生成された場合は、バケットが空になるまでエラー メッセージを送信できます。バケットが空の場合は、新規トークンがバケットに格納されるまで、IPv6 ICMP エラー メッセージは送信されません。この方法ではレート制限間隔の平均値が大きくならずに、間隔が固定されている場合よりも柔軟性が高まります。

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。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • bucketsize：（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ipv6 interface** [*interface-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

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 ルートの利点は、セキュリティが高まり、リソースが効率化されることです。スタティック ルートではルートの計算や通信が不要であるため、ダイナミック ルーティング プロトコルよりも使用帯域幅が減少します。スタティック ルートの主な欠点は、ダイナミック ルーティングと異なり、自動的に更新されず、ネットワーク トポロジが変更された場合に手動再設定が必要なことです。スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートのタイプは、次のとおりです。

- 直接接続されたスタティック ルート：宛先は現在のインターフェイスに直接接続されていると想定されるため、出力インターフェイスのみを指定します。パケットの宛先は、ネクスト ホップ アドレスとして使用されます。直接接続されたスタティック ルートが有効なのは、指定したインターフェイスが IPv6 に対応していて、起動している場合のみです。
- 再帰スタティック ルート：ネクスト ホップのみを指定し、出力インターフェイスはネクスト ホップから取得します。再帰スタティック ルートが有効なのは、指定したネクスト ホップが有効な IPv6 出力インターフェイスであり、ルートが自己再帰型でなく、再帰深度が IPv6 転送の最大再帰深度を超えていない場合のみです。
- 完全指定のスタティック ルート：出力インターフェイスとネクスト ホップを両方とも指定します。ネクスト ホップは、指定した出力インターフェイスに直接接続されていると想定されます。完全指定のスタティック ルートが有効なのは、指定した IPv6 インターフェイスが IPv6 に対応していて、起動している場合のみです。
- フローティング スタティック ルート：上記の 3 つのスタティック ルート タイプはいずれも、フローティング スタティック ルートに設定できます。このルートは、設定済みのルーティング プロトコルを介して取得されたダイナミック ルートのバックアップに使用されます。フローティング スタティック ルートに設定された管理ディスタンスは、バックアップしているルーティング プロトコルよりも非効率的です。したがって、トラフィックのルーティングには常に、フローティング スタティック ルートでなくダイナミック ルートが使用されます。ダイナミック ルートが失われた場合は、フローティング スタティック ルートが代わりに使用されます。

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。 • *ipv6-prefix :* 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。 • *ipv6-address*：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 RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進形式で指定）で設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** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**] または **show ipv6 route static** [*updated*]	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、次の URL 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。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00807fcf4b.html

IPv6 の表示

表 32-3 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 32-3　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。

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: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```



CHAPTER 33

IPv6 MLD スヌーピングの設定

Catalyst 2960 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 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。

（注） 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 コマンドで行います。

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。

（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.33-1）
- 「IPv6 MLD スヌーピングの設定」（P.33-5）
- 「MLD スヌーピング情報の表示」（P.33-11）

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。

（注）　スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 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.33-2）
- 「MLD クエリー」（P.33-3）
- 「マルチキャスト クライアント エージングの堅牢性」（P.33-3）
- 「マルチキャスト ルータ検出」（P.33-3）
- 「MLD レポート」（P.33-4）
- 「MLD Done メッセージおよび即時脱退」（P.33-4）
- 「TCN 処理」（P.33-5）

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、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して、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるよう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。IP v 6 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ついて説明します。

- 「MLD スヌーピングのデフォルト設定」（P.33-5）
- 「MLD スヌーピング設定時の注意事項」（P.33-6）
- 「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.33-6）
- 「スタティックなマルチキャスト グループの設定」（P.33-8）
- 「マルチキャスト ルータ ポートの設定」（P.33-8）
- 「MLD 即時脱退のイネーブル化」（P.33-9）
- 「MLD スヌーピング クエリーの設定」（P.33-10）
- 「MLD リスナー メッセージ抑制のディセーブル化」（P.33-11）

MLD スヌーピングのデフォルト設定

表 33-1 に、MLD スヌーピングのデフォルト設定を示します。

表 33-1　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

表 33-1　MLD スヌーピングのデフォルト設定 （続き）

機能	デフォルト設定
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル：1000（1 秒）、VLAN：0 （注）　VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2.
MLD リスナー抑制	イネーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** 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、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して、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるよう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。
- スイッチで保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチ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、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して、Catalyst 2960 スイッチが VLAN 上のクエリーを受信できるよう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。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバー 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** *vlan-id* **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。

（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。

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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID、およびマルチキャスト ルータにインターフェイスを指定します。 • 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-id*]	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。
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 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** *vlan-id* **immediate-leave**	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
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** *value*	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value*	（任意）VLAN 単位で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。
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count*	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。
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** *vlan-id* **last-listener-query-interval** *interval*	（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 tcn 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** *count*	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。
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 33-2 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 33-2　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** *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 querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意）**vlan** *vlan-id* 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。
show ipv6 mld snooping multicast-address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	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 *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。



CHAPTER 34

EtherChannel およびリンクステート トラッキングの設定

この章では Catalyst 2960 スイッチのレイヤ 2 ポート上で EtherChannel を設定する方法について説明します。EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用すると、ワイヤリング クローゼットおよびデータ センタ間の帯域幅を拡張できます。EtherChannel はネットワーク上でボトルネックの発生が見込まれるところに、任意に配置できます。EtherChannel は、他のリンクに負荷を再分散させることによって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャネル内の他のリンクにトラフィックをリダイレクトします。この章では、リンクステート トラッキングを設定する方法についても説明します。

（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。

- 「EtherChannel の概要」（P.34-1）
- 「EtherChannel の設定」（P.34-8）
- 「EtherChannel、PAgP、および LACP ステータスの表示」（P.34-17）
- 「リンクステート トラッキングの概要」（P.34-18）
- 「リンクステート トラッキングの設定」（P.34-20）

EtherChannel の概要

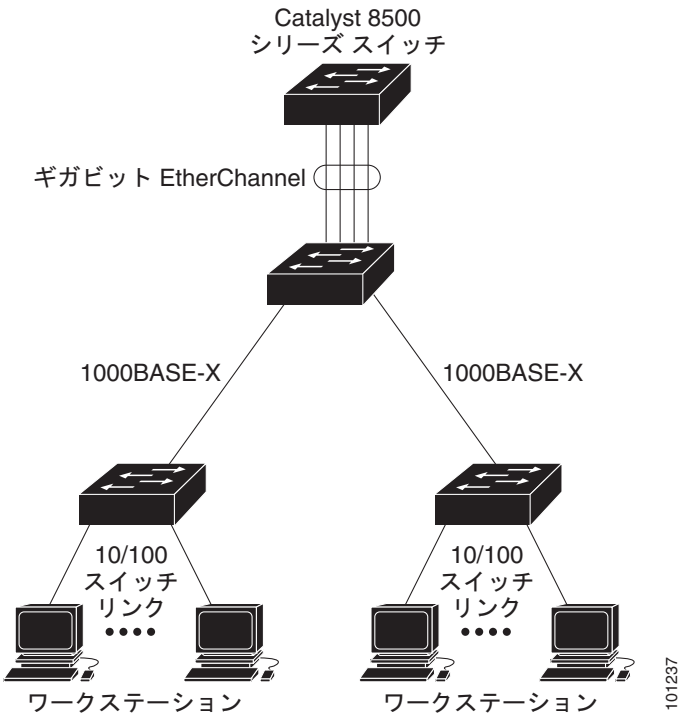
ここでは、EtherChannel の仕組みについて説明します。

- 「EtherChannel の概要」（P.34-2）
- 「ポートチャネル インターフェイス」（P.34-3）
- 「ポート集約プロトコル」（P.34-4）
- 「LACP」（P.34-5）
- 「EtherChannel の On モード」（P.34-6）
- 「ロードバランシングおよび転送方式」（P.34-6）

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 34-1 を参照）。

図 34-1　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.34-9）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 suspended ステートになります。Cisco IOS Release 12.2(35)SE より、ローカルポートはサスペンド ステートではなく独立ステートになり、他の単一リンクのようにデータ トラフィックに伝送し続けます。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。

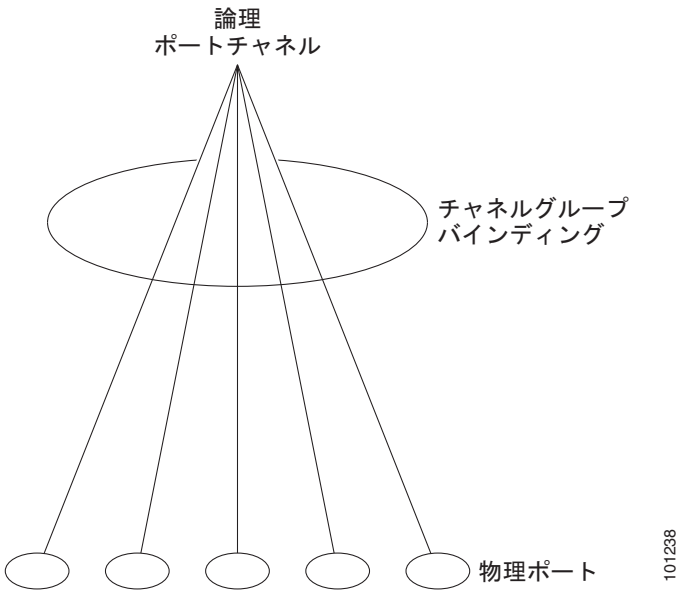
ポートチャネル インターフェイス

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 34-2 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。

図 34-2　　物理ポート、論理ポートチャネル、およびチャネル グループの関係



EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用した設定変更は、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 34-1 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 34-1　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 34-2 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 34-2　EtherChannel LACP モード

モード	説明
アクティブ	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive LACP** モードでは、どちらの場合も、ポートは相手ポートとのネゴシエーションにより、ポート速度、レイヤ 2 EtherChannel の場合はトランキング ステートおよび VLAN 番号などの条件に基づいて、EtherChannel を形成できるかどうかを判別できます。

LACP モードが異なっていても、モード間で互換性があるかぎり、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 の On モード

EtherChannel の **on** モードは、EtherChannel の手動設定に使用します。**on** モードを使用すると、ポートはネゴシエーションせずに強制的に EtherChannel に参加します。リモート デバイスが PAgP や LACP をサポートしていない場合にこの **on** モードが役立ちます。**on** モードでは、リンクの両端のスイッチが **on** モードに設定されている場合のみ EtherChannel を使用できます。

同じチャネル グループの **on** モードで設定されたポートは、速度やデュプレックスのようなポート特性に互換性を持たせる必要があります。**on** モードで設定されていたとしても、互換性のないポートは suspended ステートになります。

注意　**on** モード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。

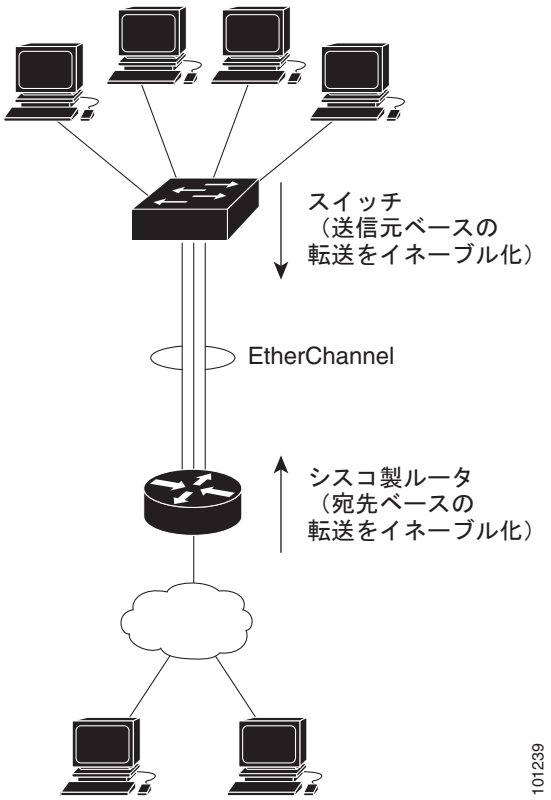
宛先 IP アドレスベース転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。したがって、ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、異なるチャネル ポートに送信できます。ただし、異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常に同じチャネル ポートで送信されます。

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 34-3 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 デバイスなので、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチがルータ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。

図 34-3　負荷の分散および転送方式



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.34-9）
- 「EtherChannel 設定時の注意事項」（P.34-9）
- 「レイヤ 2 EtherChannel の設定」（P.34-10）（必須）
- 「EtherChannel ロードバランシングの設定」（P.34-13）（任意）
- 「PAgP 学習方式およびプライオリティの設定」（P.34-14）（任意）
- 「LACP ホット スタンバイ ポートの設定」（P.34-15）（任意）

（注）　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.34-9）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 34-3 に、EtherChannel のデフォルト設定を示します。

表 34-3　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	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*	すべてのポートをスタティックアクセス ポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセス ポートとして設定する場合は、ポートを 1 つの VLAN にのみ割り当ててください。指定できる範囲は 1 ～ 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。 *channel-group-number* の範囲は 1 ～ 6 です。 **mode** には、次のキーワードのいずれか 1 つを選択します。 • **auto**：PAgP デバイスが検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。 • **desirable**：PAgP を無条件でイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • **on**：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。**on** モードの場合、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.34-4）および「LACP モード」（P.34-5）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、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、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.34-6）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
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	EtherChannel のロードバランシング方式を設定します。 デフォルトは **src-mac** です。 次のいずれかの負荷分散方式を選択します。 • **dst-ip**：宛先ホスト 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。 • **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	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show etherchannel load-balance**	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のみ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。

Catalyst 2960 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.34-13）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。 *priority* 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** または **show pagp** *channel-group-number* **internal**	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.34-16）および「LACP ポート プライオリティの設定」（P.34-16）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。 *priority* 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** または **show lacp sys-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。

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な値に変更して、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** ***priority***	LACP ポート プライオリティを設定します。 *priority* に指定できる範囲は 1 ～ 65535 です。デフォルト値は 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** または **show lacp** [*channel-group-number*] **internal**	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。

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

EtherChannel、PAgP、および LACP ステータス情報を表示するには、表 34-4 に記載された特権 EXEC コマンドを使用します。

表 34-4　EtherChannel、PAgP、および LACP ステータスを表示するためのコマンド

コマンド	説明
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロードバランシング方式またはフレーム配布方式、ポート、ポートチャネル、プロトコルの情報も表示されます。
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 PAgP 設定、近接情報などの PAgP 情報が表示されます。
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	トラフィック情報、内部 LACP 設定、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

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。

図 34-4（P.34-20）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。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。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 34-4 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。

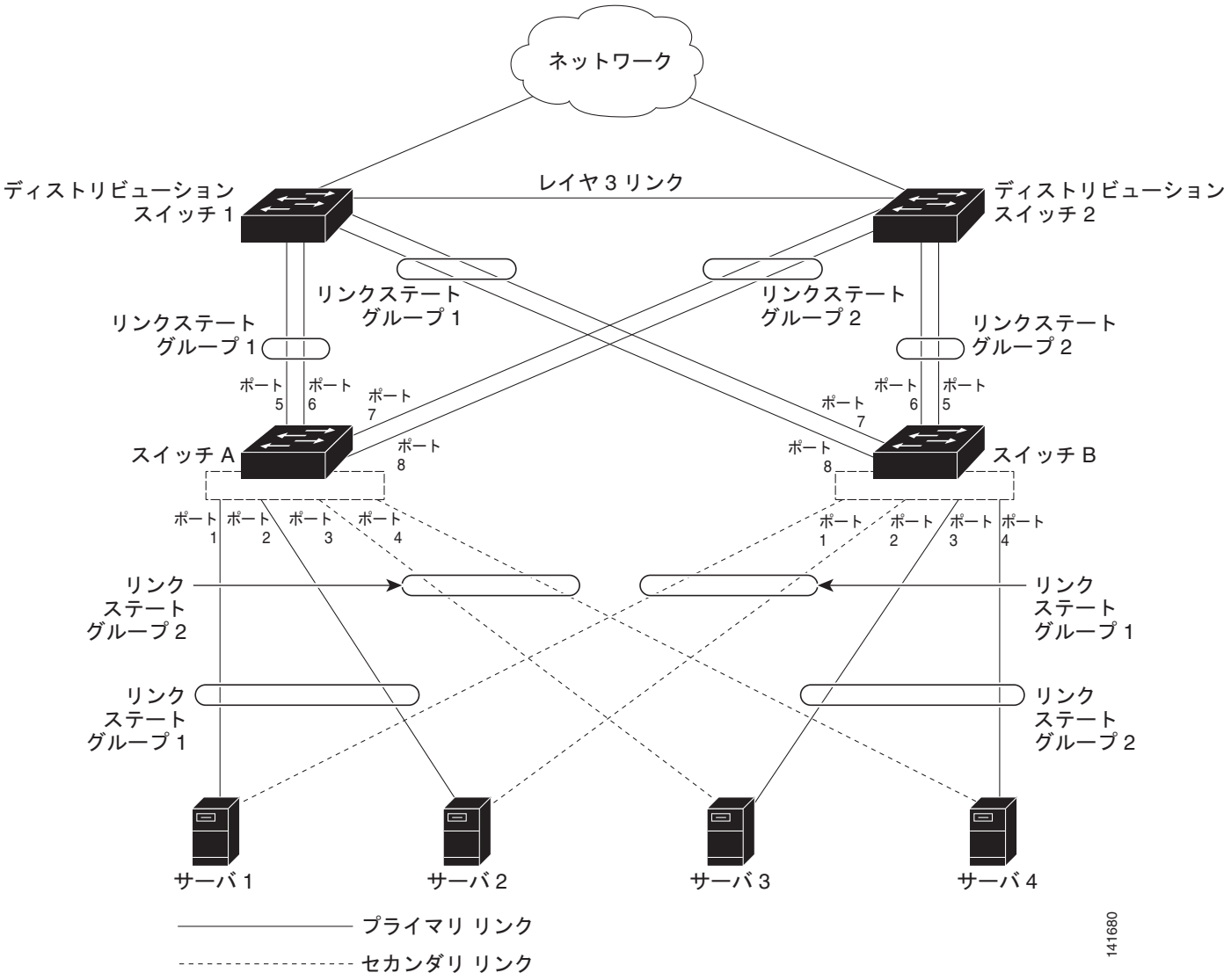
分散スイッチやルータに障害が発生したり、ケーブルが切断されたり、リンクが失われたために、リンクステート グループ内でアップストリーム ポートが利用不能や接続不能になる場合があります。これらは、リンクステート トラッキングがイネーブルの際の、ダウンストリーム インターフェイスとアップストリーム インターフェイス間の相互作用です。

- 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 34-4（P.34-20）を参照してください。ポート 6 のアップストリーム リンクが切断されても、ダウンストリーム ポート 1 および 2 のリンク ステートは変わりません。ただし、アップストリーム ポート 5 のリンクも切断された場合、ダウンストリーム ポートのリンク ステートがリンクダウン ステートに変更されます。サーバ 1 およびサーバ 2 の接続については、リンクステート グループ 1 からリンクステート グループ 2 へ変更します。ダウンストリーム ポート 3 およびダウンストリーム ポート 4 は、リンクグループ 2 であるためステートを変更しません。
- リンクステート グループが設定されている場合、リンクステート トラッキングはディセーブルで、アップストリーム インターフェイスが切断され、ダウンストリーム インターフェイスのリンク ステートは変更されないままになります。サーバはこのアップストリーム接続が切断されたことを認識せず、セカンダリ インターフェイスにフェールオーバーしません。

障害のあるダウンストリーム ポートをリンクステート グループから削除することで、ダウンストリーム インターフェイスのリンクダウン状態から復旧できます。複数のダウンストリーム インターフェイスを復旧させるには、リンクステート グループをディセーブルにします。

図 34-4　一般的なリンクステート トラッキングの設定



リンクステート トラッキングの設定

ここでは、リンクステート トラッキング ポートの設定について説明します。

- 「デフォルトのリンクステート トラッキングの設定」（P.34-21）
- 「リンクステート トラッキングの設定時の注意事項」（P.34-21）
- 「リンクステート トラッキングの設定」（P.34-21）
- 「リンクステート トラッキング ステータスの表示」（P.34-22）

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** [*number*] {**upstream** | **downstream**}	リンクステート グループを指定し、グループ内のインターフェイスを **upstream** または **downstream** インターフェイスに設定します。グループ番号は 1 ～ 2 に設定できます。デフォルトは 1 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
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
Switch(config-if)# interface gigabitethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

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 : Gi0/15(Dwn) Gi0/16(Dwn) Gi0/17(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(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。



CHAPTER 35

トラブルシューティング

この章では、Cisco IOS ソフトウェアに関連する、Catalyst 2960 スイッチの問題点を特定し、解決する方法について説明します。問題の性質に応じて、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.35-2）
- 「パスワードを忘れた場合の回復」（P.35-3）
- 「コマンド スイッチで障害が発生した場合の回復」（P.35-7）
- 「クラスタ メンバー スイッチとの接続の回復」（P.35-11）

（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.35-11）
- 「SFP モジュールのセキュリティと識別」（P.35-12）
- 「SFP モジュール ステータスのモニタリング」（P.35-12）
- 「ping の使用」（P.35-12）
- 「レイヤ 2 traceroute の使用」（P.35-14）
- 「IP traceroute の使用」（P.35-15）
- 「TDR の使用」（P.35-17）
- 「debug コマンドの使用」（P.35-18）
- 「show platform forward コマンドの使用」（P.35-20）
- 「crashinfo ファイルの使用」（P.35-21）

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。

```
switch% tar -tvf image_filename.tar
```

2. **tar -xvf** <*image_filename.tar*> <*image_filename.bin*>UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

```
switch% tar -xvf image_filename.tar image_filename.bin
x c2960-lanbase-mz.122-25FX/c2960-lanbase-mz.122-25.FX.bin, 2928176 bytes, 5720
tape blocks
```

3. **ls -l** <*image_filename.bin*> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

```
switch% ls -l image_filename.bin
-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、電源コードをスイッチに再接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、**Mode** ボタンを離します。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.35-4）
- 「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.35-6）

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　スイッチの電源を切ります。

ステップ 4　電源コードをスイッチに再接続してから 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.35-4）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.35-6）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  -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)?
```

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]: 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。

（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 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。

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。

（注）　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.35-8）
- 「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.35-9）

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]: 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 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、**Retur**n 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]: 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。

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。

（注）　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.35-13）
- 「ping の実行」（P.35-13）

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。

（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 35-1 で、ping の文字出力について説明します。

表 35-1　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。

表 35-1　ping の出力表示文字 （続き）

文字	説明
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは **Ctrl+^ X**）を入力してください。**Ctrl** キー、**Shift** キー、および **6** キーを同時に押してから離し、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.35-14）
- 「使用上のガイドライン」（P.35-14）
- 「物理パスの表示」（P.35-15）

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.35-14）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 22 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.35-15）
- 「IP traceroute の実行」（P.35-16）

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。

（注）　**traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに **traceroute** を実行する例を示します。

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
```

```
Switch#
```

ディスプレイには、送信される 3 つのプローブごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 35-2　traceroute の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	ソース クエンチ
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは **Ctrl+^ X**）を入力してください。**Ctrl** キー、**Shift** キー、および **6** キーを同時に押してから離し、そのあと **X** キーを押します。

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.35-17）
- 「TDR の実行および結果の表示」（P.35-18）

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.35-18）
- 「システム全体診断のイネーブル化」（P.35-19）
- 「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.35-19）

注意　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。

（注）　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。

（注）　デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。コンソールでメッセージ ロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージ ロギングを行うと、オーバーヘッドが小さくなります。Syslog サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージ ロギングの詳細については、第 27 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:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050002_00020002-00_00000000_00000000     00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

=========================================
Egress:Asic 2, switch 1
Output Packets:

-----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/1    0005 0001.0001.0001  0002.0002.0002

-----------------------------------------
Packet 2
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0002.0002.0002

-----------------------------------------
<output truncated>
-----------------------------------------
Packet 10
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi0/2
```

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   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    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：Cisco IOS Release 12.2(25)SEC 以降では、システムに障害が発生すると、スイッチが自動的にこのファイルを作成します。

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、およびスタック トレースです。**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

Cisco IOS Release 12.2(25)SEC 以降では、システムに障害が発生すると、スイッチが拡張 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。



APPENDIX A

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 MIB（Management Information Base; 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）

MIB の一覧

- 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-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-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO IP-STAT-MIB
- CISCO-LAG-MIB

- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-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
- 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）
- INET-ADDRESS-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.htmlMIB およびシスコ製品の情報には、シスコの Web サイトよりアクセスできます。URL は次のとおりです。
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。

（注）　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。



APPENDIX 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

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-1）
- 「コンフィギュレーション ファイルの操作」（P.B-8）
- 「ソフトウェア イメージの操作」（P.B-23）

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）
- 「デフォルト ファイル システムの設定」（P.B-3）
- 「ファイル システムのファイルに関する情報の表示」（P.B-3）
- 「ディレクトリの作成および削除」（P.B-4）
- 「ファイルのコピー」（P.B-4）
- 「ファイルの削除」（P.B-5）
- 「tar ファイルの作成、表示、および抽出」（P.B-5）

- 「ファイルの内容の表示」（P.B-7）

使用可能なファイル システムの表示

スイッチで使用可能なファイル システムを表示するには、**show file systems** 特権 EXEC コマンドを使用します（次の例を参照）。

```
Switch# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags   Prefixes
*   15998976     5135872     flash     rw   flash:
           -           -    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	値
Size（b）	ファイル システムのメモリ サイズ（バイト単位）です。
Free（b）	ファイル システムの空きメモリ サイズ（バイト単位）です。
Type	ファイル システムのタイプです。 **flash**：ファイル システムはフラッシュ メモリ デバイス用です。 **nvram**：ファイル システムは NVRAM（不揮発性 RAM）デバイス用です。 **opaque**：ファイル システムはローカルに生成された *pseudo* ファイル システム（*system* など）、または brimux などのダウンロード インターフェイスです。 **unknown**：ファイル システムのタイプは不明です。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取り / 書き込みです。 **wo**：書き込み専用です。
Prefixes	ファイル システムのエイリアスです。 **flash:** ：フラッシュ ファイル システムです。 **nvram:** ：NVRAM です。 **null:** ：コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。 **rcp:** ：Remote Copy Protocol（RCP）ネットワーク サーバです。 **system:** ：実行コンフィギュレーションを含むシステム メモリが格納されています。 **tftp:** ：TFTP ネットワーク サーバです。 **xmodem:** ：XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。 **ymodem:** ：YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。

デフォルト 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 *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。
ステップ 2	**cd new_configs**	目的のディレクトリに変更します。 コマンド例では、*new_configs* という名前のディレクトリに変更する方法を示します。
ステップ 3	**pwd**	作業ディレクトリを表示します。

ディレクトリの作成および削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。
ステップ 2	**mkdir old_configs**	新しいディレクトリを作成します。 コマンド例では、*old_configs* という名前のディレクトリの作成方法を示します。 ディレクトリ名では大文字と小文字が区別されます。 スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	**dir** *filesystem***:**	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。

注意　ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy** *source-url destination-url* 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドを実行すると、現在の実行コンフィギュレーション ファイルがフラッシュ メモリの NVRAM セクションに保存され、システム初期化中のコンフィギュレーションとして使用されます。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイル システム（**xmodem:**、**ymodem:**）を指定し、そこからコピーすることもできます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、**tftp:** などがあります。構文は次のとおりです。

- FTP（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-8）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-23）を参照してください。

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

*filesystem***:** オプションを省略すると、**cd** コマンドで指定したデフォルトのデバイスが使用されます。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

ファイルを削除しようとすると、削除の確認を求めるプロンプトが表示されます。

注意　ファイルが削除された場合、その内容は回復できません。

次に、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Switch# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次のセクションを参照）。

（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。

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:c2960-lanbase-mz.122-25.FX.tar
info (219 bytes)
```

```
c2960-lanbase-mz.122-25.FX/ (directory)
c2960-lanbase-mz.122-25.FX/html/ (directory)
c2960-lanbase-mz.122-25.FX/html/foo.html (0 bytes)
c2960-lanbase-mz.122-25.FX/c2960-lanbase-mz.122-25.FX.bin (4590080 bytes)
c2960-lanbase-mz.122-25.FX/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: c2960-lanbase-mz.12-25/html
c2960-lanbase-12-25.FX/html
c2960-lanbase-12-25.FX/html/ (directory)
c2960-lanbase-12-25.FX/html/const.htm (556 bytes)
c2960-lanbase-12-25.FX/html/xhome.htm (9373 bytes)
c2960-lanbase-12-25.FX/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:/*file-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
```

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-9）
- 「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-9）
- 「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-10）
- 「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-10）
- 「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-12）
- 「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-16）
- 「設定情報の消去」（P.B-19）
- 「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-19）

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要となるコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソール ポートから接続することを推奨します。コンソール ポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更によっては（スイッチの IP アドレスの変更やポートのディセーブル化など）、スイッチとの接続が切断される可能性があることにご注意ください。
- スイッチにパスワードが設定されていない場合は、**enable secret** *secret-password* グローバル コンフィギュレーション コマンドを使用して、パスワードを設定することを推奨します。

（注）　**copy** {**ftp: | rcp: | tftp:**} **system:running-config** 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力した場合と同様に、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成するには、コンフィギュレーション ファイルを直接スタートアップ コンフィギュレーションにコピーして（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-11）、「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-13）、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-17）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-10）
- 「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-11）
- 「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-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

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-10）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-10）を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 2　コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

ステップ 3　スイッチのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:**[[[*//location*]/*directory*]/*filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]/*directory*]/*filename*]

TFTP サーバにファイルがアップロードされます。

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- スイッチが作成した *username@switchname.domain* パスワード。変数 *username* は現在のセッションに関連付けられているユーザ名、*switchname* は設定されているホスト名、*domain* はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられてい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-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-13）
- 「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-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

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。
- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）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。

	コマンド	目的
ステップ 3	**configure terminal**	スイッチ上で、グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **system:running-config** または **copy ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] **nvram:startup-config**	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスイッチのスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-13）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy system:running-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*] または **copy nvram:startup-config ftp:**[[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定場所に格納します。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

リモート ホストとスイッチ間でコンフィギュレーション ファイルをダウンロード、アップロード、およびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけですみます （ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

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-16）
- 「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-17）
- 「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-18）

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-16）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** または **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次に、*host1-confg* という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
```

```
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.B-16）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:**[[[//[*username*@]*location*]/*directory*]/*filename*] または **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]	RCP を使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

次に、実行コンフィギュレーション ファイル *switch2-confg* を、IP アドレスが 172.16.101.101 であるリモート ホスト上のディレクトリ *netadmin1* にコピーする例を示します。

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
```

```
Connected to 172.16.101.101
Switch#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーションから設定情報を消去できます。スタートアップ コンフィギュレーションを使用しないでスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションを消去するには、**erase nvram:** または **erase startup-config** 特権 EXEC コマンドを使用します。

注意　削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、**delete flash:***filename* 特権 EXEC コマンドを使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、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。

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-20）
- 「設定時の注意事項」（P.B-21）
- 「コンフィギュレーション アーカイブの設定」（P.B-21）
- 「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-22）

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-20）
- 「コンフィギュレーションの交換」（P.B-20）
- 「コンフィギュレーションのロール バック」（P.B-21）

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 5 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）。

（注） 交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure replace コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、コンフィギュレーション ロールバックを行うときに大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**archive**	アーカイブコンフィギュレーション モードを開始します。
ステップ 3	**path** *url*	コンフィギュレーション アーカイブに、ファイルのディレクトリとファイル名プレフィクスを指定します。
ステップ 4	**maximum** *number*	（任意）コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を指定します。 *number*：コンフィギュレーション アーカイブでの実行コンフィギュレーション ファイルの最大数。有効な値は 1 ～ 14 で、デフォルトは 10 です。 **（注）** このコマンドを使用する前に **path** アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブのファイルのディレクトリとファイル名プレフィクスを指定しておく必要があります。
ステップ 5	**time-period** *minutes*	（任意）コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 *minutes*：コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブを自動保存する間隔を、分単位で指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

コンフィギュレーション交換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**archive config**	（任意）実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 **（注）** **path** アーカイブ コンフィギュレーション コマンドを入力してから、このコマンドを実行します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3		実行コンフィギュレーションに必要な変更を行います。
ステップ 4	**exit**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**]	実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換します。 *target-url :* 保存されているコンフィギュレーション ファイルの URL（ファイル システムからアクセス可能）。実行コンフィギュレーションと交換するファイルで、ステップ 2 で **archive config** 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなどです。 **list**：コンフィギュレーション交換動作のパスごとにソフトウェア パーサーによって適用されるコマンド エントリのリストを表示します。パスの合計数も表示されます。 **force**：実行コンフィギュレーション ファイルと指定した保存済みコンフィギュレーション ファイルの交換を確認なしで実行します。 **time** *seconds :* **configure confirm** コマンドを入力して実行コンフィギュレーション ファイルとの交換を確認するまでの時間を秒単位で指定します。指定時間内に **configure confirm** コマンドを入力しない場合、コンフィギュレーション交換動作が自動的に停止します （つまり、実行コンフィギュレーション ファイルは **configure replace** コマンドを入力する以前に存在していたコンフィギュレーションに保存されます）。 **（注）** **time** *seconds* コマンドライン オプションを使用する前に、コンフィギュレーション アーカイブをイネーブルにしておく必要があります。 **nolock**：コンフィギュレーション交換動作時に他のユーザが実行コンフィギュレーションを変更できないようにする実行コンフィギュレーション ファイルのロックをディセーブルにします。
ステップ 6	**configure confirm**	（任意）実行コンフィギュレーションと保存されているコンフィギュレーション ファイルとの交換を確認します。 **（注）** このコマンドは、**time** *seconds* キーワードと **configure replace** コマンドの引数が指定されている場合にだけ使用します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ソフトウェア イメージの操作

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフトウェアを格納するソフトウェア イメージ ファイルをアーカイブ（ダウンロードおよびアップロード）する方法を示します。

（注） ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

スイッチ ソフトウェアをアップグレードするには、TFTP、FTP、または RCP サーバからスイッチ イメージ ファイルをダウンロードします。TFTP サーバへアクセスできない場合、Web ブラウザ（HTTP）で PC またはワークステーションへ直接ソフトウェア イメージ ファイルをダウンロードします。次にデバイス マネージャまたは Cisco Network Assistant を使用してスイッチをアップグレードします。TFTP サーバまたは Web ブラウザ（HTTP）を使用したスイッチのアップグレードについては、リリース ノートを参照してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保存したりできます。

Cisco IOS Release 12.2(35)SE 以降では、**archive-download-sw /allow-feature-upgrade** 特権 EXEC コマンドを使用して、IP ベース イメージから IP サービス イメージへのアップグレードなど、別のフィーチャ セットを有するイメージをインストールすることができます。このリリース以降では、**boot auto-download-sw** 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、自動ソフトウェア アップグレードのイメージを取得するのに使用する URL を指定することができます。このコマンドを入力する際に、マスター スイッチではバージョン不一致の場合にこの URL を使用します。

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-24）
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」（P.B-25）
- 「TFTP によるイメージ ファイルのコピー」（P.B-25）
- 「FTP によるイメージ ファイルのコピー」（P.B-29）
- 「RCP によるイメージ ファイルのコピー」（P.B-34）

（注）　ソフトウェア イメージ、およびサポートされているアップグレード パスの一覧については、スイッチに付属のリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に *.bin* ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ（flash:）に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼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。Cisco IOS release 12.2(35)SE 以降では、**archive download-sw /directory** 特権 EXEC コマンドを使用してディレクトリを一度にひとつ指定できます。

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:c2960-lanbase-mz.122.25-FX
    image_family:C2960
    stacking_number:1.11
    info_end:

version_suffix:lanbase-122-25.FX
version_directory:c2960-lanbase-mz.122.25-FX
    image_system_type_id:0x00000000
    image_name:c2960-lanbase-mz.122.25-FX.bin
    ios_image_file_size:4413952
    total_image_file_size:4424192
    image_feature: LAYER_2|MIN_DRAM_MEG=64
    image_family:C2960
    stacking_number:1.11
    board_ids:0x00000034 0x00000042 0x00000037 0x00000041 0x0000003c
    info_end:
```

（注）　stacking_number フィールドは無視してください。このフィールドはスイッチに適用されません。

表 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。
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。

（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。

- 「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-26）
- 「TFTP によるイメージ ファイルのダウンロード」（P.B-27）
- 「TFTP によるイメージ ファイルのアップロード」（P.B-28）

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注）　/etc/inetd.conf および /etc/services ファイルを変更したあとに、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-26）を参照）。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 4	**archive download-sw/leave-old-sw/reload tftp:**[[*//location*]/*directory*]/*image-name*.**tar**	TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注）　フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼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-26）を参照）。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	現在稼動中のスイッチ イメージを TFTP サーバにアップロードします。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name*.**tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、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-29）
- 「FTP によるイメージ ファイルのダウンロード」（P.B-30）
- 「FTP によるイメージ ファイルのアップロード」（P.B-33）

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。

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-29）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	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name***.tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられてい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-29）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory/image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

	コマンド	目的
ステップ 8	**archive download-sw/leave-old-sw/reload ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]/*image-name***.tar**	FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられてい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-29）を参照してください。 • **@***location* には、FTP サーバの IP アドレスを指定します。 • *directory*/*image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼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
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-13）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	**archive upload-sw** **ftp:**[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*image-name***.tar**	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。 • *//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-29）を参照してください。 • *@location* には、FTP サーバの IP アドレスを指定します。 • */directory/image-name***.tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name***.tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされたあとに、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-34）
- 「RCP によるイメージ ファイルのダウンロード」（P.B-35）
- 「RCP によるイメージ ファイルのアップロード」（P.B-37）

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別の方法は、RCP を使用することです。コネクションレス プロトコルである UDP を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけですみます （ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スイッチのホスト名

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれるか、そこからコピーされます。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチとサーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。

  たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

  ```
  hostname Switch1
  ip rcmd remote-username User0
  ```

  このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

  ```
  Switch1.company.com Switch1
  ```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 6 の手順を実行します。現在のイメージを保存するには、ステップ 6 へ進みます。

	コマンド	目的
ステップ 1		「RCP によるイメージ 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、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。

	コマンド	目的
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive download-sw /overwrite /reload rcp:**[[[//[*username***@**]*location*]/*directory*]/*image-name***.tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。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-34）を参照してください。 • ***@****location* には、RCP サーバの IP アドレスを指定します。 • */directory/image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 7	**archive download-sw/leave-old-sw/reload rcp:**[[[//[*username***@**]*location*]/*directory*]/*image-name***.tar**]	RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。 • *//username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。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-34）を参照してください。 • ***@****location* には、RCP サーバの IP アドレスを指定します。 • */directory*]/*image-name***.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロード アルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注） フラッシュ デバイスに 2 つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、稼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。

注意 ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更*しないで*ください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。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-34）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive upload-sw rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	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。 • //*username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。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-34）を参照してください。 • @*location* には、RCP サーバの IP アドレスを指定します。 • /*directory*]/*image-name*.**tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • *image-name*.**tar** は、サーバ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。



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

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-5）

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。

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

Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）	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
	aaa processes *1-64*
	aaa route download *1-1440*
		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。
		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。
	cluster management-vlan *vlan-id*
	スイッチでクラスタが設定されている場合、このコマンドで管理 VLAN と通信します。
		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。
		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)# 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** *rate* 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。	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。 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。
	flowcontrol send {**desired** | **off** | **on**}
		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。
		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 31 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 （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
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*	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。 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。
	ip igmp snooping vlan *vlan-id* **static** *mac-address* **interface** *interface-id*
	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。
	ip igmp snooping source-only-learning [**age-timer** *value*]
	no ip igmp snooping mrouter learn pim v2
		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。
		`Switch(config)# ip igmp snooping vlan 1 static 0002.4b28.c482 interface gigabitethernet0/1`
		`^`
		`%Invalid input detected at '^' marker.`
		`Switch(config)# ip igmp snooping source-only-learning`
		`^`
		`%Invalid input detected at '^' marker.`
		`Switch(config)# no ip igmp snooping mrouter learn pim v2`
		`^`
		`%Invalid input detected at '^' marker.`

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; 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。
	mac-address *mac-address*
		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。
		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)# mac-address 0100.0ccc.cccc`
		`^`
		`%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 QoS 設定を削除して、Catalyst 2960 スイッチで新しく設定を作成することを推奨します。	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。

	auto-QoS は Catalyst 2950 スイッチではイネーブル化されませんが、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ドは、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.`

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
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。 **monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector-port** *interface-id*	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。 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.`

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 31 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。



APPENDIX D

Cisco IOS リリース 12.2(40)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 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 2960 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。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。

ACL

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ユーザ EXEC 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

組み込みイベントマネージャ

サポートされていない特権 EXEC コマンド

event manager update user policy [*policy-filename* | *group* [*group name expression*]] | *repository* [*url location*]

次のコマンドでは、パラメータがサポートされていません。

event manager run [*policy name*] |<paramater1>|... <**paramater15**>|

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 event manager directory user repository [*url location*]

event manager applet [*applet-name*] maxrun

アプレット コンフィギュレーション モードでサポートされていないコマンド

no event interface name [*interface-name*] parameter [*counter-name*] entry-val [*entry counter value*] entry-op {*gt*|*ge*|*eq*|*ne*|*lt*|*le*} [**entry-type {increment | rate | value**] [exit-val [*exit value*] exit-op {*gt*|*ge*|*eq*|*ne*|*lt*|*le*} **exit-type { increment | rate | value}**][**average-factor <average-factor-value>**]

no trigger

tag

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*

ip igmp helper-address *ip-address*

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 vlan

show mac address-table multicast

（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

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

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

snmp-server enable informs

snmp-server ifindex persist

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

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*}

（注）　このコマンドは、**vtp** グローバル コンフィギュレーション コマンドに置き換えられています。



INDEX

A

access-class コマンド 29-16
ACE
  IP 29-2
  QoS 31-7
  イーサネット 29-2
  定義 29-2
ACL
  ACE 29-2
  any キーワード 29-10
  host キーワード 29-10
  IP
    暗示のマスク 29-7
    暗黙の拒否 29-7, 29-12, 29-13
    一致条件 29-5
    作成 29-5
    フラグメントおよび QoS の注意事項 31-32
    未定義 29-17
  IPv4
    一致条件 29-5
    インターフェイスへの適用 29-17
    作成 29-5
    サポートされていない機能 29-5
    端末回線、設定 29-16
    名前付き 29-12
    番号 29-6
  MAC 拡張 29-20, 31-43
  QoS 31-7, 31-41
  QoS のためのトラフィックの分類 31-41
  一致 29-5, 29-17
  エントリの並べ替え 29-12
  拡張 IP、QoS 分類のための設定 31-42
  拡張 IPv4
    一致条件 29-5
    作成 29-8
  クラス マップごとの数 31-32
  コメント 29-15
  コンパイル 29-18
  サポート 1-8
  サポートされていない機能、IPv4 29-5
  時間範囲 29-14
  定義 29-1, 29-5
  適用
    QoS へ 31-7
    インターフェイスへの 29-17
    時間範囲 29-14
  名前付き、IPv4 29-12
  ハードウェアおよびソフトウェアの処理 29-17
  ハードウェアでのサポート 29-17
  標準 IP、QoS 分類のための設定 31-41
  標準 IPv4
    一致条件 29-5
    作成 29-7
  モニタ 29-22
  例 29-18, 31-41
ACL エントリの並べ替え 29-12
ACL での時間範囲 29-14
ACL の IP プロトコル 29-9
AC（コマンド スイッチ） 5-9
Address Resolution Protocol
  「ARP」を参照
ARP
  定義 1-5, 6-28
  テーブ
    アドレスの解決 6-28

管理 6-28
Auto-MDIX
設定 10-17
説明 10-17

B

BackboneFast
イネーブル化 17-14
サポート 1-6
説明 17-5
ディセーブル化 17-15
BPDU
errdisable ステート 17-2
RSTP フォーマット 16-13
フィルタリング 17-3
BPDU ガード
イネーブル化 17-11
サポート 1-6
説明 17-2
ディセーブル化 17-12
BPDU フィルタリング
イネーブル化 17-12
サポート 1-6
説明 17-3
ディセーブル化 17-13
Bridge Protocol Data Unit
「BPDU」を参照
broadcast storm-control コマンド 21-4

C

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-5
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
CA の信頼点
設定 8-40
定義 8-38
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 22-4
スイッチ 22-3
概要 22-1
更新 22-2
サポート 1-5
信頼境界 31-37
スイッチ クラスタの自動検出 5-5
設定 22-2
説明 22-1
送信タイマーおよびホールドタイム、設定 22-2
定義、LLDP を使用 23-1
デフォルト設定 22-2
モニタ 22-4
ルーティング デバイスでディセーブル化 22-3 ～ 22-4
CGMP
IGMP スヌーピング学習方式として 20-9
マルチキャスト グループへの加入 20-3
CipherSuites 8-39
Cisco 7960 IP Phone 14-1
Cisco Discovery Protocol
「CDP」を参照
Cisco IOS IP Service Level Agreements（SLA）responder 1-4
Cisco IOS IP SLA 30-1
Cisco IOS ファイル システム
「IFS」を参照
Cisco Network Assistant
「Network Assistant」を参照
CiscoWorks 2000 1-4, 28-4
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 5-14
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 1-4
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
CNS 1-4
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 1-4
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 4-8
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
config.text 3-12
configure terminal コマンド 10-6
config-vlan モード 2-2, 12-6
CoS
プライオリティの上書き 14-6
プライオリティを信頼する 14-6
レイヤ 2 フレーム 31-2
crashinfo ファイル 35-21
CWDM SFP 1-17

D

default コマンド 2-4
description コマンド 10-18
DHCP 19-12
Cisco IOS サーバ データベース
設定 19-11
イネーブル化
リレー エージェント 19-9
DHCP Option 82
回線 ID サブオプション 19-5
概要 19-3
設定時の注意事項 19-7
デフォルト設定 19-7
パケット形式、サブオプション
回線 ID 19-5
リモート ID 19-5
表示 19-12
リモート ID サブオプション 19-5
DHCP スヌーピング
Option 82 データ挿入 19-3
エッジ スイッチから信頼できないパケットを受信 19-3, 19-10
信頼できないインターフェイス 19-2
信頼できないメッセージ 19-2
信頼できるインターフェイス 19-2
設定時の注意事項 19-7
デフォルト設定 19-7
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 19-12
メッセージ交換プロセス 19-4

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 19-11
エージェントに関する統計情報をクリア 19-12
エントリ 19-5
削除
データベース エージェント 19-12
バインディング 19-12
バインディング ファイル 19-12
ステータスおよび統計情報の表示 19-12
設定 19-11
設定時の注意事項 19-8
説明 19-5
データベースの更新 19-12
デフォルト設定 19-7
バインディング 19-5
バインディング エントリ、表示 19-12
バインディングの追加 19-11
バインディング ファイル
形式 19-6
ロケーション 19-5
表示 19-12
リセット
タイムアウトの値 19-12
遅延時間の値 19-12
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 ベースの自動設定
BOOTP との関係 3-3
概要 3-3
クライアントのメッセージ交換要求 3-4
サポート 1-4
設定
DNS 3-6
TFTP サーバ 3-5
クライアント側 3-3
サーバ側 3-5
リレー デバイス 3-6
リース オプション
IP アドレス情報 3-5
コンフィギュレーション ファイルの受信 3-5
リレー サポート 1-4
例 3-8
Differentiated Services Code Point 31-2
Differentiated Services アーキテクチャ、QoS 31-2
DNS
DHCP ベースの自動設定 3-6
IPv6 32-4
概要 6-16
サポート 1-4
設定 6-17
設定の表示 6-18
デフォルト設定 6-17
Domain Name System
「DNS」を参照
DoS 攻撃 21-1
DSCP 1-9, 31-2
DSCP 透過 31-38
DTP 1-7, 12-15
dynamic auto トランキング モード 12-15
dynamic desirable トランキング モード 12-15
Dynamic Host Configuration Protocol
「DHCP ベースの自動設定」を参照
Dynamic Trunking Protocol
「DTP」を参照

E

ELIN ロケーション 23-3
errdisable ステート、BPDU 17-2
EtherChannel
IEEE 802.3ad、説明 34-5
LACP

システム プライオリティ 34-16
ステータスの表示 34-17
説明 34-5
他の機能との相互作用 34-6
ポート プライオリティ 34-16
ホット スタンバイ ポート 34-15
モード 34-5
PAgP
Catalyst 1900 との互換性 34-14
学習方式およびプライオリティの設定 34-14
サポート 1-3
集約ポート ラーナー 34-14
ステータスの表示 34-17
説明 34-4
他の機能との相互作用 34-5
モード 34-4
サポート 1-3
自動作成 34-4, 34-5
ステータスの表示 34-17
設定時の注意事項 34-9
説明 34-2
相互作用
STP 34-9
VLAN 34-10
チャネル グループ
数 34-3
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 34-3
デフォルト設定 34-9
転送方式 34-6, 34-13
ポート グループ 10-3
ポートチャネル インターフェイス
数 34-3
説明 34-3
レイヤ 2 インターフェイスの設定 34-10
ロードバランシング 34-6, 34-13
EtherChannel ガード
イネーブル化 17-15
説明 17-7
ディセーブル化 17-15
EUI 32-3
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 1-5
Flex Link
Link ロード バランシング 18-2
VLAN 18-2
VLAN ロード バランシングの設定 18-8
設定 18-6
設定時の注意事項 18-5
説明 18-1
デフォルト設定 18-4
モニタ 18-11
優先 VLAN の設定 18-9
Flex Link の VLAN ロード バランシング 18-2
設定時の注意事項 18-5
flowcontrol
設定 10-16
説明 10-16
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-33
サーバの準備 B-29
ダウンロード B-30
古いイメージの削除 B-32
コンフィギュレーション ファイル
アップロード B-15
概要 B-12
サーバの準備 B-13
ダウンロード B-13

G

get-bulk-request 動作 28-3
get-next-request 動作 28-3, 28-5
get-request 動作 28-3, 28-5
get-response 動作 28-3
GUI
「デバイス マネージャ」および「Network Assistant」を参照

H

Hello タイム
MSTP 16-23
STP 15-21
HP OpenView 1-4
HSRP
クラスタ スタンバイ グループに関する考慮事項 5-10
クラスタの自動復旧 5-11
「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 8-38
自己署名証明書 8-38
設定 8-41

I

ICMP
IPv6 32-4
time-exceeded メッセージ 35-16
traceroute 35-16
ICMP ping
概要 35-13
実行 35-13
ICMPv6 32-4
IDS 装置
入力 RSPAN 25-21
入力 SPAN 25-13
IEEE 802.1D
「STP」を参照
IEEE 802.1p 14-1
IEEE 802.1Q
カプセル化 12-14
設定時の制限事項 12-16
タグなしトラフィック用ネイティブ VLAN 12-20
トンネル ポート 10-3
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 802.3x フロー制御 10-16
ifIndex 値、SNMP 28-6
IFS 1-5
IGMP
join メッセージ 20-3
クエリー 20-4
サポート 1-3
サポートされているバージョン 20-3
脱退タイマーの設定
イネーブル化 20-11
説明 20-6
脱退プロセス、イネーブル化 20-11, 33-9
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 20-13
グローバル Leave 20-13
時間の制御 20-12
ディセーブル化、インターフェイス上 20-13
フラッディング モードからの回復 20-13
マルチキャスト グループからの脱退 20-5
マルチキャスト グループへの加入 20-3
レポート抑制
説明 20-6

ディセーブル化 20-16, 33-11
IGMP グループ
最大数の設定 20-27
フィルタリングの設定 20-28
IGMP スヌーピング
VLAN コンフィギュレーション 20-8
アドレス エイリアス 20-2
イネーブル化およびディセーブル化 20-7, 33-6
クエリア
設定 20-14
設定時の注意事項 20-14
グローバル コンフィギュレーション 20-8
サポート 1-3
サポートされているバージョン 20-3
設定 20-7
即時脱退 20-6
定義 20-1
デフォルト設定 20-7, 33-5, 33-6
方法 20-8
モニタ 20-16, 33-11
IGMP スロットリング
アクションの表示 20-29
設定 20-28
説明 20-25
デフォルト設定 20-26
IGMP 即時脱退
イネーブル化 20-11
設定時の注意事項 20-11
説明 20-6
IGMP フィルタリング
サポート 1-3
設定 20-26
説明 20-25
デフォルト設定 20-25
モニタ 20-29
IGMP プロファイル
コンフィギュレーション モード 20-26
設定 20-26
適用 20-27
interfaces range macro コマンド 10-8
interface コマンド 10-5
Intrusion Detection System
「IDS 装置」を参照
IP ACL
QoS 分類のため 31-7
暗示のマスク 29-7
暗黙の拒否 29-7, 29-12
名前付き 29-12
未定義 29-17
ip igmp profile コマンド 20-26
IP Phone
QoS 14-1
QoS の信頼境界 31-36
QoS を使用してポート セキュリティを確保 31-36
自動分類およびキューイング 31-19
設定 14-4
IP precedence 31-2
IP Service Level Agreement
「IP SLA」を参照
IP SLA
responder
イネーブル化 30-6
説明 30-3
SNMP サポート 30-2
応答時間 30-4
コントロール プロトコル 30-3
サポートされているメトリック 30-2
設定時の注意事項 30-5
定義 30-1
デフォルト設定 30-5
動作 30-3
ネットワーク パフォーマンスの測定 30-2
モニタ 30-7
利点 30-2
IP traceroute
概要 35-15
実行 35-16
IPv4 ACL

インターフェイスへの適用 29-17
拡張、作成 29-8
名前付き 29-12
標準、作成 29-7
IPv4 および IPv6
相違 32-2
デュアル プロトコル スタック 32-6
IPv6
ICMP 32-4
ICMP レート制限 32-8
SDM テンプレート 32-6, 33-1
アドレス 32-2
アドレス フォーマット 32-2
アプリケーション 32-5
近接ディスカバリ 32-4
サポートされている機能 32-3
自動設定 32-5
スタティック ルートの設定 32-9
定義 32-1
デフォルト設定 32-8
モニタ 32-11
利点 32-2
理由 32-1
IP アドレス
128 ビット 32-2
IPv6 32-2
クラスタ アクセス 5-2
検出 6-28
候補またはメンバー 5-4, 5-12
コマンド スイッチ 5-3, 5-10, 5-12
冗長クラスタ 5-10
スタンバイ コマンド スイッチ 5-10, 5-12
「IP 情報」も参照
IP サービス レベル、分析 30-1
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 3-3
手動で 3-10

J

join メッセージ、IGMP 20-3

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
概要 23-1
サポートされている TLV 23-2
スイッチ スタックに関する考慮事項 23-2
設定 23-3
デフォルト設定 23-3
特性 23-4
送信タイマーおよびホールドタイム、設定 23-4
ディセーブル化およびイネーブル化
インターフェイス 23-5
グローバル 23-4
モニタおよびメンテナンス 23-7
LLDP-MED
概要 23-1, 23-2
サポートされている TLV 23-2
設定
TLV 23-6
手順 23-3
モニタおよびメンテナンス 23-7
LLDP Media Endpoint Discovery
「LLDP-MED」を参照
Long-Reach Ethernet（LRE）テクノロジー 1-14

LRE プロファイル、スイッチ クラスタに関する考慮事項 5-14

M

MAC/PHY コンフィギュレーション / ステータス TLV 23-2
MAC アドレス
ACL 29-20
VLAN アソシエーション 6-21
アドレス テーブルの作成 6-21
エージング タイム 6-22
検出 6-28
スタティック
許可 6-27
削除 6-26
追加 6-25
特性 6-25
破棄 6-27
ダイナミック
削除 6-23
ラーニング 6-21
デフォルト設定 6-22
表示 6-27
MAC アドレス通知、サポート 1-10
MAC アドレス テーブル移動更新
設定 18-9
設定時の注意事項 18-5
説明 18-3
デフォルト設定 18-5
モニタ 18-11
MAC アドレスと VLAN のマッピング 12-25
MAC 拡張アクセス リスト
QoS のための設定 31-43
QoS 分類のため 31-5
作成 29-20
定義 29-20
レイヤ 2 インターフェイスへの適用 29-21
MIB
SNMP と相互作用 28-4
概要 28-1
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
MSTP
BPDU ガード
イネーブル化 17-11
説明 17-2
BPDU フィルタリング
イネーブル化 17-12
説明 17-3
CIST、説明 16-3
CIST リージョナル ルート 16-3, 16-6
CIST ルート 16-5
CST
定義 16-3
リージョン間の動作 16-4
EtherChannel ガード
イネーブル化 17-15
説明 17-7
IEEE 802.1D との相互運用性
移行プロセスの再起動 16-26
説明 16-9
IEEE 802.1s
実装 16-7
ポートの役割名の変更 16-7
用語 16-5
IST
定義 16-3
マスター 16-3
リージョン内の動作 16-3
MST リージョン
CIST 16-3
IST 16-3
サポートされるスパニング ツリー インスタンス 16-2
設定 16-16
説明 16-2

ホップ カウント メカニズム 16-6
PortFast
イネーブル化 17-10
説明 17-2
PortFast 対応ポートのシャットダウン 17-2
VLAN を MST インスタンスにマッピング 16-17
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 17-2
概要 16-2
拡張システム ID
セカンダリ ルート スイッチでの影響 16-19
予期しない動作 16-18
ルート スイッチでの影響 16-18
境界ポート
設定時の注意事項 16-16
説明 16-6
サポートされているインスタンス 15-10
サポートされているオプション機能 1-6
ステータスの表示 16-27
ステータス、表示 16-27
設定
Hello タイム 16-23
MST リージョン 16-16
高速コンバージェンスのリンク タイプ 16-25
最大エージング タイム 16-24
最大ホップ カウント 16-25
スイッチ プライオリティ 16-22
セカンダリ ルート スイッチ 16-19
転送遅延時間 16-24
ネイバ タイプ 16-26
パス コスト 16-21
ポート プライオリティ 16-20
ルート スイッチ 16-18
設定時の注意事項 16-16, 17-10
デフォルト設定 16-15
デフォルトのオプション機能の設定 17-10
モード間の相互運用性と下位互換性 15-10
モードのイネーブル化 16-16
ルート ガード
イネーブル化 17-16
説明 17-8
ルート スイッチ
拡張システム ID の影響 16-18
設定 16-18
予期しない動作 16-18
ルート スイッチの選択の防止 17-8
ループ ガード
イネーブル化 17-16
説明 17-9
multicast storm-control コマンド 21-4
Multicast VLAN Registration
「MVR」を参照
MVR
IGMPv3 20-21
アドレス エイリアス 20-21
アプリケーションの例 20-19
インターフェイスの設定 20-23
グローバル パラメータの設定 20-21
サポート 1-3
設定時の注意事項 20-21
説明 20-18
デフォルト設定 20-20
マルチキャスト TV アプリケーション 20-19
モード 20-22
モニタ 20-24

N

NAC
RADIUS サーバを使用する IEEE 802.1x 検証 9-37
RADIUS サーバを使用する IEEE 802.1x 認証 9-37
アクセス不能認証バイパス 9-33
クリティカル認証 9-13, 9-33
レイヤ 2 IEEE 802.1x 検証 1-8, 9-17, 9-37
NameSpace Mapper
「NSM」を参照
Network Admission Control
「NAC」を参照

Network Admission Control Software Configuration Guide 9-39, 9-40
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-23
説明 1-4
要件 xxxii
利点 1-1
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 6-5
定義 6-2
認証 6-4
ピア 6-5
ブロードキャスト メッセージのイネーブル化 6-7
概要 6-2
サポート 1-5
ストラタム 6-2
設定の表示 6-11
送信元 IP アドレス、設定 6-10
タイム
サービス 6-2
同期化 6-2
デバイスの同期化 6-5
デフォルト設定 6-4

P

PAgP
「EtherChannel」を参照
PC（パッシブ コマンド スイッチ） 5-9
Per-VLAN Spanning-Tree Plus
「PVST+」を参照
PIM-DVMRP、スヌーピング方法として 20-9
ping
概要 35-13
実行 35-13
文字出力の説明 35-13
PortFast
イネーブル化 17-10
サポート 1-6
説明 17-2
モード、スパニング ツリー 12-26
PVST+
IEEE 802.1Q トランキングの相互運用性 15-11
サポートされているインスタンス 15-10
説明 15-9

Q

QoS
DSCP 透過 31-38
IP Phone
検出および信頼設定 31-19, 31-36
自動分類およびキューイング 31-19
MQC コマンド 31-1
QoS ラベル、定義 31-4
暗黙の拒否 31-7
概要 31-1
書き換える 31-19
基本モデル 31-4
キュー
SRR、説明 31-12
WTD、説明 31-12
特性の設定、出力 31-62

特性の設定、入力 31-58
ハイ プライオリティ（緊急） 31-18, 31-68
場所 31-11
クラス マップ
設定 31-44
表示 31-70
グローバルなイネーブル化 31-33
サポート 1-9
自動 QoS
イネーブル化、VoIP 用 31-25
実行コンフィギュレーションでの影響 31-24
出力キューのデフォルト 31-20
初期設定の表示 31-29
生成コマンドの一覧 31-21
生成コマンドの表示 31-26
設定時の注意事項 31-24
設定とデフォルトの表示 31-29
設定例 31-27
説明 31-19
ディセーブル化 31-26
トラフィックの分類 31-20
入力キューのデフォルト 31-20
出力インターフェイスの帯域幅の制限 31-69
出力キュー
DSCP または CoS 値のマッピング 31-65
SRR 共有重みの設定 31-67
SRR シェーピング重みの設定 31-66
WTD しきい値の設定 31-63
WTD、説明 31-18
しきい値マップの表示 31-66
スケジューリング、説明 31-4
説明 31-4
バッファ スペースの割り当て 31-63
バッファ割り当て方式、説明 31-17
フローチャート 31-16
信頼状態
信頼性のあるデバイス 31-36
説明 31-5
ドメイン内 31-34
別のドメインとの境界 31-38
設定
DSCP 透過 31-38
DSCP マップ 31-53
IP 拡張 ACL 31-42
IP 標準 ACL 31-41
MAC ACL 31-43
自動 QoS 31-19
集約ポリサー 31-50
出力キューの特性 31-62
信頼境界 31-36
デフォルトのポート CoS 値 31-36
ドメイン内のポートの信頼状態 31-34
入力キューの特性 31-58
別のドメインとの境界での DSCP 信頼状態 31-38
設定時の注意事項
自動 QoS 31-24
標準 QoS 31-32
デフォルトの自動設定 31-20
デフォルトの標準設定 31-29
統計の表示 31-70
入力キュー
DSCP または CoS 値のマッピング 31-59
SRR 共有重みの設定 31-61
WTD しきい値の設定 31-59
WTD、説明 31-14
しきい値マップの表示 31-59
スケジューリング、説明 31-4
説明 31-4
帯域幅の割り当て 31-61
バッファおよび帯域幅の割り当て、説明 31-14
バッファ スペースの割り当て 31-60
プライオリティ キュー、説明 31-14
プライオリティ キューの設定 31-61
フローチャート 31-13
パケットの変更 31-19
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グ 31-16
入力キューイングおよびスケジューリング 31-13
分類 31-7
ポリシングおよびマーキング 31-10
分類
DSCP 透過、説明 31-38
DSCP を信頼、説明 31-5
IP ACL、説明 31-6, 31-7
IP precedence を信頼、説明 31-5
IP トラフィックのオプション 31-6
MAC ACL、説明 31-5, 31-7
クラス マップ、説明 31-8
信頼性のある CoS、説明 31-5
定義 31-4
転送処理 31-3
非 IP トラフィックのオプション 31-5
フレームおよびパケット 31-3
フローチャート 31-7
ポリシー マップ、説明 31-8
ポリサー
数 31-32
設定 31-49, 31-51
説明 31-9
タイプ 31-9
表示 31-70
ポリシー、インターフェイスに結合 31-9
ポリシー マップ
特性 31-46
表示 31-70
物理ポートの非階層型 31-46
ポリシング
説明 31-4, 31-9
トークン バケット アルゴリズム 31-9
マーキング、説明 31-4, 31-9
マークダウン アクション 31-49
マッピング テーブル
CoS/DSCP 31-53
DSCP/CoS 31-56
DSCP/DSCP 変換 31-57
IP precedence/DSCP 31-54
タイプ 31-10
表示 31-70
ポリシング済み DSCP 31-55
QoS の CoS/DSCP マップ 31-53
QoS の CoS 出力キューしきい値マップ 31-18
QoS の CoS 入力キューしきい値マップ 31-14
QoS の DSCP/CoS マップ 31-56
QoS の DSCP/DSCP 変換マップ 31-57
QoS の DSCP 出力キューしきい値マップ 31-18
QoS の DSCP 入力キューしきい値マップ 31-14
QoS の IP precedence/DSCP マップ 31-54
QoS の緊急キュー 31-68
QoS のクラス マップ
設定 31-44
説明 31-8
表示 31-70
QoS の信頼境界 31-36
QoS のポリシー マップ
説明 31-8
特性 31-46
表示 31-70
物理ポートの非階層型
説明 31-9
QoS のポリシング済み DSCP マップ 31-55
QoS のマッピング テーブル
設定
CoS/DSCP 31-53
DSCP 31-53
DSCP/CoS 31-56
DSCP/DSCP 変換 31-57
IP precedence/DSCP 31-54
ポリシング済み DSCP 31-55
説明 31-10
Quality of Service
「QoS」を参照

R

RADIUS
- AAA サーバ グループの定義 8-25
- アトリビュート
  - ベンダー固有 8-29
  - ベンダー独自 8-31
- 概要 8-18
- クラスタ 5-14
- サーバの識別 8-20
- サポート 1-8
- 推奨されるネットワーク環境 8-18
- 設定
  - アカウンティング 8-28
  - 許可 8-27
  - 通信、グローバル 8-21, 8-29
  - 通信、サーバ単位 8-20, 8-21
  - 認証 8-23
  - 複数の UDP ポート 8-20
- 設定の表示 8-32
- デフォルト設定 8-20
- 動作 8-19
- 方式リスト、定義 8-20
- ユーザがアクセスできるサービスのトラッキング 8-28
- ユーザが使用できるサービスの制限 8-27

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 15-11
- サポートされているインスタンス 15-10
- 説明 15-9

Rapid Spanning Tree Protocol
- 「RSTP」を参照

rcommand コマンド 5-14

RCP
- 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-16
  - サーバの準備 B-16
  - ダウンロード B-17

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 30-6
- 説明 30-3

RFC
- 1112、IP マルチキャストおよび IGMP 20-2
- 1157、SNMPv1 28-2
- 1305、NTP 6-2
- 1757、RMON 26-2
- 1901、SNMPv2C 28-2
- 1902 ～ 1907、SNMPv2 28-2
- 2236、IP マルチキャストおよび IGMP 20-2
- 2273 ～ 2275、SNMPv3 28-2

RMON
- アラームおよびイベントのイネーブル化 26-3
- 概要 26-1
- サポート 1-10
- サポートされているグループ 26-2
- ステータスの表示 26-6
- デフォルト設定 26-3
- 統計
  - 収集、イーサネット グループ 26-5
  - 収集、グループ履歴 26-5

RSPAN
- VLAN ベース 25-6
- 宛先ポート 25-6
- 概要 1-10, 25-1

受信トラフィック 25-4
ステータスの表示 25-24
セッション
イネーブルに設定された入力トラフィック 25-21
作成 25-17
送信元トラフィックを特定の VLAN に制限 25-23
定義 25-3
モニタ対象ポートの指定 25-17
設定時の注意事項 25-17
送信元ポート 25-5
他の機能との相互作用 25-8
定義 25-2
デフォルト設定 25-9
伝送トラフィック 25-5
特性 25-7
モニタ側ポート 25-6
モニタ対象ポート 25-5
RSTP
BPDU
処理 16-13
フォーマット 16-13
IEEE 802.1D との相互運用性
移行プロセスの再起動 16-26
説明 16-9
トポロジの変更 16-14
アクティブ トポロジ 16-10
概要 16-9
高速コンバージェンス
エッジ ポートおよび PortFast 16-10
説明 16-10
ポイントツーポイント リンク 16-11, 16-25
ルート ポート 16-10
指定スイッチ、定義 16-9
指定ポート、定義 16-9
提案 / 合意ハンドシェイク プロセス 16-11
ポートの役割
説明 16-9
同期 16-12
ルート ポート、定義 16-9
「MSTP」も参照

S

SC（スタンバイ コマンド スイッチ） 5-9
SDM
説明 7-1
テンプレート
数 7-1
設定 7-2
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 Shell
「SSH」を参照
Secure Socket Layer
「SSL」を参照
set-request 動作 28-5
SFP
ステータスのモニタ 10-20, 35-12
ステータス、表示 35-12
セキュリティと識別 35-12
Shaped Round Robin
「SRR」を参照
show access-lists hw-summary コマンド 29-18
show cdp traffic コマンド 22-5
show cluster members コマンド 5-14
show configuration コマンド 10-18
show forward コマンド 35-20
show interfaces コマンド 10-15, 10-18
show lldp traffic コマンド 23-8
show platform forward コマンド 35-20
show running-config コマンド
ACL の表示 29-16, 29-17
インターフェイスの記述 10-18
show および more コマンド出力、フィルタリング 2-10

Smartport マクロ
Web サイト 11-2
グローバル パラメータ値の適用 11-5, 11-6
作成 11-4
シスコのデフォルト マクロの適用 11-6
設定時の注意事項 11-3
追跡 11-3
定義 11-1
デフォルト設定 11-2
パラメータ値の適用 11-5, 11-7
表示 11-8
マクロの適用 11-5
SNAP 22-1
SNMP
ifIndex 値 28-6
informs
trap キーワード 28-12
イネーブル化 28-15
説明 28-5
ディセーブル化 28-15
トラップとの相違 28-5
IP SLA 30-2
MIB
サポートされている A-1
場所 A-3
MIB 変数にアクセス 28-4
NMS に対するシステム ログ メッセージの制限 27-10
TFTP サーバによるアクセスの制限 28-16
エージェント
説明 28-4
ディセーブル化 28-8
エンジン ID 28-7
帯域内管理 1-5
概要 28-1, 28-4
クラスタ 5-13
クラスタの管理 5-15
グループ 28-7, 28-10
コミュニティ ストリング
概要 28-4
クラスタ スイッチ 28-4
設定 28-8
サポートされているバージョン 28-2
システム コンタクトおよびロケーション 28-16
ステータス、表示 28-18
セキュリティ レベル 28-3
設定例 28-17
通知 28-5
デフォルト設定 28-7
トラップ
informs との相違 28-5
MAC アドレス通知のイネーブル化 6-23
イネーブル化 28-12
概要 28-1, 28-5
説明 28-3, 28-5
タイプ 28-12
ディセーブル化 28-15
トラップ マネージャ、設定 28-14
認証レベル 28-11
ホスト 28-7
マネージャ機能 1-4, 28-3
ユーザ 28-7, 28-10
SNMPv1 28-2
SNMPv2C 28-2
SNMPv3 28-2
SPAN
VLAN ベース 25-6
宛先ポート 25-6
概要 1-10, 25-1
受信トラフィック 25-4
ステータスの表示 25-24
セッション
宛先（モニタ側）ポートの削除 25-12
イネーブルに設定された入力トラフィック 25-13
作成 25-10
送信元トラフィックを特定の VLAN に制限 25-15

定義 25-3
入力転送の設定 25-15, 25-22
モニタ対象ポートの指定 25-10
設定時の注意事項 25-10
送信元ポート 25-5
他の機能との相互作用 25-8
デフォルト設定 25-9
伝送トラフィック 25-5
ポート、制限 21-11
モニタ側ポート 25-6
モニタ対象ポート 25-5
Spanning Tree Protocol
「STP」を参照
SPAN トラフィック 25-4
SRR
共有モード 31-13
サポート 1-9
シェーピング モード 31-12
設定
出力キューでの共有重み 31-67
出力キューでのシェーピング重み 31-66
入力キューでの共有重み 31-61
説明 31-12
SSH
暗号化ソフトウェア イメージ 8-33
暗号方式 8-34
設定 8-34
説明 1-5, 8-33
ユーザ認証方式、サポートされている 8-34
SSL
暗号化ソフトウェア イメージ 8-37
セキュア HTTP クライアントの設定 8-43
セキュア HTTP サーバの設定 8-41
設定時の注意事項 8-40
説明 8-37
モニタ 8-44
STP
BackboneFast
イネーブル化 17-14
説明 17-5
ディセーブル化 17-15
BPDU ガード
イネーブル化 17-11
説明 17-2
ディセーブル化 17-12
BPDU フィルタリング
イネーブル化 17-12
説明 17-3
ディセーブル化 17-13
BPDU メッセージ交換 15-3
EtherChannel ガード
イネーブル化 17-15
説明 17-7
ディセーブル化 17-15
IEEE 802.1D およびブリッジ ID 15-4
IEEE 802.1D およびマルチキャスト アドレス 15-8
IEEE 802.1Q トランクの制限 15-10
IEEE 802.1t および VLAN Identifier 15-4
PortFast
イネーブル化 17-10
説明 17-2
PortFast 対応ポートのシャットダウン 17-2
UplinkFast
イネーブル化 17-14
説明 17-3
インターフェイス ステート
概要 15-4
ディセーブル 15-7
フォワーディング 15-5, 15-7
ブロッキング 15-6
ラーニング 15-6
リスニング 15-6
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 17-2
下位 BPDU 15-3
概要 15-2
カウンタ、クリア 15-23
拡張システム ID

概要 15-4
セカンダリ ルート スイッチの影響 15-16
予期しない動作 15-15
ルート スイッチでの影響 15-15
間接リンク障害の検出 17-5
サポートされているインスタンス 15-10
サポートされているオプション機能 1-6
サポートされている機能 1-6
サポートされているプロトコル 15-9
サポートされているモード 15-9
指定スイッチ、定義 15-4
指定ポート、定義 15-4
冗長接続 15-8
ステータスの表示 15-23
ステータス、表示 15-23
設定
Hello タイム 15-21
最大エージング タイム 15-22
スイッチ プライオリティ 15-20
スパニング ツリー モード 15-13
セカンダリ ルート スイッチ 15-16
転送遅延時間 15-22
転送保留カウント 15-23
パス コスト 15-18
ポート プライオリティ 15-17
ルート スイッチ 15-15
設定時の注意事項 15-12, 17-10
タイマー、説明 15-20
ディセーブル化 15-14
デフォルト設定 15-11
デフォルトのオプション機能の設定 17-10
パス コスト 12-23, 12-24
負荷分散
概要 12-21
パス コストを使用 12-23
ポート プライオリティを使用 12-21
ポート プライオリティ 12-22
マルチキャスト アドレス、影響 15-8
モード間の相互運用性と下位互換性 15-10
優位 BPDU 15-3
ルート ガード
イネーブル化 17-16
説明 17-8
ルート スイッチ
拡張システム ID の影響 15-4, 15-15
設定 15-15
選択 15-3
予期しない動作 15-15
ルート スイッチの選択の防止 17-8
ルート ポート、定義 15-3
ルート ポートを短時間で選択する 17-4
ループ ガード
イネーブル化 17-16
説明 17-9
SunNet Manager 1-4
Switch Database Management
「SDM」を参照
Switched Port Analyzer
「SPAN」を参照
switchport block multicast コマンド 21-7
switchport block unicast コマンド 21-7
switchport protected コマンド 21-6
syslog
「システム メッセージ ロギング」を参照

T

TACACS+
アカウンティング、定義 8-11
概要 8-10
許可、定義 8-11
クラスタ 5-14
サーバの識別 8-13
サポート 1-8
設定
アカウンティング 8-17
許可 8-16
認証鍵 8-13

ログイン認証 8-14
設定の表示 8-17
デフォルト設定 8-13
動作 8-12
認証、定義 8-11
ユーザがアクセスできるサービスのトラッキング 8-17
ユーザが使用できるサービスの制限 8-16
tar ファイル
イメージ ファイル形式 B-25
作成 B-6
抽出 B-7
内容の表示 B-6
TDR 1-10
Telnet
管理インターフェイスへのアクセス 2-10
接続数 1-5
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-28
サーバの準備 B-26
削除 B-28
ダウンロード B-27
コンフィギュレーション ファイル
アップロード B-12
サーバの準備 B-10
ダウンロード B-11
サーバによるアクセスの制限 28-16
自動設定の設定 3-5
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 3-6
TFTP サーバ 1-4
Time Domain Reflector
「TDR」を参照
time-range コマンド 29-14
TLV
LLDP 23-2
LLDP-MED 23-2
定義 23-2
ToS 1-9
traceroute コマンド 35-16
「IP traceroute」も参照
traceroute、レイヤ 2
ARP 35-15
CDP 35-14
IP アドレスおよびサブネット 35-15
MAC アドレスおよび VLAN 35-15
使用上のガイドライン 35-14
説明 35-14
ブロードキャスト トラフィック 35-14
ポート上の複数のデバイス 35-15
マルチキャスト トラフィック 35-15
ユニキャスト トラフィック 35-14
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 31-36
QoS ドメイン間 31-38
QoS ドメイン内 31-34
サポート 1-9
分類オプション 31-5
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 24-5
グローバル 24-5
インターフェイスのリセット 24-6
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 1-6
ステータス、表示 24-7
設定時の注意事項 24-4
ディセーブル化

インターフェイス単位 24-5
グローバル 24-5
光ファイバ インターフェイス上 24-5
デフォルト設定 24-4
ネイバ データベース 24-2
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 24-6
unicast storm control コマンド 21-4
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 27-13
デーモンの設定 27-12
メッセージ ロギングの設定 27-12
UplinkFast
イネーブル化 17-14
サポート 1-6
説明 17-3
ディセーブル化 17-14

V

VLAN
config-vlan モードで作成 12-8
RSPAN 送信元トラフィックを制限 25-23
SPAN 送信元トラフィックを制限 25-15
STP および IEEE 802.1Q トランク 15-10
VLANコンフィギュレーション モードで作成 12-9
VLAN データベースへの追加 12-8
VTP モード 13-3
間のトラフィック 12-2
エージング、ダイナミック アドレス 15-9
拡張範囲 12-1, 12-11
機能 1-6
削除 12-10
サポートされている 12-2
サポートされている数 1-7
図 12-2
スタティック アクセス ポート 12-11
スパニング ツリー インスタンス 12-2, 12-6, 12-12
設定 12-1
設定、ID 1006 ～ 4094 12-12
設定オプション 12-6
設定時の注意事項、拡張範囲 VLAN 12-12
設定時の注意事項、標準範囲 VLAN 12-5
説明 10-2, 12-1
追加 12-8
デフォルト設定 12-7
トークンリング 12-5
トランク上で許可される 12-18
ネイティブ、設定 12-20
パラメータ 12-4
表示 12-14
標準範囲 12-1, 12-4
変更 12-8
ポート メンバシップ モード 12-3
マルチキャスト 20-18
vlan.dat ファイル 12-4
VLAN 1 最小化 12-19
VLAN 1、トランク ポート上でディセーブル 12-19
vlan database コマンド 12-6
VLAN ID、検出 6-28
VLAN Management Policy Server
「VMPS」を参照
VLAN Query Protocol
「VQP」を参照
VLAN Trunking Protocol
「VTP」を参照
VLAN 管理ドメイン 13-2
vlan グローバル コンフィギュレーション コマンド 12-6
VLAN コンフィギュレーション
起動時 12-7
保存 12-7
VLAN コンフィギュレーション モード 2-2, 12-6
VLAN データベース
VLAN コンフィギュレーション、保存 12-7
VLAN、保存 12-4

VTP 13-1
スタートアップ コンフィギュレーション ファイル 12-7
VLAN トランク 12-14
VLAN の削除 12-10
VLAN フィルタリングおよび SPAN 25-6
VLAN メンバシップ
確認 12-28
モード 12-3
VLAN 割り当て応答、VMPS 12-25
VMPS
MAC アドレスの VLAN へのマッピング 12-25
管理 12-29
サーバ アドレスの入力 12-27
再確認インターバル、変更 12-28
再試行の回数、変更 12-29
設定時の注意事項 12-26
設定例 12-30
説明 12-24
ダイナミック ポート メンバシップ
再確認 12-28
説明 12-25
トラブルシューティング 12-30
デフォルト設定 12-26
メンバシップの再確認 12-28
モニタ 12-29
Voice over IP 14-1
VQP 1-7, 12-24
VTP
アドバタイズ 12-16, 13-3
拡張範囲 VLAN 13-1
クライアント モード、設定 13-11
クライアントをドメインに追加 13-15
コンフィギュレーションモードのオプション 13-7
コンフィギュレーション リビジョン番号
注意事項 13-15
リセット 13-16
サーバ モード、設定 13-10
サポート 1-7
使用 13-1
整合性検査 13-4
設定
VLAN コンフィギュレーション モード 13-8
クライアント モード 13-11
グローバル コンフィギュレーション モード 13-7
サーバ モード 13-10
注意事項 13-8
特権 EXEC モード 13-7
トランスペアレント モード 13-12
保存 13-8
要件 13-9
設定要件 13-9
説明 13-1
ディセーブル化 13-12
デフォルト設定 13-7
統計 13-16
トークンリングのサポート 13-4
ドメイン 13-2
ドメイン名 13-8
トランスペアレント モード、設定 13-12
バージョン 1 13-4
バージョン 2
イネーブル化 13-13
概要 13-4
設定時の注意事項 13-9
ディセーブル化 13-14
バージョン、注意事項 13-9
パスワード 13-9
標準範囲 VLAN 13-1
プルーニング
イネーブル化 13-14
概要 13-4
サポート 1-7
ディセーブル化 13-15
例 13-6
プルーニング適格リスト、変更 12-20
モード

移行 13-3
クライアント 13-3, 13-11
サーバ 13-3, 13-10
トランスペアレント 13-3, 13-12
モニタ 13-16
VTP バージョン 2 での整合性検査 13-4

W

Web 認証
IEEE 802.1x のフォールバック 9-39
設定 9-38 ～ 9-40
説明 1-7, 9-17
Weighted Tail Drop
「WTD」を参照
WTD
サポート 1-9
しきい値の設定
出力キューセット 31-63
入力キュー 31-59
説明 31-12

X

Xmodem プロトコル 35-2

あ

アカウンティング
802.1x 9-29
IEEE 802.1x 9-8
RADIUS 8-28
TACACS+ 8-11, 8-17
アクセス
クラスタ、スイッチ 5-12
コマンド スイッチ 5-10
スイッチ クラスタ 5-12
メンバー スイッチ 5-12
アクセス拒否応答、VMPS 12-25
アクセス グループ、インターフェイスへの IPv4 ACL の適用 29-17
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 8-17
TACACS+ 8-10
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 9-13
アクセス ポート
スイッチ クラスタ 5-8
アクセス ポート、定義 10-2
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 30-1
アクティブ リンク 18-2
アップグレード情報
リリース ノートを参照
アップロード
イメージ ファイル
FTP を使用 B-33
RCP を使用 B-37
TFTP を使用 B-28
準備 B-26, B-29, B-34
理由 B-24
コンフィギュレーション ファイル
FTP を使用 B-15
RCP を使用 B-18
TFTP を使用 B-12
準備 B-10, B-13, B-16
理由 B-8
宛先 IP アドレスベース転送、EtherChannel 34-7
宛先 MAC アドレス転送、EtherChannel 34-7
宛先アドレス
IPv4 ACL 29-9
アドバタイズ

CDP 22-1
LLDP 23-2
VTP 12-16, 13-3
アトリビュート、RADIUS
ベンダー固有 8-29
ベンダー独自 8-31
アドレス
MAC アドレス テーブルの表示 6-27
MAC、検出 6-28
スタティック
追加と削除 6-25
定義 6-20
ダイナミック
エージング タイムの変更 6-22
削除 6-23
短縮、エージング 15-9
定義 6-20
デフォルト、エージング 15-9
ラーニング 6-21
マルチキャスト、STP アドレスの管理 15-8
アドレス エイリアス 20-2
アドレスの解決 6-28
アベイラビリティ、機能 1-6
アラーム、RMON 26-3
暗号化、CipherSuite 8-39
暗号化ソフトウェア イメージ
SSH 8-33
SSL 8-37
安全なリモート接続 8-33

い

イーサネット VLAN
追加 12-8
デフォルト値および範囲 12-8
変更 12-8
一時的な自己署名証明書 8-38
一致、IPv4 ACL 29-5
イネーブル シークレット パスワード 8-3
イネーブル パスワード 8-3
イベント、RMON 26-3
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 10-17
カウンタ、クリア 10-21
管理 1-4
記述、追加 10-18
再起動 10-21
サポートされている 10-5
シャットダウン 10-21
情報の表示 10-20
ステータス 10-20
設定
手順 10-6
設定時の注意事項
デュプレックスおよび速度 10-13
説明 10-18
タイプ 10-1
デフォルト設定 10-11
デュプレックスおよび速度、設定 10-14
名前付け 10-18
範囲 10-7
番号 10-5
物理、識別 10-5
フロー制御 10-16
モニタ 10-20
レンジ マクロ 10-8
インターフェイス コマンド 10-6
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 10-21
インターフェイス タイプ 10-5
インターフェイスのクリア 10-21

う

ウィザード 1-2

え

永続的な自己署名証明書 8-38
エージング タイム
MAC アドレス テーブル 6-22
最大
MSTP 16-24, 16-25
STP 用 15-22, 15-23
短縮
MSTP 16-24
STP 用 15-9, 15-22
エージング、短縮 15-9

お

応答時間、測定、IP SLA を使用 30-4
オプション、管理 1-4
音声 VLAN
Cisco 7960 Phone、ポート接続 14-1
IP Phone の音声トラフィック、説明 14-2
IP Phone のデータ トラフィック、説明 14-2
IP Phone への接続 14-4
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 14-5
802.1Q フレーム 14-5
設定時の注意事項 14-3
説明 14-1
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 14-6
着信フレームの CoS プライオリティを信頼する 14-6
デフォルト設定 14-3
表示 14-7

か

解析のためのトラフィックのミラーリング 25-1
ガイド
対象読者 xxxi
目的 xxxi
ガイド モード 1-2
回復手順 35-1
カウンタ、インターフェイスのクリア 10-21
拡張 crashinfo ファイル 35-21
拡張システム ID
MSTP 16-18
STP 15-4, 15-15
拡張範囲 VLAN
作成 12-13
設定 12-11
設定時の注意事項 12-12
定義 12-1
仮想 IP アドレス
クラスタ スタンバイ グループ 5-10
コマンド スイッチ 5-10
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 3-15
間接リンク障害の検出、STP 17-5
管理 VLAN
異なる管理 VLAN からの検出 5-7
スイッチ クラスタに関する考慮事項 5-7
管理アクセス
帯域外コンソール ポート接続 1-5
帯域内
CLI セッション 1-5
SNMP 1-5
デバイス マネージャ 1-5
ブラウザ セッション 1-5
管理アドレス TLV 23-2
管理オプション
CLI 2-1
CNS 4-1
Network Assistant 1-2
概要 1-4
クラスタ化 1-2
管理の簡易性に関する機能 1-4

き

起動
- 起動プロセス 3-1
- 手動で 3-13
- 特定のイメージ 3-14
- ブート ローダ、機能 3-2

機能、互換性のない 21-11
競合、設定 35-11
許可
- RADIUS 8-27
- TACACS+ 8-11, 8-16

許可 VLAN リスト 12-18
許可ポート、IEEE 802.1x 9-7
近接ディスカバリ、IPv6 32-4

く

クエリー、IGMP 20-4
クエリー送信要求、IGMP 20-13
クライアント モード、VTP 13-3
クラスタ、スイッチ
- LRE プロファイルに関する考慮事項 5-14
- アクセス 5-12
- 管理
  - CLI を通じて 5-14
  - SNMP を通して 5-15
- 互換性 5-4
- 自動検出 5-5
- 自動復旧 5-9
- 説明 5-1
- プラン 5-4
- プランニングに関する考慮事項
  - CLI 5-14
  - IP アドレス 5-12
  - LRE プロファイル 5-14
  - RADIUS 5-14
  - SNMP 5-13, 5-15
  - TACACS+ 5-14
- 自動検出 5-5
- 自動復旧 5-9
- パスワード 5-13
- ホスト名 5-12
- 利点 1-1

クラスタ スタンバイ グループ
- 仮想 IP アドレス 5-10
- 考慮事項 5-10
- 自動復旧 5-11
- 定義 5-2
- 要件 5-3
- 「HSRP」も参照

クラスタの要件 xxxiii
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

クリティカル認証、IEEE 802.1x 9-33
グローバル Leave、IGMP 20-13
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 9-11
権限レベル
- 回線に対するデフォルトの変更 8-9
- 概要 8-2, 8-7
- コマンド スイッチ 5-15
- コマンドの設定 8-8
- 終了 8-9
- メンバー スイッチのマッピング 5-15
- ログイン 8-9

検出、クラスタ
- 「自動検出」を参照

こ

構成例、ネットワーク 1-13
高速コンバージェンス 16-10
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 21-11
コマンド
　no および default 2-4
　省略 2-4
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 5-10
　アクティブ（AC） 5-9
　交換
　　クラスタ メンバー 35-8
　　他のスイッチと 35-9
　冗長 5-9
　スタンバイ（SC） 5-9
　設定の競合 35-11
　定義 5-2
　パスワード、権限レベル 5-15
　パッシブ（PC） 5-9
　復旧
　　コマンド スイッチで障害が発生した場合 5-9, 35-7
　　メンバー スイッチとの接続の回復 35-11
　プライオリティ 5-9
　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 5-13
　概要 28-4
　クラスタ 5-13
　クラスタ スイッチ 28-4
　設定 5-13, 28-8
コンソール ポート、接続 2-10
コントロール プロトコル、IP SLA 30-3
コンフィギュレーション交換 B-19
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 28-16
　アーカイブ B-20
　アップロード
　　FTP を使用 B-15
　　RCP を使用 B-18
　　TFTP を使用 B-12
　　準備 B-10, B-13, B-16
　　理由 B-8
　交換、実行コンフィギュレーション B-19, B-20
　交換またはロール バックの注意事項 B-21
　コピー時の無効な組み合わせ B-5
　削除、格納されたコンフィギュレーション B-19
　作成および使用上の注意事項 B-9
　作成、テキスト エディタを使用 B-10
　システム コンタクトおよびロケーション情報 28-16
　消去、スタートアップ コンフィギュレーション B-19
　説明 B-8
　タイプおよび場所 B-9
　ダウンロード
　　FTP を使用 B-13
　　RCP を使用 B-17
　　TFTP を使用 B-11
　　自動 3-12
　　準備 B-10, B-13, B-16
　　理由 B-8
　デフォルトの名前 3-12

入手、DHCP を使用 3-7
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 3-12
ロール バック、実行コンフィギュレーション B-19, B-21
コンフィギュレーション ロールバック B-19, B-20
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 23-2, 23-6

さ

サーバ モード、VTP 13-3
サービス プロバイダー ネットワーク、MSTP および RSTP 16-1
再確認インターバル、VMPS、変更 12-28
再試行の回数、VMPS、変更 12-29
最大エージング タイム
MSTP 16-24
STP 15-22
最大ホップ カウント、MSTP 16-25
サマー タイム（夏時間） 6-14

し

しきい値、トラフィック レベル 21-2
システム記述 TLV 23-2
システム機能 TLV 23-2
システム クロック
概要 6-1
設定
サマー タイム（夏時間） 6-14
手動で 6-12
タイム ゾーン 6-13
夏時間 6-14
日時の表示 6-12
「NTP」も参照
システム プロンプト、デフォルト設定 6-15, 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 23-2
システム メッセージ ロギング
facility キーワード、説明 27-13
level キーワード、説明 27-9
syslog ファシリティ 1-10
UNIX Syslog サーバ
サポートされているファシリティ 27-13
デーモンの設定 27-12
ロギング ファシリティの設定 27-12
イネーブル化 27-4
概要 27-1
シーケンス番号、イネーブル化およびディセーブル化 27-8
設定の表示 27-14
タイム スタンプ、イネーブル化およびディセーブル化 27-7
ディセーブル化 27-4
デフォルト設定 27-3
表示宛先デバイスの設定 27-5
メッセージ重大度の定義 27-8
メッセージの制限 27-10
メッセージ フォーマット 27-2
ログ メッセージの同期化 27-6
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
交換 B-19, B-20
ロール バック B-19, B-21
実行コンフィギュレーション、保存 3-10
自動 QoS
「QoS」を参照
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 5-8
管理 VLAN 5-7

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 5-8
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 3-3
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 10-14
デュプレックス モード 1-3
不一致 35-11
自動復旧、クラスタ 5-9
「HSRP」も参照
重大度、システム メッセージでの定義 27-8
集約可能なグローバル ユニキャスト アドレス 32-3
集約ポート
「EtherChannel」を参照
集約ポリサー 31-50
集約ポリシング 1-9
冗長性
EtherChannel 34-3
STP
パス コスト 12-23
バックボーン 15-8
ポート プライオリティ 12-21
冗長リンクと UplinkFast 17-14
初期設定
Express Setup 1-2
デフォルト 1-10
『Getting Started Guide』および『Hardware Installation Guide』も参照
資料、関連 xxxii
信頼できるタイム ソース、説明 6-2
信頼点、CA 8-38

す

スイッチ ソフトウェア機能 1-1
スイッチド ポート 10-2
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 1-5
スイッチ プライオリティ
MSTP 16-22
STP 15-20
スタートアップ コンフィギュレーション
起動
手動で 3-13
特定のイメージ 3-14
起動のデフォルト設定 3-12
コンフィギュレーション ファイル
自動ダウンロード 3-12
ファイル名の指定 3-12
消去 B-19
スタティック MAC アドレッシング 1-7
スタティック VLAN メンバシップ 12-2
スタティック アクセス ポート
VLAN への割り当て 12-11
定義 10-3, 12-3
スタティック アドレス
「アドレス」を参照
スタティック ルート
設定、IPv6 用 32-9
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 5-10
考慮事項 5-10
設定
定義 5-2
プライオリティ 5-9
要件 5-3

「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 18-2
スティッキー ラーニング 21-9
ステートレス自動設定 32-5
ストーム制御
サポート 1-3
しきい値 21-1
設定 21-3
説明 21-1
ディセーブル化 21-5
表示 21-18
ストラタム、NTP 6-2
スヌーピング、IGMP 20-1
スパニング ツリーおよびネイティブ VLAN 12-16

せ

制限付き VLAN
IEEE 802.1x で使用 9-12
設定 9-31
説明 9-12
成功応答、VMPS 12-25
セキュア HTTP クライアント
設定 8-43
表示 8-44
セキュア HTTP サーバ 8-38
設定 8-41
表示 8-44
セキュア MAC アドレス
最大数 21-9
削除 21-15
タイプ 21-9
セキュア ポート、設定 21-8
セキュリティ機能 1-7
セキュリティ、ポート 21-8
接続、安全なリモート 8-33
接続の問題 35-12, 35-14, 35-15
設定、初期
Express Setup 1-2
デフォルト 1-10
『Getting Started Guide』および『Hardware Installation Guide』も参照
設定値、保存 3-10
設定の競合、メンバー スイッチとの接続の回復 35-11
設定の変更、ロギング 27-11
設定ロガー 27-11
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 35-8
故障したコマンド スイッチの交換 35-9

そ

送信元 IP アドレスベース転送、EtherChannel 34-7
送信元 MAC アドレス転送、EtherChannel 34-6
送信元 / 宛先 IP アドレスベース転送、EtherChannel 34-7
送信元アドレス
IPv4 ACL 29-9
送信元および宛先 MAC アドレス転送、EtherChannel 34-7
即時脱退、IGMP 20-6
イネーブル化 33-9
ソフトウェア イメージ
tar ファイル形式、説明 B-25
回復手順 35-2
場所、フラッシュ B-24
リロードのスケジュール 3-16
「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 3-16

た

対象読者 xxxi
ダイナミック VLAN メンバシップの再確認 12-28
ダイナミック アクセス ポート

設定 12-27
定義 10-3
特性 12-3
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 12-28
接続のタイプ 12-27
説明 12-25
トラブルシューティング 12-30
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-30
HTTP を使用 1-2, B-23
RCP を使用 B-35
TFTP を使用 B-27
準備 B-26, B-29, B-34
デバイス マネージャまたは Network Assistant の使用 B-23
古いイメージの削除 B-28
理由 B-24
コンフィギュレーション ファイル
FTP を使用 B-13
RCP を使用 B-17
TFTP を使用 B-11
準備 B-10, B-13, B-16
理由 B-8
脱退タイマーの設定、IGMP 20-6
端末回線、パスワードの設定 8-6

ち

注意、説明 xxxii
(注)、説明 xxxii

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

て

ディレクトリ
作成と削除 B-4
表示、作業 B-3
変更 B-3
デバイス B-23
デバイス検出プロトコル 22-1, 23-1
デバイス マネージャ
帯域内管理 1-5
スイッチのアップグレード B-23
説明 1-2, 1-4
要件 xxxii
利点 1-1
デバッグ
イネーブル化、特定機能に関する 35-18
エラー メッセージ出力のリダイレクト 35-19
コマンドを使用 35-18
システム全体診断のイネーブル化 35-19
デフォルト ゲートウェイ 3-10
デフォルト設定
802.1x 9-19
CDP 22-2
DHCP 19-7
DHCP Option 82 19-7
DHCP スヌーピング 19-7
DHCP スヌーピング バインディング データベース 19-7
DNS 6-17
EtherChannel 34-9
Flex Link 18-4, 18-5
IGMP スヌーピング 20-7, 33-5, 33-6
IGMP スロットリング 20-26
IGMP フィルタリング 20-25

IP SLA 30-5
IPv6 32-8
LLDP 23-3
MAC アドレス テーブル 6-22
MAC アドレス テーブル移動更新 18-5
MSTP 16-15
MVR 20-20
NTP 6-4
RADIUS 8-20
RMON 26-3
RSPAN 25-9
SDM テンプレート 7-2
SNMP 28-7
SPAN 25-9
SSL 8-40
STP 15-11
TACACS+ 8-13
UDLD 24-4
VLAN 12-7
VLAN、レイヤ 2 イーサネット インターフェイス 12-16
VMPS 12-26
VTP 13-7
イーサネット インターフェイス 10-11
オプションのスパニング ツリー機能 17-10
音声 VLAN 14-3
起動 3-12
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 27-3
自動 QoS 31-20
スイッチの初期情報 3-3
パスワードと権限レベル 8-2
バナー 6-18
標準 QoS 31-29
レイヤ 2 インターフェイス 10-11
デュアル IPv4/IPv6 SDM テンプレート 32-7
デュアル IPv4/IPv6 テンプレート 32-1, 32-6
デュアルパーパス アップリンク
LED 10-4
タイプの設定 10-12
定義 10-4
リンクの選択 10-4
デュアル プロトコル スタック
IPv4 および IPv6 32-6
SDM テンプレート、サポート 32-7
電源管理 TLV 23-2, 23-6
転送遅延時間
MSTP 16-24
STP 15-22
転送保留カウント
「STP」を参照
テンプレート、SDM 7-1

と

統計
802.1x 9-41
CDP 22-4
LLDP 23-7
LLDP-MED 23-7
QoS 入力および出力 31-70
RMON イーサネット グループ 26-5
RMON グループ履歴 26-5
SNMP 入出力 28-18
VTP 13-16
インターフェイス 10-20
トークンリング VLAN
VTP サポート 13-4
サポート 12-5
都市ロケーション 23-3
特権 EXEC モード 2-2
ドメイン名
DNS 6-16
VTP 13-8
トラップ
MAC アドレス通知の設定 6-23
イネーブル化 6-23, 28-12
概要 28-1, 28-5

通知タイプ 28-12
定義 28-3
マネージャの設定 28-12
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 29-3
フラグメント化されていない 29-3
ブロッキング、フラッディング 21-7
トラフィックの優先処理
「QoS」を参照
トラフィックの抑制 21-1
トラフィック ポリシング 1-9
トラブルシューティング
CiscoWorks 28-4
debug コマンド 35-18
ping を使用 35-13
SFP セキュリティと識別 35-12
show forward コマンド 35-20
traceroute 35-15
クラッシュ情報の表示 35-21
システム メッセージ ロギング 27-1
接続の問題 35-12, 35-14, 35-15
単一方向リンクの検出 24-1
パケット転送の設定 35-20
トランキング カプセル化 1-7
トランク
DTP をサポートしないデバイス 12-15
許可 VLAN リスト 12-18
タグなしトラフィック用ネイティブ VLAN 12-20
パラレル 12-23
負荷分散
STP パス コストの設定 12-23
STP ポート プライオリティを使用 12-21, 12-22
プルーニング適格リスト 12-20
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 12-17
定義 10-3, 12-3
トランスペアレント モード、VTP 13-3, 13-12

な

夏時間 6-14
名前付き IPv4 ACL 29-12

に

認識不能な Type-Length-Value（TLV）のサポート 13-4
認証
NTP アソシエーション 6-4
RADIUS
鍵 8-21
ログイン 8-23
TACACS+
鍵 8-13
定義 8-11
ログイン 8-14
ローカル モード、AAA 8-32
「ポートベース認証」も参照
認証失敗 VLAN
「制限付き VLAN」を参照

ね

ネイティブ VLAN
設定 12-20
デフォルト 12-20
ネットワーク管理
CDP 22-1
RMON 26-1
SNMP 28-1
ネットワーク設計
サービス 1-14
パフォーマンス 1-13
ネットワークの構成例

サーバ集約と Linux サーバ クラスタ 1-15
中小規模のネットワーク 1-16
長距離広帯域トランスポート 1-17
ネットワーク サービスの提供 1-14
ネットワーク パフォーマンスの向上 1-13
ネットワークの設計、例 1-13
ネットワーク パフォーマンス、測定、IP SLA を使用 30-2
ネットワーク ポリシー TLV 23-2, 23-6

は

バージョン依存型トランスペアレント モード 13-4
バインディング
DHCP スヌーピング データベース 19-5
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
パケットの変更、QoS を使用 31-19
パス コスト
MSTP 16-21
STP 15-18
パスワード
VTP ドメイン 13-9
暗号化 8-3
回復 35-3
回復のディセーブル化 8-5
概要 8-1
クラスタ 5-13
セキュリティ 1-7
設定
Telnet 8-6
イネーブル 8-3
イネーブル シークレット 8-3
ユーザ名 8-7
デフォルト設定 8-2
パスワードの暗号化 8-3
破損したソフトウェア、Xmodem を使用した回復手順 35-2
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 18-2
バナー
設定
Message-of-The-Day (MoTD) ログイン 6-19
ログイン 6-20
デフォルト設定 6-18
表示されるとき 6-18
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 1-13
範囲
インターフェイス 10-7
マクロ 10-8

ひ

非 IP トラフィックのフィルタリング 29-20
非階層型のポリシーマップ
説明 31-9
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 12-15
xxxii
表記法
コマンド xxxii
テキスト xxxii
マニュアル xxxii
例 xxxii
標準範囲 VLAN 12-4
コンフィギュレーション モード 12-6
設定 12-4
設定時の注意事項 12-5
定義 12-1

ふ

ファイル
- crashinfo、説明 35-21
- tar
  - イメージ ファイル形式 B-25
  - 作成 B-6
  - 抽出 B-7
  - 内容の表示 B-6
- 拡張 crashinfo
  - 説明 35-22
  - ロケーション 35-22
- 基本 crashinfo
  - 説明 35-21
  - ロケーション 35-21
- コピー B-4
- 削除 B-5
- 内容の表示 B-7

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-4
- 表示、ファイル情報 B-3
- ローカル ファイル システム名 B-1

不一致、自動ネゴシエーション 35-11

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 29-20

フィルタリング、show および more コマンド出力の 2-10

フィルタリングの 17-3

ブート ローダ
- アクセス 3-14
- 環境変数 3-14
- 説明 3-2
- トラップドア メカニズム 3-2
- プロンプト 3-14

フィルタ、IP
- 「ACL」と「IP」を参照

不正アクセスの防止 8-1

物理ポート 10-2

不適合マークダウン 1-9

プライオリティ
- CoS の上書き 14-6
- CoS を信頼する 14-6

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 18-2

フラッシュ デバイス、数 B-1

フラッディング トラフィック、ブロッキング 21-7

プリエンプト遅延、デフォルト設定 18-5

プリエンプト、デフォルト設定 18-4

プルーニング、VTP
- イネーブル化
  - VTP ドメイン内 13-14
  - ポート上 12-20
- 概要 13-4
- ディセーブル化
  - VTP ドメイン内 13-15
  - ポート上 12-20
- 例 13-6

プルーニング適格リスト
- VLAN 13-15
- VTP プルーニング用 13-5
- 変更 12-20

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グ 31-16
- QoS 入力キューイングおよびスケジューリング 31-13
- QoS 分類 31-7
- QoS ポリシングおよびマーキング 31-10

ブロードキャスト ストーム 21-1

フローベースのパケット分類 1-9

ブロッキング、パケット 21-7

へ

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 12-11
アクセス 10-2
スイッチ 10-2
スタティック アクセス 12-3, 12-11
セキュア 21-8
ダイナミック アクセス 12-3
デュアルパーパス アップリンク 10-4
トランク 12-3, 12-14
ブロッキング 21-7
保護 21-5
ポート ACL、説明 29-2
ポート VLAN ID TLV 23-2
ポート記述 TLV 23-2
ポートシャットダウン応答、VMPS 12-25
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 31-36
違反 21-9
エージング 21-16
スティッキー ラーニング 21-9
設定 21-12
説明 21-8
他の機能との 21-11
デフォルト設定 21-10
トランク ポート上 21-13
表示 21-18
ポートチャネル
「EtherChannel」を参照
ポート プライオリティ
MSTP 16-20
STP 15-17
ポート ブロッキング 1-3, 21-7
ポートベース認証
EAPOL-Start フレーム 9-5
EAP-Request/Identity フレーム 9-5
EAP-Response/Identity フレーム 9-5
VLAN 割り当て
AAA 許可 9-22
設定作業 9-10
説明 9-9
特性 9-10
Wake-on-LAN、説明 9-15
アカウンティング 9-8
アクセス不能認証バイパス
設定 9-33
説明 9-13
注意事項 9-21
音声 VLAN
PVID 9-14
VVID 9-14
説明 9-14
開始およびメッセージ交換 9-5
カプセル化 9-3
旧版のリリースからのアップグレード 9-22
クライアント、定義 9-2
ゲスト VLAN
設定時の注意事項 9-11, 9-12
説明 9-11
スイッチ
RADIUS クライアント 9-3
プロキシとして 9-3
設定
802.1x 認証 9-22
RADIUS サーバ 9-24
アクセス不能認証バイパス 9-33
クライアントの手動での再認証 9-26

ゲスト VLAN 9-30
スイッチからクライアントへの再送信時間 9-27
スイッチからクライアントへのフレーム再送信回数 9-28
スイッチ上の RADIUS サーバ パラメータ 9-23
制限付き VLAN 9-31
待機時間 9-26
定期的な再認証 9-25
ホスト モード 9-25
設定時の注意事項 9-20
説明 9-1
デバイスの役割 9-2
デフォルト設定 9-19
デフォルト値へのリセット 9-41
統計の表示 9-41
統計、表示 9-41
認証サーバ
RADIUS サーバ 9-3
定義 9-2
方式リスト 9-22
ポート
音声 VLAN 9-14
許可および無許可 9-7
許可ステートおよび dot1x port-control コマンド 9-7
クリティカル 9-13
ポート セキュリティ
音声 VLAN 9-15
説明 9-14
相互作用 9-15
マルチ ホスト モード 9-8
ホスト モード 9-7
マジック パケット 9-15
マルチ ホスト モード、説明 9-8
ポート メンバシップ モード、VLAN 12-3
保護ポート 1-7, 21-5
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 12-30
ホスト名、クラスタ 5-12
ポリサー
数 31-32
設定
一致したトラフィック クラスごと 31-46
複数のトラフィック クラス 31-50
説明 31-4
タイプ 31-9
表示 31-70
ポリシング
説明 31-4
トークン バケット アルゴリズム 31-9

ま

マーキング
集約ポリサーを使用するアクション 31-50
説明 31-4, 31-9
マクロ
「Smartport マクロ」を参照
マジック パケット 9-15
マニュアルの表記法 xxxii
マルチキャスト TV アプリケーション 20-19
マルチキャスト VLAN 20-18
マルチキャスト グループ
加入 20-3
静的な加入 20-10, 33-8
即時脱退 20-6
脱退 20-5
マルチキャスト ストーム 21-1
マルチキャスト ルータ インターフェイス、モニタ 20-17, 33-12
マルチキャスト ルータ ポート、追加 20-9, 33-8

む

無許可ポート、IEEE 802.1x 9-7

め

メッセージ、ユーザへの、バナー経由 6-18
メンバー スイッチ
管理 5-14
自動検出 5-5
接続の回復 35-11
定義 5-2
パスワード 5-12
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 12-3

も

モジュール番号 10-5
モニタ
CDP 22-4
Flex Link 18-11
IGMP
スヌーピング 20-16, 33-11
フィルタ 20-29
IP SLA 動作 30-7
IPv4 ACL の設定 29-22
IPv6 32-11
MAC アドレス テーブル移動更新 18-11
MVR 20-24
SFP ステータス 10-20, 35-12
VLAN 12-14
VMPS 12-29
VTP 13-16
アクセス グループ 29-22
インターフェイス 10-20
解析のためのネットワーク トラフィック（プローブあり） 25-2
機能 1-10
スイッチ間で流れるトラフィック 26-1
速度およびデュプレックス モード 10-15
単一方向リンク用のケーブル 24-1
トラフィックの抑制 21-18
ポート
ブロッキング 21-18
保護 21-18
マルチキャスト ルータ インターフェイス 20-17, 33-12

ゆ

ユーザ EXEC モード 2-2
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 1-5
CPU パケット 6-26
スタティック アドレスの追加 6-26
設定時の注意事項 6-26
説明 6-26
マルチキャスト MAC アドレス 6-26
マルチキャスト アドレス 6-26
ルータ MAC アドレス 6-26
ユニキャスト ストーム 21-1
ユニキャスト トラフィック、ブロッキング 21-7
ユニキャスト要求の転送 1-4

よ

要件
Network Assistant xxxii
クラスタ xxxiii
デバイス マネージャ xxxii

ら

ライン コンフィギュレーション モード 2-3

り

リモート SPAN 25-2
「RSPAN」を参照

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
履歴テーブル、syslog メッセージのレベルと数 27-10
リロードのスケジュール 3-16
リンク冗長性
「Flex Link」を参照
リンクステート トラッキング
設定 34-20
説明 34-18
リンク、単一方向 24-1
リンクに対してローカルなユニキャストアドレス 32-3
リンクの失敗、検出、単一方向 16-8

る

ルート ガード
イネーブル化 17-16
サポート 1-6
説明 17-8
ルート スイッチ
MSTP 16-18
STP 15-15
ループ ガード
イネーブル化 17-16
サポート 1-6
説明 17-9

れ

例
ネットワークの構成 1-13
表記法 xxxii
レイヤ 2 traceroute
ARP 35-15
CDP 35-14
IP アドレスおよびサブネット 35-15
MAC アドレスおよび VLAN 35-15
使用上のガイドライン 35-14
説明 35-14
ブロードキャスト トラフィック 35-14
ポート上の複数のデバイス 35-15
マルチキャスト トラフィック 35-15
ユニキャスト トラフィック 35-14
レイヤ 2 インターフェイス、デフォルト設定 10-11
レイヤ 2 フレーム、CoS で分類 31-2
レイヤ 3 パケット、分類方法 31-2
レポート抑制、IGMP
説明 20-6
ディセーブル化 20-16, 33-11

ろ

ローカル SPAN 25-2
ログイン認証
RADIUS 8-23
TACACS+ 8-14
ログイン バナー 6-18
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 27-8
ログ メッセージのタイム スタンプ 27-7
ロケーション TLV 23-3, 23-6